

Concienciación Estratégica en Ciberseguridad

Alejandro Corletti Estrada
(acorletti@darFe.es)

Hoy en día, toda empresa u organización tiene un altísimo grado de dependencia con sus redes y sistemas de TI.

El área de gobierno, seguramente conoce al detalle sus aspectos de producto, financieros, de negocio, de mercado, laborales, legales, etc.

Pero el **CEO** y su entorno, ¿Conoce el ciber riesgo al que se expone?

¿Es consciente del conjunto de medidas y acciones?

CEO

¿Cómo puede el CEO marcar la diferencia en materia de ciberseguridad?

La digitalización ha hecho que la ciberseguridad sea un asunto que interesa a todos, y ese cambio cultural empieza por el primer ejecutivo de la compañía.

Las grandes transformaciones son la forma más eficaz de potenciar la ciberseguridad dentro de las compañías y sólo el CEO es capaz de impulsarlas.

- El 51% de los CEO y de los miembros de la alta dirección exigen planes para la gestión de los ciberriesgos cuando se producen grandes cambios de negocio en las empresas.

Llamada a la acción:
Comunicar el compromiso del CEO con la ciberseguridad y utilizar su influencia para impulsar cambios profundos y eliminar las barreras que existen dentro de la empresa y que impiden alcanzar una buena coordinación con la alta dirección.

La unión de la alta dirección, clave en la protección contra los ciberataques

pwc

Principales conclusiones de la Digital Trust Survey 2023

Consejos de Administración

El Consejo de Administración, ¿está haciendo lo suficiente? ¿Cómo pueden sus integrantes gestionar mejor la ciberseguridad de la empresa?

Gartner
"Para 2026, el 70% de los consejos de administración incluirán un miembro con experiencia en ciberseguridad"

1 Sistema inmunitario digital

En 2025, las organizaciones que inviertan en conseguir inmunidad digital mejorarán la satisfacción del cliente, al reducir un 80 % el tiempo de inactividad.

Gartner

Las principales tendencias tecnológicas estratégicas para 2023

Discurso de apertura de la Cumbre de Seguridad y Gestión de Riesgos de Gartner **Richard Addiscott** (Sídney, 28/03/2023)

2023 Deloitte Global Future of Cyber Survey

Building long-term value by putting cyber at the heart of the business

91%
Organizations reporting at least one cyber incident or breach.

Las organizaciones de alta madurez tienen casi el triple de probabilidades que las de baja madurez, y casi el doble que las de madurez media, de contar con un **órgano de gobierno compuesto por altos directivos de la empresa y de TI** para supervisar sus programas cibernéticos (60% de alta frente a 36% de media y 22% de baja).

Por qué el CEO y su entorno deben conocer el negocio de ciberseguridad

dir&ge

Plataforma líder del entorno directivo



Inicio > Innovación > Implicación de los CEOs con la ciberseguridad: ¿Proactivos o reactivos?

INNOVACIÓN NOTICIAS

Implicación de los CEOs con la ciberseguridad:
¿Proactivos o reactivos?

20 de enero de 2022

pwc

Servicios Sectores Temas clave Quiénes somos Carrera profesional

¿Puede el CEO marcar la diferencia
en la gestión de la ciberseguridad?

Haz de la seguridad tu mantra empresarial



EXPANSION

OPINIÓN
**Ciberseguridad: la
importancia del
CEO en la estrategia**

Las organizaciones deberán tener estrategias efectivas que les permitan ser preventivas y no esperar el ataque para defenderse, señalan Fernando Román y Juan Carlos Carrillo.

- Porque del mismo depende su supervivencia.
- Porque el “compromiso de la dirección” es un parámetro de certificación ISO 27001.
- Porque es el máximo responsable de la “política de Ciberseguridad” de su empresa/organización.
- Porque debe comprender, y ser consciente de los riesgos a los que se expone.
- Para “conducir” adecuadamente al área de Gobierno de la Ciberseguridad.
- Para aportar en la estrategia de Ciberseguridad de su empresa/organización.
- Porque será el máximo responsable ante incidentes (*interno y ante las autoridades y medios de difusión*).
- Porque es justamente el nivel que **NO** puede cometer fallos de Ciberseguridad (*si los comente son críticos*).
- Por el valor de la “privacidad” de los datos personales que maneja.
- Porque tiene acceso a la información de más alto nivel, impacto y criticidad.

telcel

empresas

Menú ▾

EMPRESAS / Tendencias / Notas / CEO y la ciberseguridad

Las 5 cosas que cualquier
CEO debe dominar
acerca de Ciberseguridad

kaspersky daily

My Kaspersky ▾

5 lecciones de ciberseguridad para tu CEO

Las medidas de seguridad de la información son más eficaces cuando reciben el apoyo de la alta directiva. ¿Cómo puedes conseguirlo?



