APUNTES 01

DESARROLLO DE PLANES DE PREVENCIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

Incidentes de Ciberseguridad: es un evento o una serie de eventos singulares, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.
Por ello, es clave conocer su tipología, analizar su impacto, determinar su causa raíz u origen y reaccionar para contenerlo.
En esta unidad se reflexionará acerca de cómo efectuar las tareas pertinentes con objeto de prepararse adecuadamente antes de la aparición del posible incidente.

1.- TAXONOMÍA DE INCIDENTES DE CIBERSEGURIDAD

La Clasificación de los Incidentes de Ciberseguridad INCIBE.
La taxonomía empleada por INCIBE-CERT, en concordancia con la taxonomía definida en la Guía Nacional de Notificación y Gestión de Ciberincidentes, se basa en la Taxonomía de Referencia para la Clasificación de Incidentes de Seguridad, desarrollada coordinadamente por un grupo internacional de equipos de respuesta a incidentes.
Su propósito es alinear los conceptos de análisis, impacto, contención, tratamiento y estudio de todos los incidentes, con objeto de adoptar políticas similares y diseñar respuestas sinérgicas entre las diferentes organizaciones.

Contenido abusivo

- SPAM: correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
- Delito de odio: contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
- Pornografía infantil, contenido sexual o violento inadecuado: material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.

Contenido dañino

- Sistema infectado: sistema infectado con malware. Ejemplo: sistema, ordenador o teléfono móvil infectado con un rootkit (malware que brinda acceso y control remoto de un dispositivo a un hacker).
- Servidor C&C: conexión con servidor de Mando y Control (control centralizado de redes de robots o botnets, además de otras amenazas complejas) mediante malware o sistemas infectados.
- Distribución de malware: recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.
- Configuración de malware: recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de webinjects (robo de credenciales e información personal a través de un navegador) para troyano.
- Malware dominio DGA: nombre de dominio generado mediante DGA, empleado por malware para contactar con un servidor de Mando y Control.

Obtención de información

- Escaneo de redes (scanning): envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP (ping), SMTP (correo), escaneo de puertos.
- Análisis de paquetes (sniffing): observación y grabación del tráfico de redes.
- Ingeniería Social: recopilación de información personal con técnicas cercanas al puro espionaje. Ejemplos: mentiras, trucos, sobornos, amenazas aunque, por lo general, en esta categoría también se suelen incluir los mecanismos de recopilación de información personal basados en herramientas tecnológicas, como pueden ser los stealers y los keyloggers.

Intento de intrusión

- Explotación de vulnerabilidades conocidas: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (CVE). Ejemplos: desbordamiento de buffer, puertas traseras, XSS.
- Intento de acceso con vulneración de credenciales: múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.
- Ataque desconocido: ataque empleando exploit desconocido.

Intrusión

- Compromiso de cuenta con privilegios: compromiso de un sistema en el que el atacante ha adquirido privilegios.
- Compromiso de cuenta sin privilegios: compromiso de un sistema empleando cuentas sin privilegios.
- Compromiso de aplicaciones: compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.
- Robo: intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.

Disponibilidad

- DoS: ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
- DDoS: ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN (sincronización), ataques de reflexión y amplificación utilizando servicios basados en UDP(datagramas, no orientados a conexión).
- Sabotaje: sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados. Interrupciones: interrupciones por causas externas. Ejemplo: desastre natural.

Compromiso de la información

- Acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
- Modificación no autorizada de información. Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación, o encriptado de datos mediante ransomware.
- Pérdida de datos: pérdida de información. Ejemplos: pérdida por fallo de disco duro o robo físico.
- Fuga de Información Confidencial. Información confidencial filtrada, como credenciales o datos personales.

Fraude

- Uso no autorizado de recursos: uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales.
- Derechos de autor: ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplos: Warez (distribución de información a grupos, violando los derechos de autor).
- Suplantación: tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
- Phishing: suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

Vulnerabilidad

- Criptografía débil: servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK (vulnerabilidades y ataques a sistemas de cifrado).
- Amplificador DDoS: servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist (para obtener información de depuración de servidores de hora).
- Servicios con acceso potencial no deseado: servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.
- Revelación de información: acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos: SNMP (mantenimiento) o Redis (gestor de bases de datos en memoria, basado en tablas de hash).
- Sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Otros

- Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
- APT: ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
- Ciberterrorismo: uso de redes o sistemas de información con fines de carácter terrorista.
- Daños informáticos PIC: borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Ejercicio Phishing y Emulación Web - Se mostrará un escenario de Phishing y Emulación Web. Para ello, se emularán las pantallas de entrada de algunos portales populares mediante un Phisher, con objeto de capturar las credenciales de acceso de los usuarios forma fraudulenta.
Ejercicio Stealers y Keyloggers - Existen multitud de herramientas de Ingeniería Social, aparte del espionaje en directo. Estas herramientas permiten robar credenciales e información personal, como se verá a continuación. En este ejercicio esta basada en Stealers y Keyloggers, con objeto de capturar información crítica de forma imperceptible y fraudulenta
Ejercicio Vectores de Infeccion - "Vector de Infección" es un concepto que procede del mundo de la biología, por ejemplo, el mosquito Anopheles es el vector de infección del parásito Plasmodium, causante de la malaria. El procedimiento de actuación de un Vector Informático es idéntico, esto es, es un portador de una infección maliciosa que puede contaminar un sistema informático. Existen muchas variantes de vectores, según el método de infección y el tipo de ataque asociado a la misma. En este ejercicio se generará un vector que actuará a través de un exploit y abrirá una shell inversa en un servidor, permitiendo al hacker tomar el control del mismo.

2.- CONTROLES, HERRAMIENTAS Y MECANISMOS

¿Realmente se ha producido un incidente?
No es fácil en todos los casos determinar con precisión si se ha producido o no un ciberincidente y, si es así, identificar su tipo y evaluar a priori su peligrosidad.
Por esta razón se recomienda implementar y utilizar controles, herramientas y mecanismos de análisis de incidentes, como se estudia a continuación.

2.1.- MONITORIZACIÓN, IDENTIFICACIÓN, DETECCIÓN Y ALERTA DE INCIDENTES: TIPOS Y FUENTES

Básicamente, los indicios de la existencia de un ciberincidente pueden provenir de dos tipos de fuentes: los precursores y los indicadores.

- Un precursor es un indicio de que puede ocurrir un incidente en el futuro.
- Un indicador es un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.

Algunos ejemplos de precursores son:

- Las entradas de log del servidor Web, con los resultados de un escáner de vulnerabilidades.
- El anuncio de un nuevo exploit, dirigido a una atacar una vulnerabilidad que podría estar presente en los sistemas de la organización.
- Amenazas explícitas provenientes de grupos o entidades concretos, anunciando ataques a organizaciones objetivo (es el caso del anuncio de ataques por grupos hacktivistas, por ejemplo).

Los indicadores son muy comunes, tales como:

- El sensor de intrusión de una red emitiendo una alerta cuando ha habido un intento de desbordamiento de buffer de un servidor de base de datos.
- Las alertas generadas por software antivirus.
- La presencia de un nombre de archivo con caracteres inusuales.
- Un registro de log sobre un cambio no previsto en la configuración de un host.
- Los logs de una aplicación, advirtiendo de reiterados intentos fallidos de login desde un sistema externo desconocido.
- La detección de un número importante de correos electrónicos rebotados con contenido sospechoso.
- Una desviación inusual del tráfico de la red interna.

La gestión y coordinación de incidentes desarrollada por el CCN-CERT para los organismos del sector público español, a través del Sistema de Alerta Temprana de Red SARA (SATSARA) y del Sistema de Alerta Temprana para Sistemas de Control Industrial (SAT-ICS) da adecuada respuesta a todas estas necesidades.

2.2.- DETECCIÓN E IDENTIFICACIÓN DE INCIDENTES DE SEGURIDAD FÍSICA

La seguridad física trata del conjunto de medidas que protegen la documentación y equipos ante pérdidas, robos o accesos por personal no autorizado, incluyendo además la formación y habilitación de las personas que deban acceder a materias clasificadas.
La Norma ISO/IEC 27001 da una serie de recomendaciones en el ámbito de la seguridad física y del entorno, en lo relativo a Áreas Seguras y Seguridad de los Equipos, que se resumen a continuación.

