

DarFe - Oferta formativa



La empresa "DarFe Learning & Consulting S.L." fue creada en 2009 dedicándose a Redes y Ciberseguridad desde esa fecha.

Es la **única empresa española** que basa su formación y concienciación en Ciberseguridad sobre el 100% de su propio Know How.

Presenta para su libre y gratuita descarga en Internet:



Formación y concienciación en Ciberseguridad.



En la actualidad el mayor riesgo que tienen las organizaciones pasa por el factor humano. Es una realidad que el más alto porcentaje de los ataques que sufren las redes y sistemas de TI tienen su puerta de entrada en errores, generalmente ocasionados por desconocimiento y las menos por imprudencia. En ambos casos, la solución pasa por la preparación y el lanzamiento de un adecuado plan de formación y concienciación de ciberseguridad.

La formación y concienciación en Ciberseguridad, para que sea eficiente debe ser planificada en detalle y de ser posible ajustada y particularizada para cada empresa. No es lo mismo la respuesta que posee una empresa tecnológica, que otra de marketing, provisión, automotriz, ropa, restauración, etc. Cada una de ellas, debería recibir un “discurso” diferente.




Lo mismo sucede sobre los diferentes roles, perfiles, responsabilidades y grupos dentro de cada organización, pues nuevamente no debería ser igual el plan de formación y concienciación del equipo directivo, gerencial, operativo, ni el de los responsables de redes y TI (que también necesitan su cuota en estos temas).

DarFe posee una basta experiencia, sobre todo demostrada y perfectamente verificable por toda su trayectoria y la cantidad de evidencias que pueden encontrarse en cualquier buscador de Internet y/o en redes sociales. En particular debemos poner de manifiesto los comentarios, “likes” y recomendaciones que pueden verse sobre la calidad que ponemos en esta labor. Al respecto debemos destacar, otro aspecto que nos llena de orgullo: no tenemos absolutamente NINGÚN “dislike” en ninguna de nuestras publicaciones, esto es algo muy difícil de encontrar y, en definitiva, no deja de evidenciar que sabemos lo que hacemos, y sobre todo le ponemos mucho cariño.




La actividad de formación y concienciación que ofrece **DarFe**, siempre nace de una primera aproximación con el potencial cliente para conocer algunos detalles sobre su funcionamiento, actividad y magnitud. Este primer reconocimiento, nos permite ofrecer dos cosas:

-  Un “Plan de formación y concienciación”.
-  Una propuesta de cronología de formación y concienciación”.

En general, esta actividad suele estar dirigida al menos a tres grupos:

-  Directivo y gerencial.
-  Empleados.
-  Administradores de redes y sistemas.

La plataforma de formación On-line con la que cuenta DarFe (<https://moodle.darfe.es>), sumado a la importante base de conocimientos de casi quince años de impartir formación y concienciación, en la actualidad nos permite ofrecer cursos:

-  Presenciales.
-  Semipresenciales.
-  100% Online.












Cualquiera de ellos ajustable a las necesidades y requerimientos del cliente.

La experiencia con que cuenta DarFe, como así también la del personal que imparte estos temas, nos permite abarcar un amplio abanico de detalle que va desde la formación básica, orientada al personal no técnico que está empezando a cobrar consciencia de ciberseguridad, hasta los más altos expertos de redes y TI. Sobre cualquiera de estos extremos, y por supuesto sobre los perfiles intermedios también, ya hemos llevado adelante varios programas de formación.

A continuación, se presenta brevemente los cursos y temáticas sobre las que ya hemos trabajado en más de una oportunidad, y dejamos para el final, algunos de los temarios y programas para que puedan ser tenidos como referencia.

Actividades profesionales y de formación realizadas por DarFe

1. Proyectos y capacitaciones ejecutadas.

-  Impartición del curso “Técnico en Seguridad de Redes y Sistemas”.
-  Impartición del curso “Administrador de Sistemas UNIX”
-  Diseño, implantación y securización de redes WiFi.
-  Capacitación y Concienciación en Seguridad y RD 03/2010.
-  Implantación y certificación de la norma ISO/UNE-27001.
-  Auditoría Interna de la norma ISO/UNE-27001 .
-  Capacitación y Concienciación en el Esquema Nacional de Seguridad.
-  Auditoría Interna de Ley Orgánica de Protección de datos de carácter personal.
-  Adecuación a la LOPD.
-  Adecuación al Reglamento Europeo de Protección de Datos (GDPR).
-  Securitización de plataforma empresarial en Internet e Intranet.