Propuesta de un temario a desarrollar para CEOs y entorno

1. Cómo es esta gran red mundial (*cables submarinos, satélites, red fija y móvil*).
2. Cómo viaja nuestra información.
3. Los grandes carrier de Internet (sus sistemas autónomos).
4. Nuestras propias arquitecturas de red y sistemas de TI (Defensa en profundidad y en altura).
5. Conceptos importantes de Sistemas y Telecomunicaciones que deben ser comprendidos.
6. Conceptos de “red país” (vías de aproximación y vectores de ataque).
7. De quién nos defendemos.
8. Incidentes de ciberseguridad y gestión de los mismos (qué son, clasificación, tipos y casos recientes).
9. Impactos generados por incidentes de ciberseguridad.
10. El análisis de Riesgo de ciberseguridad.
11. Tipos de riesgo, impacto, mitigación y seguimiento.
12. El Ciclo de vida de la ciberseguridad.
13. La familia ISO/UNE 27000 (Sistema de Gestión de la Seguridad de la Información).
14. Política de Seguridad y Plan Director de Ciberseguridad.
15. La organización del área de Ciberseguridad (Gobierno, Planificación y Operación de la Ciberseguridad)
16. Qué son y para qué sirven el NOC (Network Operation Center) y SOC (Security O.C.).
17. Servicios Digitales Financieros (FinTech), nuestros pagos, transacciones y validaciones por la red.
18. Mejores prácticas en Ciberseguridad empresarial.

Aspectos de detalle de esta capacitación

Público al que va dirigido: Personal directivo y gerencial de la empresa/organización.

Objetivos:

- 👤 Preparar al alto nivel de la empresa/organización para el “Gobierno de Ciberseguridad”.
- 👤 Despertar consciencia sobre la importancia que tiene el compromiso de la Dirección sobre la Ciberseguridad.
- 👤 Ofrecer los conocimientos firmes para la toma de decisiones y la conducción concreta y adecuada de esta área.
- 👤 Consolidar un equipo de trabajo específico para la gestión del riesgo y las crisis en incidentes de ciberseguridad.

Metodología: Este plan de capacitación, ha sido impartida bajo tres formas:

- 👤 Presencial.
- 👤 Semipresencial.
- 👤 On-line.

Nuestra experiencia a lo largo de las decenas de veces que lo hemos impartido, nos permite afirmar que la mejor forma es “Semipresencial”, desarrollando el temario inicial “in situ” y luego retomar el tema en 3 o 4 clases “On-line” vía Zoom.

Duración: De acuerdo al nivel de profundidad/detalle deseado, este plan puede desarrollarse entre 3 y 12 horas.

Recursos: Para la realización de la capacitación DarFe aporta el 100% del material (Plataforma de formación On-Line (<https://moodle.darfe.es>), documentación en formato PDF, videos y enlaces a contenidos).





Precio: Se define, sobre la base de su duración, sitio, medios y participantes.

Material de apoyo de DarFe

DarFe es la única empresa del mundo hispano que sustenta la totalidad de sus cursos y capacitaciones en el **100% de su propio Know How**.

Para ello, ofrece de forma permanente en Internet y de forma gratuita los siguientes recursos:

Cuatro libros:

-  Seguridad por niveles
-  Seguridad en Redes
-  Ciberseguridad, una estrategia Informático/Militar
-  Manual de la Resiliencia



Curso gratuito de “Técnico en Ciberseguridad”



Más de cien videos disponibles en nuestro canal Youtube (DarFe)



Ciclo “Aprendiendo Ciberseguridad paso a paso”



