

CONTENIDO

11 INTRODUCCIÓN

sección 1

ENTENDER LA INSEGURIDAD:

CONCEPTOS Y GUÍAS

- 13 Función y propósito de la seguridad de la información
- 15 Seguridad de la información: Una estrategia de aprendizaje
- 17 Arquitectura de seguridad de la información: Una lección pendiente para los CISO
- 21 Cultura de seguridad de la información: Entender una percepción
- 23 Métricas en seguridad de la información: Un reto permanente
- 26 Reflexiones sobre las métricas en seguridad de la información
- 28 Expectativas y motivaciones de la función de seguridad de la información
- 30 Inversión en seguridad de la información: Volver a los principios
- 33 Signos y señales: Pérdida y/o fuga de la información
- 36 Confusión de fines y perfección de medios
- 38 Inseguridad tercerizada: Un reto de confianza, acuerdos y riesgos
- 40 Inseguridad de la información: Gerencia en movimiento
- 42 Descubrimiento electrónico: Evidencia digital y retos empresariales
- 44 Ciclo de vida del descubrimiento electrónico en la empresa

- 47 Retos emergentes para el descubrimiento electrónico
- 49 Análisis forense digital en la nube: Reto de la inseguridad en un ecosistema tecnológico
- 53 ¿Bases de datos inseguras? Algunas reflexiones básicas
- 56 Peritos informáticos: Testigos de la inseguridad en la información

sección 2

REFLEXIONES ESTRATÉGICAS

PARA LA ALTA GERENCIA

- 63 Seguridad de la información: Tres conceptos distintos y un solo responsable verdadero
- 69 Privacidad de los datos: Más que un aspecto de cumplimiento
- 74 Postura individual de seguridad de la información: Un hábito requerido para sobrevivir a la inevitabilidad de la falla
- 78 El debido cuidado en seguridad de la información: Un ejercicio de virtudes
- 82 Innovación, cambio y estrategia: Tres claves para potenciar la función de seguridad de la información
- 84 Compartir o proteger: Tensiones en la gerencia de seguridad de la información
- 89 Facilitar la madurez de la función de seguridad: Algunos arquetipos propuestos

- 91 Doce recomendaciones para configurar su estrategia de seguridad de la información
- 93 Integrar la seguridad de la información en la estrategia empresarial: Una reflexión sociotécnica para enfrentar la inseguridad
- 98 Maestra en la ciencia de la protección de la información
- 101 Inseguridad de la información: Fuente de la innovación en seguridad
- 104 Inseguridad de la información: Asegurar el 99,9% y sobrevivir al 0,1%
- 110 Lo estratégico de la inseguridad informática
- 111 Fraude y fuga de información: Inseguridad en dos sectores críticos
- 113 Fugas de información: Revelar la inseguridad en el factor humano
- 116 La inseguridad de la información y las juntas directivas: ¿Déficit de atención?
- 121 Pensar como el atacante: Mente y corazón de la inseguridad de la información
- 124 Focalizar la articulación de valor más que el retorno de la inversión
- 126 Amenazas persistentes avanzadas: La inseguridad de la información como fuente de inteligencia estratégica para los intrusos

sección 3

TEMAS EMERGENTES: EN LA NUBE, REDES SOCIALES, CIBERSEGURIDAD. RETOS Y PRONÓSTICOS

- 131 Inseguridad en la nube: Retos y riesgos
- 136 Inseguridad en redes sociales: La inevitabilidad de la falla en nuestros comportamientos y valores
- 139 Fraude a través de medios tecnológicos: Más que predicciones, algunos pronósticos sobre su evolución
- 146 Ciberseguridad y ciberdefensa: Dos conceptos emergentes en la gobernabilidad de una nación
- 150 Cibercrimen: Evolución y desafíos en una sociedad digital
- 154 Nuevas posibilidades para el cibercrimen: Desafíos a un ecosistema tecnológico
- 156 Cultura de ciberseguridad: Un estándar de comportamiento colectivo
- 158 Lecciones aprendidas: Más que pecados de obra u omisión
- 162 Inseguridad de la información: Retos de “espacios en blanco” y lecciones de “cisnes negros”
- 165 Evolución de los pronósticos en seguridad de la información 2010-2012
- 174 Inseguridad informática: Lecciones aprendidas y exploración del futuro

177 REFERENCIAS BIBLIOGRÁFICAS

187 ÍNDICE ANALÍTICO