2.2.1.- ÁREAS SEGURAS

El objetivo de estas recomendaciones es prevenir el acceso físico no autorizado, los daños e interferencias a la información de la organización y a los recursos de tratamiento de la información.

- Perímetro de seguridad física. Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.

- Controles físicos de entrada. Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

- Seguridad de oficinas, despachos y recursos. Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.

- Protección contra las amenazas externas y ambientales. Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.

- Trabajo en áreas seguras. Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.

- Áreas de carga y descarga. Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.

2.2.2.- SEGURIDAD DE LOS EQUIPOS

El objetivo de estas recomendaciones es evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

- Emplazamiento y protección de equipos. Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.

- Instalaciones de suministro. Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

- Seguridad del cableado. El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.

- Mantenimiento de los equipos. Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

- Retirada de materiales propiedad de la empresa. Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.

- Seguridad de los equipos fuera de las instalaciones. Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

- Reutilización o eliminación segura de equipos. Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.

- Equipo de usuario desatendido. Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.

- Política de puesto de trabajo despejado y pantalla limpia. Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

2.3.- MONITORIZACIÓN, IDENTIFICACIÓN, DETECCIÓN Y ALERTA DE INCIDENTES.

Inteligencia de fuentes abiertas u Open Source Intelligence (OSINT) hace referencia al conocimiento recopilado a partir de fuentes de información de acceso público. El proceso incluye la búsqueda, selección y adquisición de la información, así como su posterior procesado y análisis, con el fin de obtener conocimiento útil y aplicable en distintos ámbitos.

Existen multitud de fuentes abiertas a partir de las cuales se puede obtener información relevante, entre las que destacan:

- Medios de comunicación: revistas, periódicos, radio, etc.
- Información pública de fuentes gubernamentales.
- Foros, redes sociales, blogs, wikis, etc.
- Conferencias, simposios, papers, bibliotecas online, etc.

Algunos ejemplos de la utilización de OSINT son los siguientes:

- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.
- Auditoria de empresas y diferentes organismos con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluar tendencias de mercados.
- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional.
- Como aspecto negativo, es utilizado por cibercriminales para lanzar ataques APT (Amenaza Persistente Avanzada) y Spear Phishing (estafa de correo electrónico o comunicaciones dirigida específicamente a una empresa o una persona).

El Proceso OSINT consta de las siguientes fases:

- Requisitos: es la fase en la que se establecen todos los requerimientos que se deben cumplir, es decir, aquellas condiciones que deben satisfacerse para conseguir el objetivo o resolver el problema que ha originado el desarrollo del sistema OSINT.
- Identificar fuentes de información relevante: consiste en especificar, a partir de los requisitos establecidos, las fuentes de interés que serán exploradas y recopiladas. Hay que tener presente que el volumen de información disponible en Internet es prácticamente inabordable por lo que se deben identificar y concretar las fuentes de información relevante con el fin de optimizar y acotar el proceso de adquisición.
- Adquisición: etapa en la que se obtiene la información a partir de los orígenes indicados. Procesamiento: consiste en dar formato a toda la información recopilada de manera que pueda analizarse posteriormente.
- Análisis: es la fase en la que se genera inteligencia a partir de los datos recopilados y procesados. El objetivo es relacionar la información de distintos orígenes buscando patrones que permitan llegar a alguna conclusión significativa.
- Presentación de inteligencia: consiste en presentar la información obtenida de una manera eficaz, potencialmente útil y comprensible, de manera que pueda ser correctamente explotada.

Se pueden identificar principalmente 2 problemas a la hora de utilizar un sistema OSINT:

- Demasiada información: como ya se ha puesto de manifiesto, la cantidad de información pública disponible en Internet es más que notable. Es por ello, que se debe realizar un proceso muy exhaustivo a la hora de identificar y seleccionar las fuentes de información de interés que se van a recopilar, y que posteriormente servirán para la generación de inteligencia. El hecho de utilizar un catálogo extenso de fuentes conlleva obviamente un mayor gasto a la hora de implementar el sistema, y en el caso de no tener disponibles los recursos necesarios, provoca una significativa ralentización del mismo.
- Fiabilidad de las fuentes: es importante valorar previamente las fuentes que van a nutrir el sistema de información ya que una selección incorrecta de las mismas puede provocar resultados erróneos y desinformación.

La inteligencia recopilada a partir de fuentes de acceso público (OSINT) ha cobrado una especial relevancia en los últimos años, principalmente promovida por la proliferación del uso de Internet y de las redes sociales. Existe una enorme cantidad de información disponible en la web y especialmente en la Deep Web, que puede resultar de gran interés en muy diversos campos que abarcan desde la seguridad de la información, la reputación online o la identificación y gestión de posibles riesgos para la seguridad nacional. Asimismo, cada vez se llevan a cabo más estudios sociológicos, psicológicos, o de otras materias que utilizan como base la información pública disponible en internet.

Otro aspecto significativo, y que permite darse cuenta de la importancia de este tipo de información, es la aparición en el mercado laboral de la figura del Analista OSINT, el cual es el encargado, entre otras cosas, de implementar y gestionar los sistemas OSINT.
Todo esto ha provocado que diferentes países destinen cada vez más recursos a implementar estos sistemas, creando incluso organismos como el Open Source Center (OSC) en Estados Unidos o asociaciones como Eurosint en Bélgica, encargadas de analizar los datos públicos con el fin de identificar y prevenir amenazas.
Por todo lo anteriormente indicado, es innegable que la inteligencia de fuentes abiertas puede aportar gran cantidad de beneficios.

2.4.- HERRAMIENTAS OSINT

Hay multitud de herramientas y servicios útiles a la hora de implementar un sistema OSINT. A continuación se mencionan algunos de ellos:

- **Buscadores habituales**

Google, Bing, Yahoo, Ask. Permiten consultar toda la información que indexan. Asimismo, permiten especificar parámetros concretos (Hacking con buscadores: por ejemplo “Google Hacking” o “Bing Hacking") de manera que se pueden realizar búsquedas con mucha mayor precisión que la que utilizan los usuarios habitualmente.
Dependiendo del buscador empleado se utilizan distintos parámetros, si bien algunos de ellos son comunes, como ocurre con las búsquedas parametrizadas:

- Ficheros con extensión pdf de un sitio web concreto.
- Exploración de sitios hackeados.

Mediante estos parámetros se puede obtener, entre otras cosas, información sensible como nombres de usuarios y contraseñas procedentes de volcados de bases de datos, localización de servidores vulnerables, acceso a dispositivos hardware online como webcams, cámaras de vigilancia o impresoras, o datos personales como DNI, cuentas bancarias, etc.

- **Buscadores especializados:**

- Shodan: Permite entre otras cosas localizar ordenadores, webcams, impresoras, etc. basándose en el software, la dirección IP, la ubicación geográfica, etc. Mediante este servicio es posible localizar información de interés o de acceso a diversos sistemas, como por ejemplo: acceder a los sistemas de control de una Smart City y alterar su funcionamiento.
- NameCHK: es una herramienta que permite comprobar si un nombre de usuario está disponible en más de 150 servicios online. De este modo, se puede saber los servicios que utiliza un usuario en concreto, ya que habitualmente la gente mantiene dicho nombre para todos los servicios que utiliza. Además, disponen de una API que permite automatizar las consultas.
- Knowem: es una herramienta de similares características que NameCHK pero comprueba el nombre en más de 550 servicios, incluyendo dominios disponibles.
- Tineye: es un servicio que, partiendo de una imagen, indica en qué sitios web aparece. Es similar a la búsqueda por imagen que incorpora Google Imágenes.
- Buscadores de información de personas: permiten realizar búsquedas a través de diferentes parámetros como nombres, direcciones de correo o teléfonos. A partir de datos concretos localizan a usuarios en servicios como redes sociales, e incluyen posibles datos relacionados con ellos como números de teléfono o fotos. Algunos de los portales que incorporan este servicio son: Spokeo, Pipl, 123people o Wink.