- 🔒 Establecimiento de radio enlace seguro (redundante con dos tecnologías inalámbricas diferentes) entre dos edificios para voz y datos.
- 🔒 Diseño y planificación del Sistema de Gestión Informático en entornos LAN y WAN.
- 🔒 Implantación de una plataforma de Video Conferencia y de e-Learning (con Open Source).
- 🔒 Migración de una infraestructura de red LAN (física y lógica) con sus servicios y plataformas, adecuación a LOPD de la misma y securización final.
- 🔒 Diseño de arquitectura de red para gran empresa carrier de telecomunicaciones.
- 🔒 Auditorías y diagnósticos de seguridad en entornos internacionales de redes de telecomunicaciones de voz y datos, fija y móvil.
- 🔒 Análisis de seguridad sobre tecnología LTE (4G móvil) para gran empresa de telecomunicaciones.
- 🔒 Análisis de seguridad sobre tecnología 5G para gran empresa de telecomunicaciones.
- 🔒 Auditorías de ciberseguridad de redes y servicios TI.
- 🔒 Plan de concienciación sobre el empleo de código seguro.
- 🔒 Bastionado (Hardening) de plataformas e infraestructuras.
- 🔒 Uso seguro de las redes y sistemas de la organización.
- 🔒 El peligro del mal uso de Internet, correo electrónico y ordenadores no plataformados.
- 🔒 Capacitación sobre “trabajo remoto seguro”.
- 🔒 Mejoras en la monitorización y supervisión de infraestructuras de redes y TI.

2. Publicaciones y artículos redactados.

Todos estos documentos pueden ser descargados desde nuestra Web (www.DarFe.es) o encontrados en Internet a través de cualquier buscador.

- 🔒 Libro **“Seguridad por Niveles”**
- 🔒 Libro **“Seguridad en Redes”**
- 🔒 Libro **“Ciberseguridad, una estrategia Informático/Militar”**

 Libro **“Manual de la Resiliencia”**

 IP Versión 6 (parte 01) – Componentes

 IP Versión 6 (parte 02) – Direcciones

 IP Versión 6 (parte 03) – Encabezado

 Análisis de ISO-27001

 Implantación práctica de ISO-27001


 ISO-27001 e ISO-27004

 ISO-27001 Los controles (Parte I)

 ISO-27001 Los controles (Parte II)

 Revista Auditoría y Seguridad (Nº 3 - 2006) “Auditoría, Evaluación, Test de seguridad (Metodología OSSTMM)”


 Revista Auditoría y Seguridad (Nº 4 - 2006) "Análisis de ISO-27001-2005 (Parte 1)"

 Revista Auditoría y Seguridad (Nº 5 - 2006) “Análisis de ISO-27001:2005 - Breve Resumen”


 Revista Auditoría y Seguridad (Nº 9 - 2007) “ISO-27001 e ISO-27004”


 Revista Auditoría y Seguridad (Nº 13 - 2007) " ISO 27001 y las PyMEs"

 Revista Auditoría y Seguridad (Nº 14 - 2007) Problemática, Ventajas y Desventajas de ISO 27001

 Revista Auditoría y Seguridad (Nº 16 - 2007) "¿ISO 20000 ó ISO 27000?"


 Revista Auditoría y Seguridad (Nº 17 - 2007) Metodología de Implantación y Certificación en PyMEs

 Revista Auditoría y Seguridad (Nº 18 - 2008) ISO-27001, y las AAPP

 Revista Auditoría y Seguridad (Nº 19 - 2008) ISO-IEC 27001:2005; LOPD (Parte1)

 Revista Auditoría y Seguridad (Nº 20 - 2008) ISO-IEC 27001:2005; LOPD (Parte2)

 Revista Auditoría y Seguridad (Nº 21-2008) Métricas de Seguridad, Indicadores y Cuadros de Mando

 Revista Auditoría y Seguridad (Nº 22 - 2008) " Auditoria Interna en ISO-27001"

 Revista Security & Technology (Nro 4-2006) ANÁLISIS DE ISO-27001 Implantación y certificación

 Revista Auditoría y Seguridad (Nº 24 - 2008) " La Ley 11...¿J?"