Ciclo sobre Ciberdefensa



Ciclo Webinar sobre Ciberseguridad en 5G



Ciberdefensa: nuevos conceptos, nuevas metodologías, nuevos desafíos



Ciberseguridad: empleo de SOC y NOC



Ciberseguridad: Como son las entrañas de esta gran red mundial



Ciberseguridad: La importancia de los procesos

- Ciberseguridad:**
- Sea aplicable e implementable.
 - Se mantengan vigentes.
 - Se audite su correcto cumplimiento.
- Específicamente, estos ocho son los procesos que cobran una importancia básica en Ciberseguridad desde nuestro punto de vista:
- En la entrada de la imagen se indica: **La importancia de los procesos**
- Gestión de cambios.
 - Gestión de accesos.
 - Configuración de sistemas e infraestructura.
 - Gestión de Backup.
 - Gestión de Incidencias.
 - Supervisión y Monitorización.
 - Gestión de Logs.

Ciberdefensa en profundidad y en altura



Gobierno de la Ciberseguridad y estrategias Resilientes

"Gobierno de la Ciberseguridad y estrategias resilientes"

México, agosto de 2021



Alejandro Corletti Estrada
(acorletti@darFe.es - acorletti@hotmail.com)
www.darFe.es

Estrategia de Ciberseguridad en Grandes Redes



Seguridad en IMS (Internet Multimedia Subsystem)



Fraude y medidas de Seguridad en transacciones a través de Servicios Digitales Financieros (DFS)

10 Reglas de Fortificación de Redes

Fraude y medidas de Seguridad en transacciones a través de Servicios Digitales Financieros (DFS)

Presentación del tema

Nos encontramos ante un nuevo paradigma o nicho de mercado donde, los tradicionales servicios financieros, están migrando hacia servicios dispendiosos con por ciento de las Telecomunicaciones.

Las autoridades y grandes holding financieros están empujando fuertemente a la sociedad y empresas a hacer uso de ellos, para los cuales en todo sentido. El crecimiento de estos Servicios Digitales Financieros en empresas, como, El Usabio, la Banca y los Siglo XXI, requiere y exige **SEGURIDAD** y la masa de la responsabilidad sobre estos temas la tienen los **FinTech**.

En este texto, se trata de resumir el problema y sus potenciales soluciones a través del siguiente temario:

1. FinTech.
2. Dar forma al futuro de los servicios financieros en la economía digital.
3. ¿Qué son los Servicios Financieros Digitales? (DFS: Digital Financial Services).
4. ¿Por qué nos interesa todo lo desarrollado anteriormente?
5. El problema concreto de la seguridad y su evolución hacia entornos seguros.
6. Modelos Prácticos.
7. Conclusiones finales.

Cientos de artículos disponibles en formato “PDF” en nuestra sección “Descargas”

- Algunos conceptos de criptografía
- Auditoría Forense
- Auditorías de Seguridad (parte técnica)
- Conceptos de Redes
- Curso de análisis de tráfico
- El Modelo OSI
- IPv6 (parte 1) - Los componentes

- IPv6 (Parte 2) - Las direcciones
- IPv6 (Parte 3) - El encabezado
- En seguridad hay que Hacer y saber vender (la Biografía de Van Gogh)
- Esquema Nacional de Seguridad e ISO 27001 ¿Cómo implantar ambos en mi empresa?
- Esquema Nacional de Seguridad, se lanzó la “cuenta atrás”
- Estructura y metodología de la codificación de la información
- Instalación de Kali en VirtualBox (paso a paso)
- La Interfaz Digital Estándar
- La red telefónica conmutada
- Matriz de estado de Seguridad
- Medios de Comunicaciones
- Metodología Nessus - Snort
- Modulación
- Nivel de inmadurez de los NIDS
- Plan Director de Seguridad (una visión: práctica, eficiente y estándar)
- Política de Seguridad
- Protocolo IPSEC (isakmp)
- Resiliencia Cibernética (tesis) My. Mariano Gómez
- Seguridad empleando Kali y Raspberry PI

-
- Seguridad en 5G (¿estamos mejor o peor que antes?) Ponencia en OpenExpo2021
 - Seguridad en el protocolo SNMPv3
 - Seguridad en IMS
 - Seguridad en SS7 empleando Wireshark y Snort en español
 - Seguridad WiFi (Parte técnica)
 - Seguridad WiFi (resumen ejecutivo)
 - SS7 Security - Wireshark & Snort (EN)
 - Técnicas de transmisión de información
 - ...