- **Herramientas de recolección de metadatos:**

- Metagoofil: permite la extracción de metadatos de documentos públicos (pdf, doc, xls, ppt, docx, pptx, xlsx). A partir de la información extraída se pueden obtener direcciones de correo electrónico del personal de una empresa, o el software utilizado para la creación de los documentos y por tanto poder buscar vulnerabilidades para dicho software, nombres de empleados, etc.

- Libextractor: es una aplicación similar a Metagoofil que soporta muchos más formatos, si bien la información obtenida no es de tanta utilidad.

- **Servicios para obtener información a partir de un dominio:**

- Domaintools: es uno de los servicios referentes en este ámbito ya que incorpora un gran número de funcionalidades. Cabe destacar que permite crear alertas a usuarios que registran dominios, monitorizar dominios e IPs, crear alertas para dominios nuevos que contengan ciertas palabras, e incluso un servicio de investigación de gran cantidad de amenazas como spear phishing, denegación de servicio, spam, fraude o malware.

- Robtex: muestra, entre otras cosas, la fiabilidad del dominio, su posición en el ranking Alexa, el listado de subdominios, los servidores de correo o el ISP que utiliza.

- MyIPNeighbors: permite obtener el listado de dominios que comparten servidor con el dominio indicado.

- **APIs de diferentes servicios como Facebook, Twitter o Youtube:**

Mediante los métodos que implementan se pueden consultar de una manera automatizada los datos publicados.

- **Herramientas Palantir y Maltego**

Merecen una mención especial Palantir y Maltego al implementar un gran número de funcionalidades y ser unos de los grandes referentes en la materia de la inteligencia de las fuentes abiertas.

- Palantir: es una empresa que tiene como cliente a diferentes servicios del Gobierno de Estados Unidos (CIA, NSA y FBI) y que se centra en el desarrollo de software contra el terrorismo y el fraude, mediante la gestión y explotación de grandes volúmenes de información.

- Maltego: permite visualizar de manera gráfica las relaciones entre personas, empresas, páginas web, documentos, etc. a partir de información pública.

- **Otras herramientas de interés:**

- GooScan: permite automatizar búsquedas en Google pudiendo identificar de una manera sencilla subdominios de un dominio concreto, fugas de información o posibles vulnerabilidades.

- SiteDigger: al igual que GooScan permite automatizar búsquedas. Busca en la caché de Google para identificar vulnerabilidades, errores, problemas de configuración, etc.

- OsintStalker (FBStalker y GeoStalker): utilizan diferentes redes sociales como Facebook, LinkedIn, Flickr, Instagram y Twitter para recolectar gran cantidad de información sobre una persona. Permiten localizar lugares y sitios web visitados con regularidad, amigos online, etc. y mostrar los datos en Google Maps.

- Cree.py: permite obtener datos de Twitter, Flickr e Instagram. A partir de la selección de una cuenta extrae fechas e información GPS, y crea una base de datos en formato csv o kmz para visualizarlos.

- TheHarvester: esta herramienta obtiene emails, subdominios, host, nombres de empleados, puertos abiertos, etc. a través de diferentes servicios como Google, Bing, LinkedIn y Shodan.

3.- CLASIFICACIÓN, VALORACIÓN, DOCUMENTACIÓN, SEGUIMIENTO INICIAL DE INCIDENTES DE CIBERSEGURIDAD

La gestión de incidentes se basa en disponer de un plan de acción para atender a los incidentes que vayan surgiendo. Además de resolverlos, dicho plan debe incorporar medidas de rendimiento que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
Para ello, la estrategia más importante es la detección temprana de incidentes mediante un IDS eficiente y su análisis rápido en varias etapas (preliminar, profundo, forense) para implementar políticas de respuesta inmediata y programación IPS (prevención de incidentes).

La base del análisis de incidentes está constituida principalmente por dos categorías de herramientas:

- El SIEM, que almacenará la información de los incidentes de forma estructurada, permitiendo a los expertos efectuar el correspondiente estudio y obtener conclusiones aplicables a la prevención.
- Si el incidente ya ha tenido lugar, sólo cabrá utilizar herramientas de Análisis Forense (por ejemplo, Volatility) con el mismo objetivo de fondo, esto es, obtener suficiente información como para efectuar la prevención adecuada, además de rescatar toda la información válida que sea posible.

Además de esto y de forma continua, se deberá efectuar un análisis de rendimiento y solidez de los sistemas de protección, de forma contrastada con las amenazas más frecuentes registradas o reportadas externamente, para reforzar las políticas preventivas.

Ejercicio Resuelto - Muchos ciberataques tienen éxito, por tanto, la clave está en analizarlos bien y extraer las correspondientes conclusiones de cara a la prevención de futuros ataques de similar etiología. En este ejercicio se efectuará un análisis forense preliminar utilizando la herramienta Volatility, con objeto de mostrar qué información se puede derivar de un estudio de la información con posterioridad a un ataque.

Autoevaluación I
¿A qué categoría de la taxonomía de incidentes pertenece el Compromiso de Cuenta, con o sin privilegios?

a) Contenido Abusivo
b) Contenido Dañino
c) Obtención de Información
d) Intento de Intrusión
e) Intrusión
f) Disponibilidad
g) Compromiso de la Información
h) Fraude
i) Vulnerabilidad

Autoevaluación II
¿Cuál de las siguientes herramientas OSINT se centra en el desarrollo de software contra el terrorismo?

a) Maltego
b) SiteDigger
c) TheHarvester
d) Palantir
e) GooScan

Autoevaluación III
¿Cuál es la estrategia más importante en la Gestión de Incidentes?

a) El análisis de rendimiento y solidez de los sistemas de protección
b) La implementación y mantenimiento de un Inventario de Activos
c) La Detección Temprana de incidentes
d) El Análisis Forense de los incidentes

TEST I
1- ¿En qué categoría se clasifica la Explotación de Vulnerabilidades Conocidas?:

a) Compromiso de la Información.
b) Intrusión.
c) Contenido Dañino
d) Intento de Intrusión.
e) Contenido Abusivo.
f) Disponibilidad.
g) Obtención de Información.
h) Vulnerabilidad.
i) Fraude.

2- ¿Qué organismo publica periódicamente la Guía Nacional de Notificación y Gestión de Ciberincidentes?:

a) El CSIRT.
b) El CNI.I
c) INCIBE.
d) El CCN.

3- ¿En qué categoría se clasifica una Denegación de Servicio Distribuida?:

a) Intrusión.
b) Compromiso de la Información.
c) Contenido Dañino.
d) Contenido Abusivo.
e) Intento de Intrusión.
f) Obtención de Información.
g) Disponibilidad.
h) Vulnerabilidad.
i) Fraude.

4-¿En qué categoría se clasifica la Ingeniería Social?:

a) Intento de Intrusión.
b) Compromiso de la Información.
c) Fraude.
d) Disponibilidad.
e) Contenido Abusivo.
f) Intrusión.
g) Vulnerabilidad.
h) Obtención de Información.
i) Contenido Dañino.

5- Un precursor es:

a) Un indicio de que puede ocurrir un incidente en el futuro.
b) Un indicio de que puede haber ocurrido un incidente.
c) Un indicio de que puede estar ocurriendo un incidente en este mismo momento.
d) Un indicio de que puede repetirse un incidente que ya ocurrió en el pasado.

6- ¿En qué categoría se clasifica un Acceso No Autorizado a Información?:

a) Obtención de Información.
b) Contenido Dañino.
c) Disponibilidad.
d) Vulnerabilidad.
e) Intrusión.
f) Compromiso de la Información.
g) Contenido Abusivo.
h) Fraude.
i) Intento de Intrusión.

7-¿Cuál es la clave para combatir un incidente de Ciberseguridad?:

a) Reaccionar para contenerlo.
b) Determinar su causa raíz.
c) Analizar su impacto.
d) Conocer su tipología.
e) Todas las anteriores.

8-¿En qué categoría se clasifica un Phishing?:
a) Contenido Dañino.
b) Obtención de Información.
c) Disponibilidad.
d) Fraude.
e) Contenido Abusivo.
f) Intrusión.
g) Intento de Intrusión.
h) Compromiso de la Información.
i) Vulnerabilidad.