- 👤 Esquema Nacional de Seguridad
- 👤 Análisis de ataques/vulnerabilidades SS7/Sigtran empleando Wireshark (y/o tshark) y Snort.
- 👤 Esquema Nacional de Seguridad e ISO 27001, ¿Cómo implantar ambos en mi empresa?
- 👤 Seguridad en IMS (Internet Multimedia Subsystem).
- 👤 Seguridad informática empleando Raspberry Pi y Kali.
- 👤 Análisis de ataques/vulnerabilidades SS7/Sigtran empleando Wireshark (y/o tshark) y Snort.
- 👤 Fraude y medidas de Seguridad en transacciones a través de Servicios Digitales Financieros (DFS).
- 👤 Auditorías - test de Seguridad (OSSTMM)
- 👤 Seguridad en WiFi (Resumen Ejecutivo)
- 👤 Seguridad en WiFi (Técnico)
- 👤 Política de seguridad (rfc 1244)
- 👤 Ciclo de Ciberseguridad en 5G.

3. Algunos temarios de formación que hemos impartido.

Temario de curso: Concienciación en Ciberseguridad.

Duración: 24 horas.

Público: Personal no técnico de la empresa

Objetivo: Ofrecer una visión clara sobre los aspectos fundamentales a considerar para evitar incidentes de seguridad y mejorar el estado de la misma en mi organización.

Temario

1. De quién nos defendemos.
2. Cómo y por dónde suele iniciarse un incidente de seguridad.
3. Qué consideramos “malware”.
4. La ingeniería social.
5. ¿Por qué es importante el empleo de software legal?
- 6.Cuál es el riesgo a que nos exponemos.

7. Qué puedo y qué no puedo instalar en el ordenador de mi empresa.
8. Empleo del teléfono móvil en el trabajo.
9. Las redes Wifi de la empresa.
10. La importancia y clasificación de la información de mi empresa.
11. Procederes correctos e incorrectos.
12. Qué principios básicos JAMÁS debo dejar de lado.
13. El uso correcto de mis redes, Internet y del correo electrónico.
14. Las fugas de información.
15. El trabajo en la oficina y el trabajo en casa.
16. Dónde y cómo recurrir ante cualquier sospecha.
17. Derechos, responsabilidades y obligaciones.
18. El uso de los datos personales.
19. El teletrabajo.
20. Dónde y cómo recurrir ante cualquier sospecha.
21. Proceder ante un incidente ya ocurrido.

Temario del curso: Seguridad básica en Sistemas de Información.

Duración: 16 horas.

Público: Usuarios y administradores de SSII.

Objetivo: Presentar el estado actual de la cuestión en temas de seguridad orientado hacia entornos TCP/IP. Despertar conciencia en Seguridad, y medidas básicas a tener en cuenta.

Temario

1. La importancia de la transmisión digital
2. Inicios de TCP/IP
3. Protocolos de la familia TCP/IP
4. Analizadores de protocolos
5. Intranet, Extranet e Internet
6. Límites o fronteras de una red
7. Estrategias de Seguridad
8. Servicios de seguridad
9. Pasos a seguir en ataques a redes y sistemas TCP/IP
10. Metodología de ataques
11. Seguridad por niveles

12. Software o Hardware a emplear
13. Ejemplo de ataques reales
14. Aspecto de especial interés para este curso: *Estándar IEEE: 802.11*
15. Conclusiones

Temario de curso: Gerenciamiento de la seguridad.

Duración: 12 horas.

Público: Directivos, gerentes y administradores de sistemas.

Objetivo: Ofrecer una visión clara sobre los aspectos fundamentales a considerar para “Gestionar” la seguridad.

