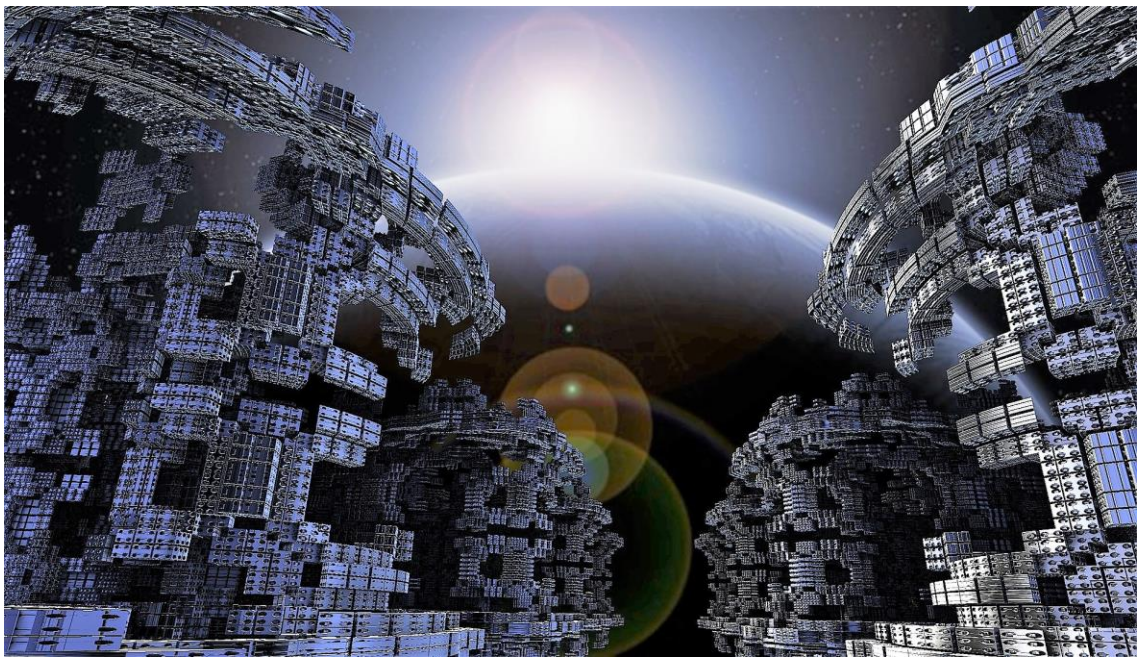
CIBERSEGURIDAD Machine 4.0

En **Encriptia** nos preocupa la **seguridad de la información**. Consideramos que la información es uno de los activos más valiosos de las empresas y por lo tanto debe protegerse. Es por ello que ofrecemos una serie de servicios relacionados con la seguridad de la información.



Tratamos de evitar que la información pueda ser revelada a individuos, entidades o procesos no autorizados y asegurar la **continuidad adecuada de los procesos de negocio** hasta en los casos más extremos mediante un ciclo de mejora continua y situando el gasto en seguridad por debajo de los impactos potenciales de los riesgos que se pretenden evitar.

Todos los servicios son realizados por analistas de seguridad informática que cuentan con la Certificación de Hacking Ético (CEH) y la Certificación de Análisis Forense (CHFI) y son miembros de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos y de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica, existiendo la posibilidad de visado de los informes periciales realizados por dichas asociaciones.

Seguridad dirigida a la industria

Análisis forense de los controles numéricos

Mediante el análisis forense de los controles numéricos basado en la metodología que recomienda la norma ISA95 detectamos las vulnerabilidades que esconden y que permitirían a un extraño acceder a los datos de producción, consumo, etc. que tiene la máquina que controla. Mediante el análisis de los ficheros de almacenamiento de datos y su estructura verificamos que no se recoge más información que la especificada. A través de los controles de entrada y salida detectamos flujos anormales de datos que pueden indicar que se está produciendo una fuga de información.

Auditoría de seguridad de las redes

Una auditoría de redes inalámbricas (Wifi, ZIGBEE, …) permite conocer el nivel de seguridad en las comunicaciones inalámbricas de la organización incluyendo dispositivos del internet de las cosas como smartphones, tablets, sistemas SCADA, TVs, dispositivos de domótica. Del mismo modo la seguridad de las redes soportadas en sistemas alámbricas (UTP, fibra, …..) puede verse comprometida.

Mediante el **análisis de la estructura de la red** y sus subredes descubrimos la eficacia de aporta la segmentación de la misma si es que la tiene.

La existencia de **cortafuegos** no garantiza su efectividad a la hora de proteger la red interna del exterior, por ello es necesario verificar la correcta configuración del mismo.

El **análisis de los paquetes de datos**. Mediante la captura de las tramas de estos, se chequean los datos que son enviados por la red, de esta manera salen a la luz fallos que permiten descubrir problemas como cuellos de botella, detectar a intrusos y la creación de registros de red no autorizados.

Verificación de software seguro

Mediante un test de estrés al que es sometido al software que incorporan los sistemas de implantados en la máquina se comprueba su robustez, verificando que no tiene un vía indirecta para poder ser saboteado.

Política de la gestión de la seguridad

Todos los elementos que conforman la seguridad de la infraestructura han de tener una monitorización y seguimiento periódico para determinar necesidades de parcheado, actualizaciones y otros problemas derivados de la aparición de vulnerabilidades o defectos que puedan detectarse en el periodo de funcionamiento.

Internet of Things

Es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet. Se analizan la existencia de elementos a evaluar, tales como máquinas, elementos domóticos, etc.

Auditoría de caja negra

El auditor toma el papel de un atacante externo que no conoce ninguna característica interna de la organización. Tiene una visión ciega del sistema y debe recopilar todo tipo de información sobre el objetivo para la planificación de potenciales ataques.

Auditoría de caja gris

Permite al auditor tomar el papel de un empleado con privilegios limitados que realiza su trabajo en una ubicación concreta. En esta auditoría se evalúan los riesgos para la organización donde un empleado intenta acceder a información a la que no tiene acceso simulando un ataque interno a la empresa.

Auditoría de caja blanca

El auditor toma el rol de un usuario de la empresa con acceso a la totalidad de los datos de la misma y se le proporciona de toda la información necesaria para evaluar la seguridad del entorno sometido a prueba, incluyendo el código fuente, archivos de configuración, documentación, diagramas, etc.

Albert Einstein 15 Of.19
Edificio CEIA
Parque Tecnológico de Álava
C.P. 01510 Miñano (Araba/Álava)
info@encriptia.com
+34 945 067 000

Colón de Larreategui 26, 4ºC
C.P. 48009 Bilbao (Bizkaia)
info@encriptia.com
+34 944 666 000

www.encriptia.com

Encriptia
INTELIGENCIA CORPORATIVA Y SEGURIDAD

GRUPO SVC