9- ¿En qué categoría se clasifican las Conexiones con Servidor C&C?:
a) Vulnerabilidad.
b) Contenido Dañino.
c) Contenido Abusivo.
d) Intento de Intrusión.
e) Compromiso de la Información.
f) Fraude.
g) Intrusión.
h) Disponibilidad.
i) Obtención de Información.

10- ¿En qué categoría se clasifica la Vulneración de Credenciales?:
a) Fraude.
b) Disponibilidad.
c) Contenido Abusivo.
d) Intrusión.
e) Vulnerabilidad.
f) Intento de Intrusión.
g) Contenido Dañino.
h) Compromiso de la Información.
i) Obtención de Información.

TEST II

1-Categoría de la Pornografía infantil:
a) Compromiso de la Información.
b) Vulnerabilidad.
c) Contenido Dañino.
d) Contenido Abusivo
e) Intrusión.
f) Disponibilidad.
g) Obtención de Información.
h) Intento de Intrusión.
i) Fraude.

2-¿En qué categoría se clasifica el Sniffing?:
a) Contenido Abusivo.
b) Intrusión.
c) Obtención de Información.
d) Intento de Intrusión.
e) Fraude.
f) Compromiso de la Información.
g) Contenido Dañino.
h) Vulnerabilidad.
i) Disponibilidad.

3- ¿En qué categoría se clasifica la Infección de Sistemas con Malware?:
a) Obtención de Información.
b) Intrusión.
c) Disponibilidad.
d) Vulnerabilidad.
e) Contenido Dañino.
f) Contenido Abusivo.
g) Intento de Intrusión.
h) Fraude.
i) Compromiso de la Información.

4- ¿En qué categoría se clasifica una Suplantación?:
a) Intrusión.
b) Fraude.
c) Intento de Intrusión.
d) Disponibilidad.
e) Contenido Abusivo.
f) Contenido Dañino.
g) Vulnerabilidad.
h) Compromiso de la Información.
i) Obtención de Información.

5-¿En qué categoría se clasifica un Sabotaje Físico?:
a) Fraude.
b) Compromiso de la Información.
c) Disponibilidad.
d) Obtención de Información.
e) Intento de Intrusión.
f) Intrusión.
g) Vulnerabilidad.
h) Contenido Dañino.
i) Contenido Abusivo.

6- Señalar cuáles de las siguientes herramientas no se usan en OSINT:
a) Metagoofil, Libextractor.
b) Shodan, NameCHK, Knowem, Tineye.
c) Google, Bing, Yahoo, Ask.
d) GrassMarlin, Tshark, MQTT.

7-¿En qué categoría se clasifica un incidente de Criptografía Débil?:
a) Contenido Abusivo.
b) Intrusión.
c) Compromiso de la Información.
d) Obtención de Información.
e) Fraude.
f) Disponibilidad.
g) Vulnerabilidad.
h) Intento de Intrusión.
i) Contenido Dañino.

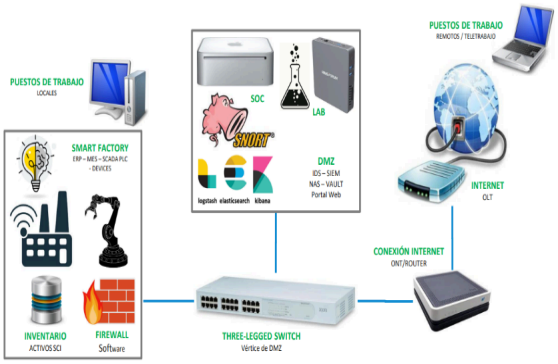
8- ¿En qué categoría se clasifica el Malware de Dominio DGA?:
a) Intento de Intrusión.
b) Vulnerabilidad.
c) Intrusión.
d) Compromiso de la Información.
e) Contenido Abusivo.
f) f. Fraude.
g) Disponibilidad.
h) Contenido Dañino.
i) Obtención de Información

9- ¿En qué categoría se clasifica una Fuga de Información Confidencial?:
a) Vulnerabilidad.
b) Intrusión.
c) Intento de Intrusión.
d) Obtención de Información.
e) Disponibilidad.
f) Fraude.
g) Contenido Abusivo.
h) Contenido Dañino.
i) Compromiso de la Información.

10- Un correo SPAM se clasifica como:
a) Obtención de información.
b) Contenido abusivo.
c) Intento de Intrusión.
d) Contenido dañino

Solución
Autoevaluación I: e)
Autoevaluación II: d)
Autoevaluación III: c)
TEST I: 1 d), 2 c), 3 g), 4 h), 5 a), 6 e), 7 e), 8 d) ,9 b), 10 f)
TEST II: 1 d), 2 c), 3 e), 4 b), 5 c), 6 d), 7 g), 8 h) ,9 i), 10 b)

Clasificación de riesgos y potenciales incidentes.
Un Sistema de Gestión de Seguridad de la Información debe disponer de un correcto sistema de gestión de riesgos.
Un proceso de gestión de riesgos de seguridad de la información trata de identificar, comprender, evaluar y mitigar los riesgos.
El concepto de riesgo se corresponde con la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo.
En esta tarea realizaremos un análisis y gestión de riesgos en la empresa ficticia de la unidad anterior para evitar o disminuir la probabilidad de que se produzcan diversos incidentes. Para este análisis seguiremos la metodología Magerit v.3 desarrollada por el gobierno español.
Además, haremos uso de la herramienta PILAR (versión Basic) que implementa la metodología MAGERIT que ha sido desarrollada por el Centro Criptológico Nacional (CCN). Este software es privativo y debe licenciarse, pero provee de una licencia de evaluación de 30 días, que es la que usaremos en este caso práctico.
Introducción: Diagrama de bloques y detalles de activos de la empresa.
La empresa tiene el siguiente diagrama de bloques:



Activo	Dirección IP	Sistema Operativo	Modelo Máquina	Función Empresa
Router	192.168.1.1	Askey SO	RTF3505VW	Router conexión Internet
Switch	192.168.1.11	3COM SO	SuperStack 3 3300XM	Three-Legged Switch
SOC	192.168.1.101	MacOS Ventura	Mac Mini M1	IDS/SIEM/NAS/VAULT
Labo_Server	192.168.1.102	Debian 11	MinisForum HM90	Servidor Laboratorio
ERP	192.168.1.25	Debian 11	ProLiant uServer Intel Xeon E	Servidor Gestor Empresarial
MES	192.168.1.24	Raspbian	Raspberry Pi 4B	Servidor Gestor Factoría
SCADA	192.168.1.23	Raspbian	Raspberry Pi 4B	Supervisión / Control / Firewall / Inventario
PLC	192.168.1.22	Raspbian	Raspberry Pi 4B	Controlador lógico
DEVICE	192.168.1.21	Raspbian	Raspberry Pi 4B	Dispositivo fabril
B.D. Inventario	192.168.1.25	MacOS Ventura	Mac Mini M1	Base de datos de Inventario
B.D. ECO/FIN	192.168.1.25	MacOS Ventura	Mac Mini M1	Base de datos ECO / FIN
Puestos trabajo	192.168.1.50-99	Windows 11 Pro	Lenovo ThinkCentre M720t	Puestos de trabajo
Maquetas, Prototipos	192.168.1.102	Debian 11	MinisForum HM90	Maquetas, prototipos, lanzaderas
Portal Web	192.168.1.102	Debian 11	MinisForum HM90	Portales web
Big Data, IA	192.168.1.50-99	Windows 11	Lenovo ThinkCentre M720t	Sistemas Big Data, IA

Apartado 1: Priorización y jerarquía de activos.

- A partir de la lista de activos de la introducción, se deben priorizar y jerarquizar indicando los que crees que son esenciales para la empresa. Se ordenan desde el de más importancia al de menor, además se deben indicar aquellos que dependen de otros.