Temario

1. Importancia de la visión interna en la propia red.
 - a. Aspectos a considerar.
 - b. Conceptos a tener en cuenta.
 - c. Visión interna y externa de una red.
2. Metodología de análisis perimetral (Visión de frontera).
 - a. Conceptos de defensa en profundidad.
 - b. Clasificación de zonas de impacto (Acceso, servicios, almacenamiento).
 - c. Metodología de "Acción retardante".
 - d. Auditoría constante de Firewalls y Routers de frontera.
 - e. Cálculo y mantenimiento del Índice de seguridad.
3. Correlación de eventos (Visión Interna y de flujos):
 - a. Disparidad en la detección de un mismo evento por distintos productos (Disparidad y volumen de logs y eventos).
 - b. No cumplimiento a lo establecido por las RFCs.
 - c. Faltas de desarrollos en el relevamiento del software y hardware de red.
 - d. Faltas de iniciativas sobre trabajo en reglas “Proactivas”.
 - e. Empleo correcto de IDSs (o IPSs) y Honey Pots.
4. Metodología de trabajo:
 - a. Definición de objetivos.
 - b. Evaluación de índices y parámetros.
 - c. Definición de informes y reportes.
 - d. Organización, planificación y periodicidad del trabajo.
 - e. Documentación y normativas de seguimiento.

Temario del curso: Auditorías de Seguridad.

Duración: 24 horas.

Público: administradores de sistemas, responsable de empresa.

Objetivo: Proporcionar conocimientos sólidos para la realización de auditorías de seguridad, tanto internas como externas.

Temario

1. Introducción:

Penetration Test.

Diagnóstico o evaluación de Seguridad.

Auditoría de seguridad.

- Definición del alcance del proyecto.
- Penetration Test o evaluación Externo e Interno.
- Penetration Test vía Internet.
- Duración del proyecto.
- Objetivos del proyecto.

2. Pasos para realizar un Penetration Test o evaluación

Definición del alcance.

Definición de la metodología a utilizar.

Aplicación de la metodología.

Evaluación de los resultados obtenidos.

Corrección de los expuestos detectados.

3. Metodologías y Estándares en proyectos de Penetration Testing:

OSSTMM (Open Source Security Testing Methodology Manual.)

Metodología de Penetration Test o evaluación de Seguridad.:

- Descubrimiento.
- Exploración.
- Evaluación.
- Intrusión.

4. Fase de Descubrimiento

Recolección de información.

Descubriendo la red.

Fuentes de información en Internet.

Dirección física.
Detección de Redes WiFi.
Números telefónicos.
Nombres de personas y cuentas de correo electrónico.
Rango de direcciones IP.
Información de prensa sobre el lugar.
Análisis de las páginas Web Institucionales y/o Intranet Corporativa.
Evaluación del código fuente.

5. Fase de Exploración:

Scanning telefónico.
Detección de hosts activos.
Detección y Análisis de servicios activos
Detección remota de sistemas operativos.
Determinación de mecanismos de encriptación en redes Wi-Fi.
Relevamiento de aplicaciones Web.

6. Fase de Evaluación:

Detección de vulnerabilidades en forma remota.
Herramientas de detección de vulnerabilidades.
Testing de seguridad en Routers / Firewalls/ Dispositivos de Comunicaciones
Testing de seguridad de un servidor UNIX.
Testing de seguridad de un servidor Windows NT/2000.
Testing de seguridad de un servidor Novell.
Testing de eficacia de Sistemas de Detección de Intrusiones.
Testing de seguridad de una Base de Datos.
Testing de seguridad de aplicaciones Web.

7. Fase de Intrusión:

Planificación de la intrusión.
Utilización de ingeniería social para obtención de información.
Explotación de las vulnerabilidades detectadas.
Acceso vía módems o accesos remotos detectados.
Intrusiones vía web.
Escalada de privilegios.
Combinación de vulnerabilidades para elevar el control.
Acceso a información interna.
Generación de evidencia de expuestos detectados.

8. Evaluación y corrección:

- Evaluación de los resultados obtenidos.
- Determinación de niveles de riesgo.
- Propuesta de soluciones de seguridad.
- Corrección de las vulnerabilidades detectadas.

Temario del curso: Accionar en Internet y Cyberterrorismo.

Duración: 8 horas.

Público: Personal relacionado al control de la seguridad pública en Internet.

Objetivo: Realizar una primera aproximación hacia los conceptos a tener en cuenta, para la realización de un sistema defensivo proactivo contra el Cyberterrorismo.

Temario :

Internet:

1. Conceptos de amenazas / ataques.
2. Quién es el enemigo?
3. Algunos números relacionados a ataques .
4. Orígenes de los ataques.
5. Metodologías de ataques.
6. Mecanismos de seguridad.
7. Como se prepara el personal.

Cyberterrorismo:

1. Conceptos.
2. Metodología.
3. Objetivos potenciales.
4. Doctrina defensiva proactiva.
5. Plan de acción.