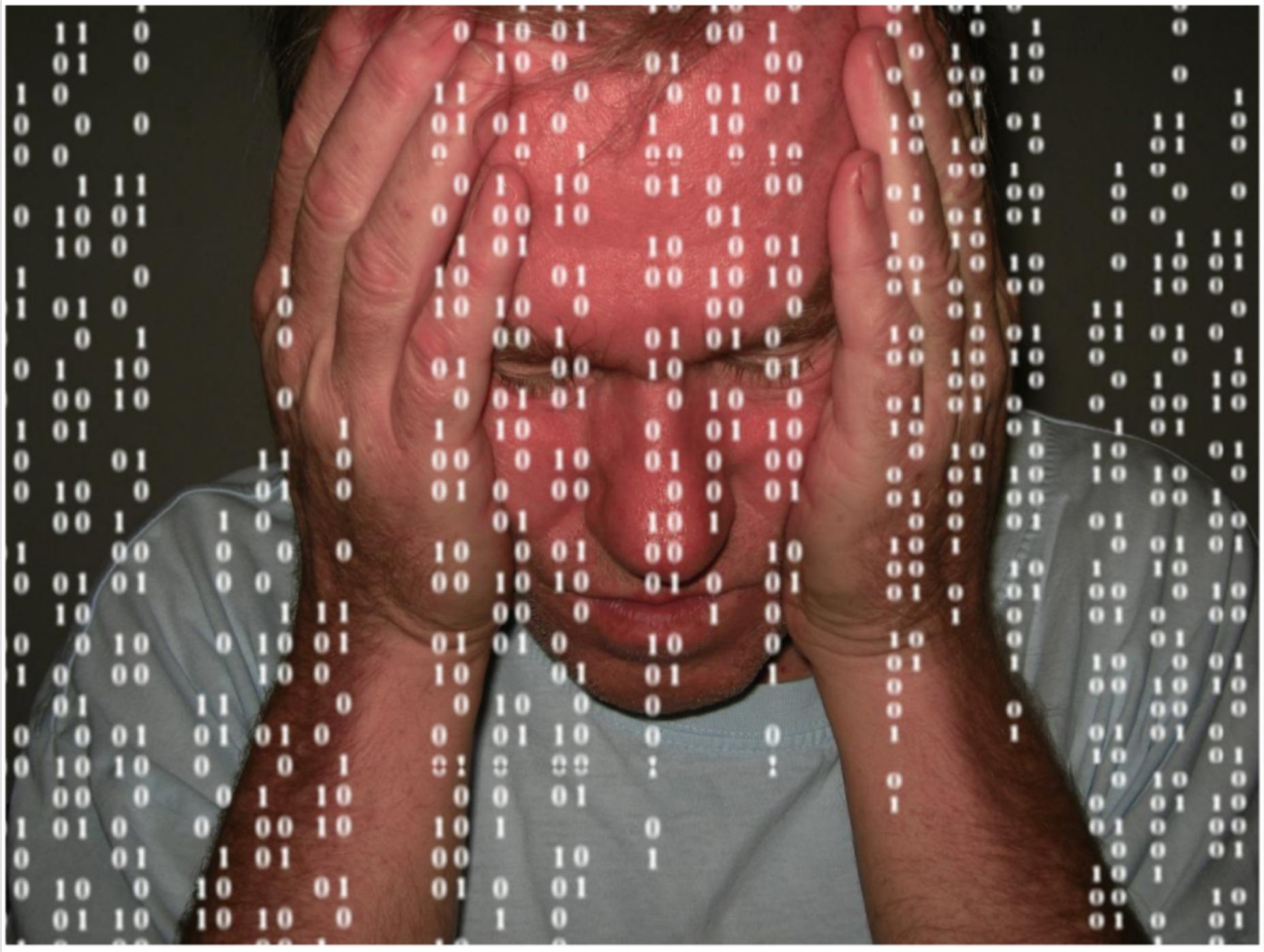
CIBERSEGURIDAD

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 buscando la eficiencia, 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).

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, 1ºC
C.P. 48009 Bilbao (Bizkaia)

info@encriptia.com

+34 944 666 000

www.encriptia.com

Encriptia
INTELIGENCIA CORPORATIVA Y SEGURIDAD

GRUPO SVC

Servicios de seguridad informática

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.

Análisis de vulnerabilidades en aplicaciones web

Para el diagnóstico de vulnerabilidades en aplicaciones web se utilizará la metodología OWASP, que define una serie de pruebas agrupadas en 11 categorías que suponen un total de 91 puntos de control de análisis exhaustivo.

Concienciación en ingeniería social

Los empleados son la última barrera del sistema de defensa de la seguridad de las empresas y por ello ofrecemos dos tipos de campañas de concienciación cuyos resultados se reportarán a la dirección en un informe ejecutivo.

Auditoría de seguridad wireless

Una auditoría wireless 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.

Pericial de análisis forense

El análisis forense es la solución ideal para empresas que tienen la necesidad de investigar los incidentes de seguridad informática que se producen en sus sistemas de información. Permite tomar las medidas oportunas para que el suceso no vuelva a ocurrir, además de conocer en profundidad los detalles del mismo.

Diagnóstico de denegación de servicio

Dicho diagnóstico evalúa la fortaleza y recuperación ante situaciones de estrés de la infraestructura TIC en una organización. Permiten comprobar las contramedidas existentes ante un ataque de denegación de servicio distribuido, el tiempo de recuperación y evalúa la disponibilidad de los servicios enfocado en el ámbito de continuidad de negocio.

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.

Tasaciones y valoraciones

Nuestros peritos pueden certificar el valor económico de su parque informático y su software valorándolo como aportación en la creación de sociedades o fundaciones, procesos concursales o entregas tangibles ante situaciones delicada, mediante una valoración experta.

Borrado seguro de datos certificado

El borrado seguro de datos se basa en la eliminación de datos sensibles ofreciendo un certificado y si la situación lo requiere una incorporación de certificación notarial, tanto en las instalaciones del cliente como en el lugar que nos indique y con la supervisión que sea necesaria.

Análisis de fugas de información

Ante una sospecha de fuga de información, el auditor, intentará determinar si el personal interno podría desvelar información confidencial de la organización. Además tratará de evadir el proxy de la organización para enviar la información al exterior y analizará si es posible infectar las máquinas con software malicioso no detectable.

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, 1ºC
C.P. 48009 Bilbao (Bizkaia)

info@encriptia.com

+34 944 666 000

www.encriptia.com

Encriptia
INTELIGENCIA CORPORATIVA Y SEGURIDAD

GRUPO SVC