Jerarquía de activos según la importancia para la empresa:

1. ERP — depende de: bd eco/fin, puestos trabajo, router, switch
2. SCADA — depende de: PLC y router y switch
3. MES — depende de: ERP, SCADA, PLC, router y switch
4. PLC — depende de: SCADA y router y switch
5. Base datos Económica/Financiera — depende de: ERP, router, switch
6. Base de Datos Inventario — depende de: ERP, router, switch
7. SOC — depende de: router, switch
8. Router — depende de: switch
9. Switch — depende de: router
10. Big Data e Inteligencia Artificial — depende de: bd inventario y eco/fin puestos, router, switch
11. Puestos de Trabajo — depende de: ERP, MES, router, switch
12. Portal Web — depende de: router, switch
13. Servidor Laboratorio — depende de: puestos trabajo, router, switch
14. Dispositivos/Device — depende de: router, switch
15. Maquetas y Prototipos — depende de: servidor laboratorio y puestos de trabajo

El orden que se ha establecido, se basa en la importancia de los activos para la continuidad de las operaciones y eficiencia, teniendo en cuenta el impacto que tendría la pérdida o interrupción de cada uno en las operaciones, la seguridad y los objetivos de la empresa.
Los activos más importantes como ERP, MES y SCADA, son prioritarios debido a su papel central en la gestión de la producción, inventario y recursos. También se ha dado alta prioridad a los PLC y las bases de datos debido a su conexión con la fabricación y las decisiones financieras.
Orden de prioridad:

- Prioridad alta (1-5), activos esenciales para la operación
- Prioridad media-baja (6-9) sirven de soporte a la operación crítica
- Prioridad media (10-12) tienen importancia operativa, pero no son activos críticos inmediatos
- Prioridad baja (13-15) tienen importancia estratégica o de soporte, pero con menor impacto directo.

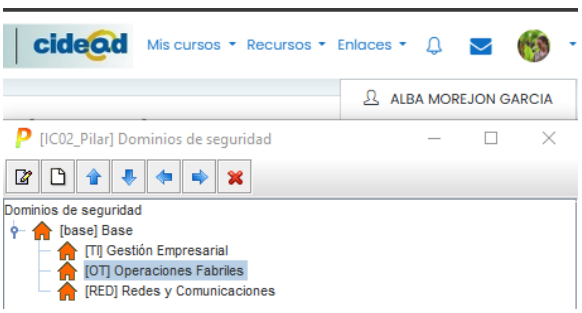
- De la anterior lista de activos, se debe seleccionar uno por cada uno de estos tipos indicados: activo esencial de información, activo esencial de servicio, activo de equipamiento informático y un activo de redes de comunicación.

Activos Información	Activos Servicio	Activos Equipamiento informático	Activos Redes de Comunicación
ERP	SCADA	Puestos Trabajo	Router
BD Eco/Fin	MES	Labo Server	Switch
BD Inventario	PLC	Dispositivos	SOC
Big Data e IA	Portal Web	Maquetas/Prototipo	

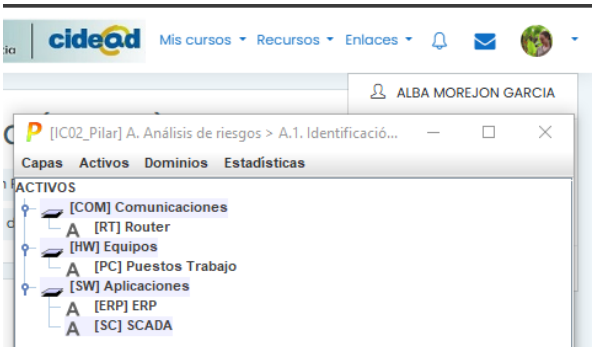
Activos Información, engloba los sistemas que manejan y centralizan datos críticos para las operaciones administrativas.
Activos Servicio, sistemas que soportan los procesos operativos y fabriles.
Activos Equipamiento informático, dispositivos físicos utilizados por los empleados o en entornos de prueba.
Activos Redes de Comunicación, incluimos los elementos que garantizan la conectividad y seguridad de la red.
ERP, centraliza la información para la toma de decisiones, además,integra todas las áreas de la empresa (inventario, producción, ventas…). Es importante para la gestión de recursos, planificación y control de las operaciones.
SCADA, tiene un rol crítico en la gestión y seguridad de los procesos a tiempo real, si falla la seguridad, calidad y la producción pueden verse comprometidos de inmediato
Puestos de Trabajo, permite al empleado interactuar con los sistemas de información y gestión. Sin ellos, los empleados no tendrían acceso a las herramientas necesarias para su trabajo, paralizando las operaciones administrativas y productivas.
Router, asegura la conectividad entre las zonas de la empresa y gestiona las conexiones con el exterior, no contar con él bloquearía la operación de los sistemas dependientes de él.

- Con el uso de la herramienta PILAR se debe recoger la información de los cuatro activos anteriores. Estos activos deben definirse en su capa correcta y en un dominio de seguridad adecuado, por lo que habrá que crear los dominios de seguridad necesarios.
Muestra la ventana detallada de información de estos cuatro activos.
La herramienta PILAR es un software que se utiliza para el análisis y la gestión en sistemas de información, sirve para ayudar a identificar, clasificar y proteger los activos. Su principal enfoque es evaluar los riesgos de seguridad y definir las medidas de protección.
A continuación se muestra la configuración elegida:

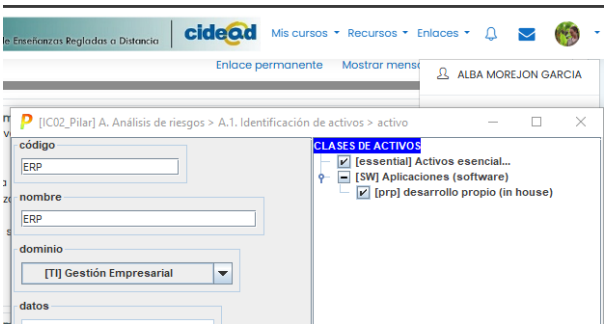
- Dominios

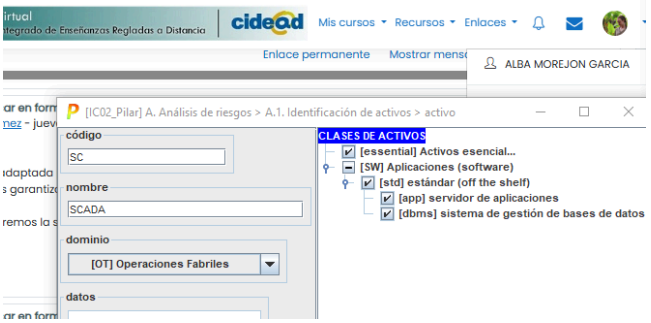


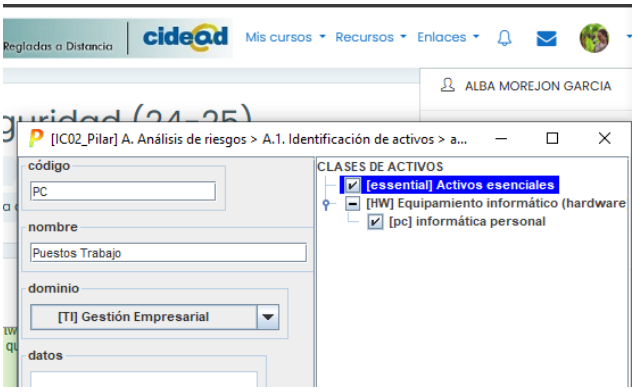
- Clases

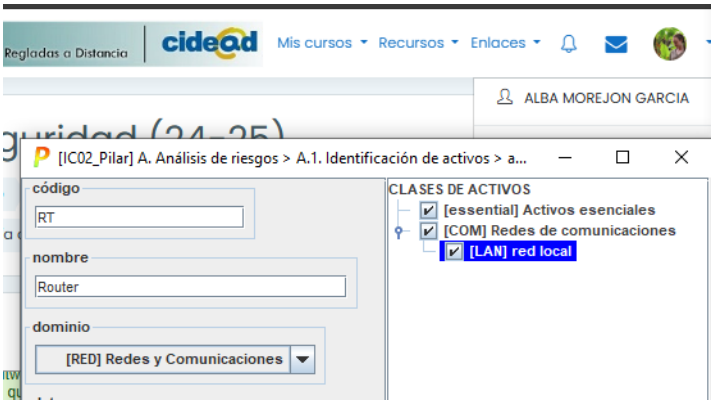


- Activos







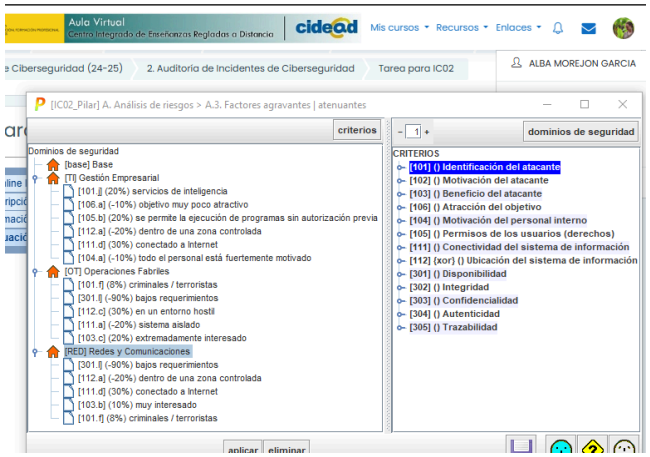


Apartado 2: Valoración de los dominios de seguridad.

- Debes determinar el nivel de importancia que tienen los activos esenciales en sus diferentes dominios de seguridad definidos. Muestra una captura de pantalla con la valoración numérica de los activos en sus dominios de seguridad.

Para el Router se prioriza la importancia en la conectividad y seguridad de la red. La disponibilidad crítica, se refleja en un tiempo de recuperación rápido, ya que su interrupción afecta las operaciones inmediatas. La Integridad y confidencialidad se vincula a la posible manipulación y accesos no autorizados, lo que podría derivar en incidentes graves o problemas legales al procesar datos personales. La autenticidad y trazabilidad son relevantes para investigar accesos indebidos y asegurar la continuidad del servicio.
El impacto en las operaciones de la organización de los Puestos de Trabajo es central. Una interrupción afecta directamente a la productividad y el manejo de información personal, dado que maneja datos confidenciales y accesos críticos, los riesgos de seguridad y autenticidad son altos con potencial de incidentes graves. La trazabilidad asegura el monitoreo de actividades, lo que ayuda en las auditorías y control de riesgos laborales.
El ERP es vital para la gestión empresarial, por lo que su disponibilidad debe ser inmediata. La integridad es crucial porque cualquier error podría generar incumplimientos legales significativos. Su información confidencial tiene alto valor económico y comercial, lo que lo convierte en un objetivo atractivo para ataques. Además, garantizar autenticidad y trazabilidad es esencial para proteger datos sensibles y cumplir normativas.
Finalmente, el SCADA controla los procesos industriales críticos, lo que lo hace indispensable para las operaciones. Su disponibilidad tiene impacto directo en la seguridad física de las infraestructuras, ya que un fallo podría causar pérdidas o interrupciones graves, así como afectar a la integridad de los datos. La confidencialidad y trazabilidad aseguran que las operaciones sean seguras y que los incidentes puedan ser investigados eficazmente.

- Además, debes indicar, al menos, un par de factores atenuantes y/o agravantes por cada dominio de seguridad. Muestra una captura de estos factores.

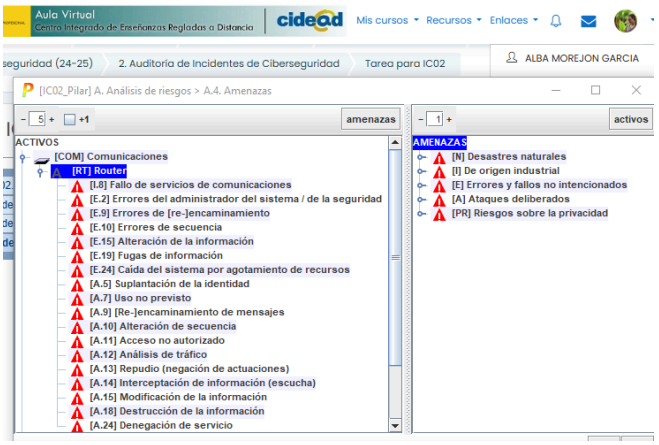


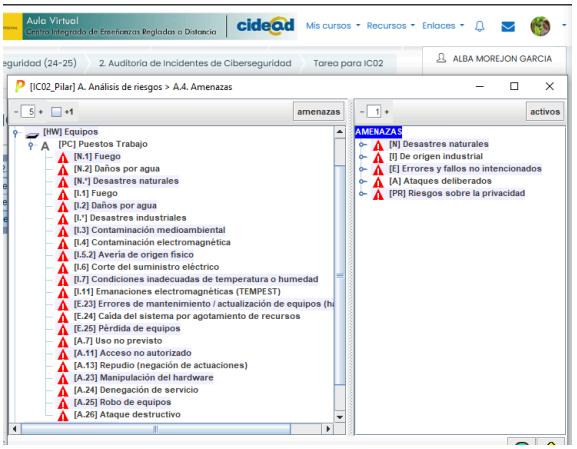
En el dominio de Gestión Empresarial los principales agravantes seleccionados están relacionados con la alta exposición a ataques debido a la conexión a Internet y la flexibilidad de los permisos que pueden permitir la ejecución de programas no autorizados, lo que eleva significativamente el riesgo. Como atenuantes están la ubicación controlada de los sistemas y la motivación del personal, que reduce la probabilidad de riesgos internos
En el caso de Operaciones Fabriles se prioriza como agravante la ubicación en el entorno hostiles, donde los sistemas están más expuestos a riesgos físicos y lógicos, además del alto interés que puede suscitar en atacantes que buscan interrumpir procesos industriales críticos. Sin embargo, el aislamiento del sistema y los menores requerimientos de disponibilidad, actúan como factores atenuantes al limitar las posibles vías de ataque y tolerar pequeñas interrupciones.
Para Redes y Comunicaciones, los agravantes destacados son la conexión a Internet, que lo expone a amenazas externas y el interés de los atacantes, dado que comprometer el router puede proporcionar acceso a toda la red. Como atenuantes, se ha considerado la ubicación controlada, que protege físicamente el dispositivo y los bajos requerimientos de confidencialidad en la configuración, lo que disminuye la sensibilidad de los datos asociados

Apartado 3: Determinación de las amenazas y sus salvaguardas dispuestas.

- Para cada uno de los cuatro activos seleccionados en el apartado uno, indica la lista de amenazas asociada a estos activos. Realiza una captura de cada activo con su lista de amenazas asociada.

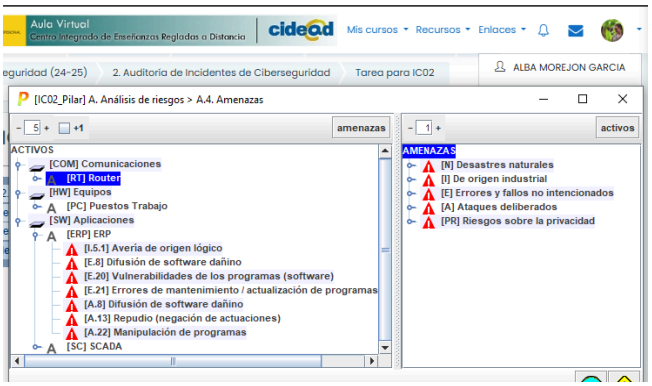
PILAR aplica automáticamente los valores prefijados del fichero TSV

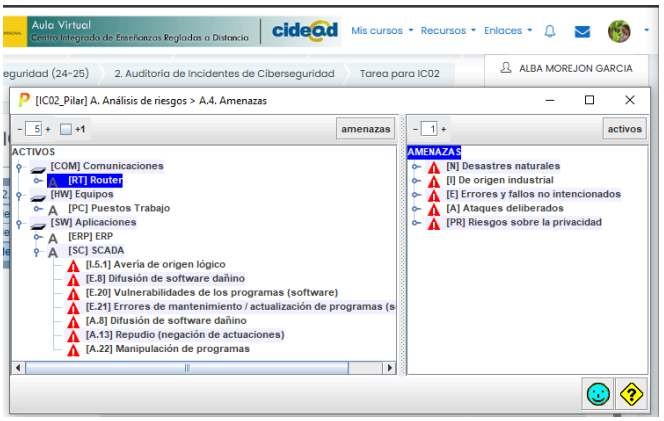




El router tiene vulnerabilidades relacionadas con el acceso no autorizado a la red, ya que un atacante podría intentar obtener acceso a la red interna a través de él. Las amenazas como la intercepción de información y el análisis de tráfico, son comunes en este tipo de equipos. La denegación de servicios también es una amenaza relevante ya que podrían afectar a la disponibilidad de los servicios, además, los routers pueden ser atacados a través de vulnerabilidades de software y fallos en los servicios de comunicaciones lo que hace que la gestión del dispositivo y su actualización sea crucial.

Los puestos de trabajo son puntos de entrada frecuente para los atacantes, debido al abuso de privilegios de acceso y la suplantación de identidad. Las amenazas como la difusión de software dañino o el robo de equipos, son importantes dado que los dispositivos pueden ser comprometidos o sustraídos. Además, las vulnerabilidades de configuración y los errores del administrador, las técnicas de ingeniería social abren las puertas a los atacantes.





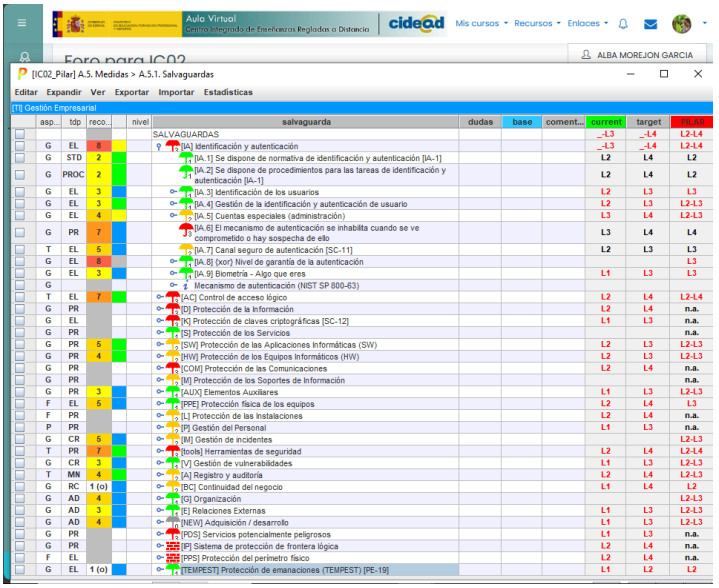
En el sistema SCADA la denegación de servicio es una amenaza considerable ya que un ataque puede paralizar la planta, así como, el corte del suministro eléctrico y averías físicas o lógicas son riesgos comunes que podrían afectar la operación del sistema. La destrucción de información también es una amenaza significativa ya que podría alterar los procesos de producción o incluso causar daños materiales. Además, la inyección de código malicioso y el acceso no autorizado pueden ser explotadas por ciberdelincuentes.

El sistema ERP, las amenazas de abuso de privilegios o suplantación de identidad son relevantes debido a la cantidad de usuarios que interactúan con el sistema. La manipulación de configuraciones y modificación de información pueden alterar el funcionamiento del sistema comprometiendo su integridad. También, se debe tener en cuenta el riesgo de errores administrativos en la configuración y mantenimiento del sistema que podrían generar vulnerabilidades.

- Además, para cada dominio de seguridad recoge las salvaguardas que te muestra la herramienta ordenadas de mayor a menor prioridad según la herramienta. Para cada una de estas salvaguardas debes indicar una acción concreta que se puede realizar para llevarla a cabo en cierto grado. Incluye también el estado actual y el estado objetivo de esta salvaguarda. Por último realiza una captura de pantalla en la que se muestran estas salvaguardas configuradas.

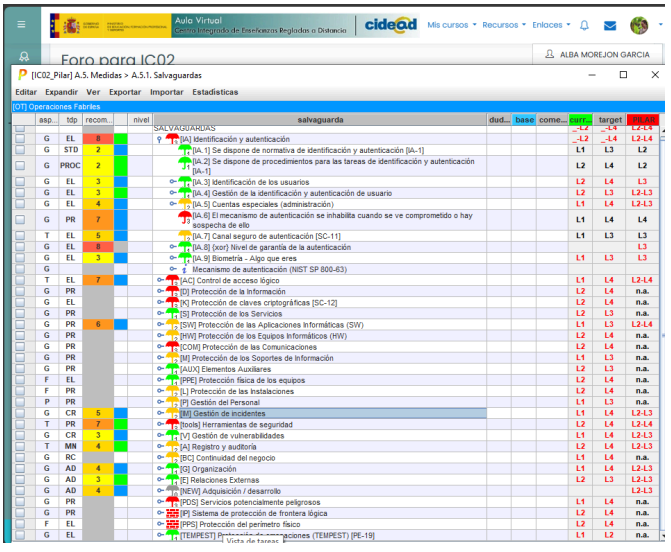
Hay valores que no permitía modificar como es el caso de Mecanismos de autenticación, que luego más adelante seguirá afectando al desempeño de la práctica.

Salvaguardas Gestión Empresarial:



- Se dispone de normativas de identificación y autenticación, crear y publicar una política formal de identificación y autenticación, indicando procedimientos para gestionar usuarios y contraseñas. (L2-L4)
- Registro y auditoría, implementar un sistema centralizado que capture logs de eventos importantes. (L2-L4)
- Gestión de incidentes, diseñar un plan de respuesta a incidentes, incluyendo simulaciones periódicas para asegurar su eficiencia. (L2-L4)
- Continuidad del negocio, desarrollar y mantener un plan con estrategias de recuperación ante desastres naturales y ciberataques. (L1-L4)
- Protección de las aplicaciones informáticas, implementar un programa de revisión y actualización software para garantizar la corrección de vulnerabilidades críticas. (L2-L3)

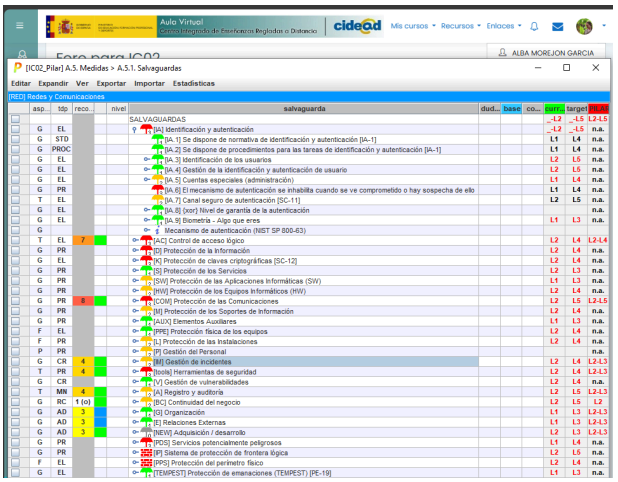
Salvaguardas Operaciones Fabriles:



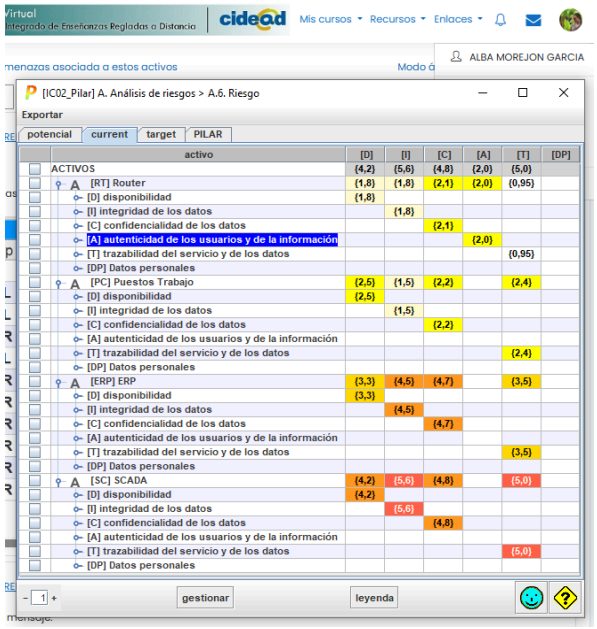
- Identificación de usuarios, configurar cuentas individuales para cada operativo cuentas compartidas. (L2-L4)
- Protección física de equipos, instalar cerraduras y controles de acceso para proteger equipos críticos. (L2-L4)
- Protección física de las instalaciones, instalar cámaras de vigilancia y personal de seguridad. (L2-L4)
- Gestión de incidentes, enseñar a los empleados para que reporten incidentes de los sistemas de control. (L1-L4)
- Protección de las comunicaciones, configurar canales cifrados para comunicaciones entre los sistemas de control y centros de operaciones. (L2-L4)

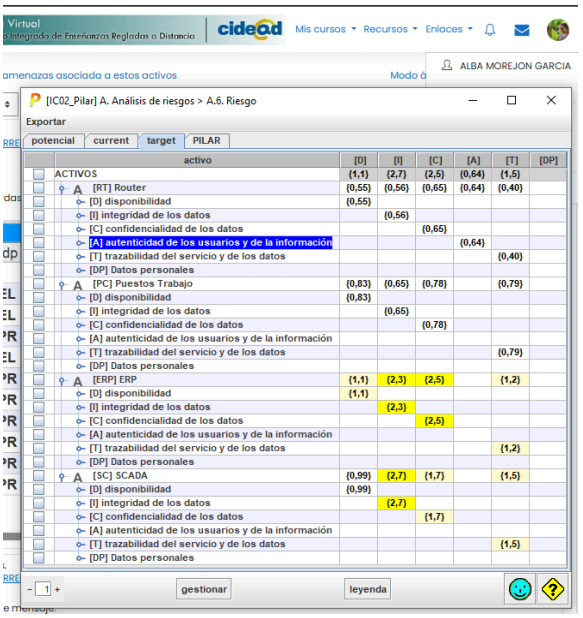
Salvaguardas Redes y Comunicaciones:

- Canal seguro de autenticación, configurar autenticación a través de protocolos seguros (HTTPS SSH VPN). (L2-L5)
- Control de acceso lógico, implementar listas de control de acceso en dispositivos de red para segmentar y restringir el tráfico no autorizado. (L2-L4)
- Sistemas de protección de frontera lógica, configurar un firewall con políticas de inspección de tráfico y detección de intrusiones. (L2-L5)
- Herramientas de seguridad, instalar y mantener actualizadas herramientas de seguridad como antivirus, IDS/IPS y escáneres de vulnerabilidades en los equipos de red. (L2-L4)
- Registro y auditoría, configurar syslog para centralizar los registros de los dispositivos de red y generar alertas de eventos críticos. (L2-L5)



Apartado 4: Estimación del riesgo a considerar por la empresa para su estudio y toma de decisiones.
- Para cada uno de los cuatro activos seleccionados en el apartado uno, indica la estimación del estado del riesgo a asumir por la empresa. Se debe indicar la estimación actual (current) y la estimación objetivo (target).





Hay espacio sin rellenar porque en las salvaguardas anteriores hubo espacio que no me dejaba rellenar la propia aplicación.

- Calcula la bajada que se produce en los riesgos en cada uno de los criterios de seguridad para cada activo.

Router

- Disponibilidad: 1,8 - 0,55 = 1,25
- Integridad:1,8 - 0,56 = 1,24
- Confidencialidad: 2,1 - 0,65 = 1,45
- Autenticidad: 2,0 - 0,64 = 1,36
- Trazabilidad: 0,95 - 0,40 = 0,55

Puestos Trabajo

- Disponibilidad: 2,5 - 0,83 = 1,67
- Integridad: 1,5 - 0,65 = 0,85
- Confidencialidad: 2,2 - 0,78 = 1,42
- Trazabilidad: 2,4 - 0,79 = 1,61

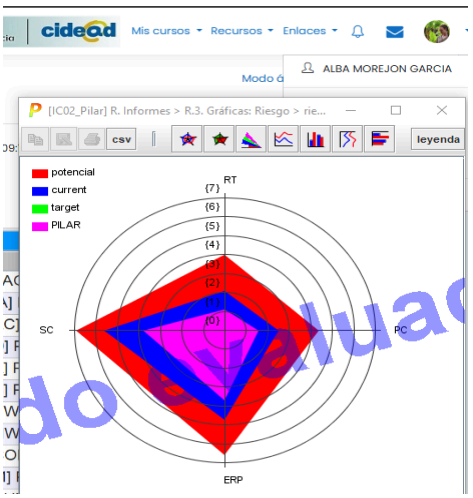
ERP

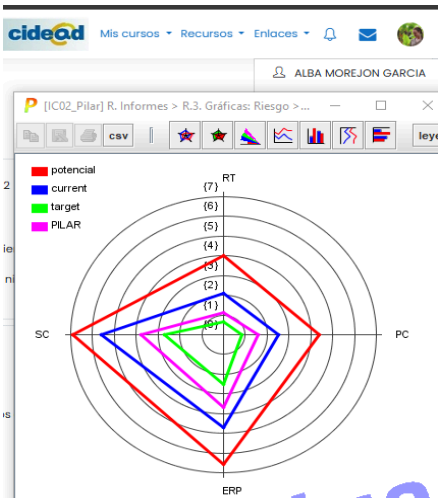
- Disponibilidad: 3,3 - 1,1 = 2,2
- Integridad: 4,5 - 2,3 = 2,2
- Confidencialidad: 4,7 - 2,5 = 2,2
- Trazabilidad: 3,5 - 1,2 = 2,3

SCADA

- Disponibilidad: 4,2 - 0,99 = 3,21
- Integridad: 5,6 - 2,7 = 2,9
- Confidencialidad: 4,8 - 1,7 = 3,1
- Trazabilidad: 5,0 - 1,5 = 3,5

- Además, muestra una captura de la gráfica de riesgos de tipo "Área" en la que se muestran los cuatro activos con sus valores actuales, objetivo y recomendados por PILAR.





Apartado 5: Taxonomía de incidentes.

Para cada uno de los cuatro activos seleccionados en el apartado uno y tras el estudio de sus riesgos, determina un tipo de incidente que podría producirse en relación a sus riesgos. Para este tipo de incidente indica el grupo al que pertenece y realiza una pequeña explicación sobre este.

Router

Tipo de Incidente: Acceso no autorizado

Grupo: Ciberataque

Un atacante podría aprovechar una puerta trasera en el firmware del router o descifrar las contraseñas con técnicas de fuerza bruta. Una vez dentro la red interna se habría visto comprometida, ya que el intruso podría interceptar el tráfico, descifrando mensajes confidenciales o desconfigurando las rutas críticas de la red. Este incidente no sólo pondría en jaque las comunicaciones, sino que abriría las puertas a un ataque más completo en la infraestructura tecnológica

Puestos de trabajo

Tipo de Incidente: Difusión de software

Grupo: Malware

Los puestos de trabajo son un objetivo común para la difusión de malwares, debido a descargas inadvertidas, correos electrónicos de phishing o dispositivos externos infectados, basta con que un empleado haga clic en un archivo adjunto sospechosamente o conecte un USB. Una vez activado el malware se despliega extendiéndose por la red, además si el atacante utiliza ingeniería social las víctimas podrían ayudarse en saberlo abriendo las puertas a sus datos o a los sistemas críticos. Este tipo de incidentes podría comprometer la confidencialidad y disponibilidad de la información, además de permitir movimientos laterales dentro de la red poniendo en riesgo sistemas críticos como el ERP o SCADA.

ERP

Tipo de Incidente: Abuso de privilegios

Grupo: amenazas internas

Un usuario con permisos elevados podría acceder a datos sensibles de manera indebida, alterar configuraciones o manipular datos financieros, esta acción podría desestabilizar todo el sistema empresarial: facturas, estrategias, pedidos... Este incidente comprometería la integridad y la confidencialidad del sistema, generando posibles pérdidas financieras, dañando a la reputación y causando dificultades operativas en la gestión empresarial.

SCADA

Tipo de Incidente: Denegación de servicios

Grupo: Ciberataque

Un ataque DoS contra un sistema SCADA, supondría la detención de las máquinas, los sensores inutilizados, las líneas de producción paradas, entre otras consecuencias. Este ataque satura los recursos del sistema hasta que el sistema colapsa, puede tener efectos devastadores: interrupción, inhabilitación, pérdida, paralización… Un pequeño comando ejecutado desde un lugar remoto podría afectar a los procesos críticos y detener una operación multimillonaria. Este incidente afecta directamente la disponibilidad del sistema con graves consecuencias económicas y operativas.