ÍNDICE

3.1.3.4. Validez y gestión documental

3.1.3.5. Formulario por cada acción correctiva

3.1.3.5.1. Ejemplo de formulario de acción correctiva

3.2. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

3.2.1. La Función de la Auditoría en los Sistemas de información. Conceptos básicos. Estándares y Directrices de Auditoría de SI.

3.2.1.1. Introducción

3.2.1.2. La Auditoría

3.2.1.3. Carácter interdisciplinar de la auditoría informática

3.2.1.4. Objetivos

3.2.1.5. Pasos para realizar una auditoría informática

3.2.1.6. Controles

3.2.1.7. Conclusiones

3.2.1.8. Anexo 1. Estándares

3.2.1.8.1. Ejemplos de diferentes metodologías

3.2.2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoría de protección de datos en la auditoría de SI

3.2.2.1. Introducción

3.2.2.2. Importancia del ciclo de mejora continua

3.2.2.3. El ciclo de gestión

3.2.2.4. Correspondencia entre el sistema de control interno y las fases del modelo PDCA

3.2.2.4.1. Fase 1. Plan (Planificar)

3.2.2.4.2. Fase 2. Do (Hacer)

3.2.2.4.3. Fase 3. Check (Verificar)

3.2.2.4.4. Fase 4. Act (Actuar)

3.2.2.4.5. Ciclos sucesivos

3.2.2.5. La monitorización continua del control

3.2.2.5.1. Selección de controles

3.2.2.5.2. Diseño de reglas de supervisión automáticas

3.2.3. Planificación, ejecución y seguimiento

3.2.3.1. Metodología de una auditoría de sistemas

3.2.3.1.1. Definición y alcance de los objetivos

3.2.3.1.2. Estudio inicial del entorno

3.2.3.1.3. Asignación de recursos necesarios

3.2.3.1.4. Ejecución de las tareas propias de la auditoría

3.2.3.1.5. Elaboración del informe

3.2.3.2. Objetivos habituales de una auditoría de sistemas

3.2.3.2.1. Análisis de vulnerabilidades

3.2.3.2.2. Resolución de las vulnerabilidades

3.2.3.2.3. Planificación de respuesta de incidentes

3.2.3.2.4. La seguridad como proceso continuo

3.3. LA GESTIÓN DE LA SEGURIDAD DE LOS TRATAMIENTOS

3.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI)

3.3.1.1. Esquema Nacional de Seguridad

3.3.1.2. Objetivos del ENS

3.3.1.3. Contenido del ENS

3.3.1.4. Herramientas del ENS

3.3.1.5. Sistema de gestión de seguridad de la información

3.3.1.6. Objetivos y beneficios de un SGSI

3.3.1.7. Plan de implantación del SGSI

3.3.1.8. Requisitos y factores de éxito del SGSI

3.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación

3.3.2.1. Introducción

3.3.2.2. Clasificación de las medidas de seguridad lógicas

3.3.2.3. Algunos ejemplos de medidas y procedimientos de seguridad

3.3.2.4. Control de Acceso

3.3.2.4.1. La gestión de Identidades (IAM)

3.3.2.5. Conclusiones

3.3.3. Recuperación de desastres y continuidad del negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación de Desastres

3.3.3.1. Introducción

3.3.3.2. Objetivos

3.3.3.3. Implementación y mantenimiento-ISO22301

3.3.3.4. Contenido de la ISO-22301

3.4. OTROS CONOCIMIENTOS

3.4.1. El Cloud Computing

3.4.1.1. Definición

3.4.1.2. Ventajas e inconvenientes

3.4.1.3. Tipos de nube

3.4.1.3.1. Nube pública

3.4.1.3.2. Nube privada

3.4.1.3.3. Nube híbrida

3.4.1.4. Modalidades de servicio

3.4.1.5. Legislación y elementos del contrato

3.4.1.6. Cloud Computing y protección de datos

3.4.1.7. Situaciones frecuentes

3.4.1.7.1. Transferencias internacionales

3.4.1.7.2. Calidad de los servicios Cloud

3.4.2. Los Smartphones y la protección de datos

3.4.2.1. Introducción

3.4.2.2. Evolución de los terminales móviles

3.4.2.3. La protección de datos en los Smartphones

3.4.2.4. Riesgos relativos a la protección de datos en nuestros Smartphones

3.4.2.5. Medidas de seguridad aplicables

3.4.3. Internet de las cosas (IoT)

3.4.3.1. Introducción

3.4.3.2. Legislación vigente

3.4.3.3. Monitorización y Perfilado

3.4.3.4. RGPD e IoT

3.4.4. Big Data y elaboración de perfiles

3.4.4.1. Definición

3.4.4.1.1. Ventajas, inconvenientes y características

3.4.4.1.2. Legislación y elementos del contrato

3.4.5. Redes sociales

3.4.5.1. Introducción

3.4.5.2. Protección de datos en las Redes Sociales

3.4.6. Tecnologías de seguimiento de usuario

3.4.6.1. Introducción

3.4.6.2. Las tecnologías de seguimiento

3.4.6.3. Requisitos y procedimientos

3.4.7. Blockchain y últimas tecnologías

3.4.7.1. Introducción

3.4.7.2. Qué es el Blockchain, funcionamiento y ventajas

3.4.7.3. El Blockchain vs el RGPD

ANEXO

01. Cloud Computing: retos y Oportunidades. ONTSI

02. Opinion 05/2012 on Cloud Computing. Grupo de Trabajo del Artículo 29.

Directiva 95/46/CE

03. Opinion 2/2015 on C-SIG Code Of Conduct on Cloud Computing

04. Guidelines of the use of cloud computing service by de European instituons and bodies

05. Los dispositivos móviles

06. Dispositivos móviles personales para uso profesional (BYOD). Una guía de aproximación para el empresario. INCIBE

07. El Instituto Nacional de Ciberseguridad recuerda que los dispositivos móviles también están en el punto de mira de los ciberdelincuentes. INCIBE

08. Guía para proteger y usar de forma segura su móvil. INTECO

09. “Del Internet de las cosas al Internet de los cuerpos”. Javier Puyol. Confilegal

10. Opinion 8/2014 on the on Recent Developments on the Internet of Things. Grupo de Trabajo del Artículo 29 Directiva 95/46/CE

11. CCN-CERT BP/05. Internet de las cosas

12. Si usas Big Data que sea respetando la privacidad de tus clientes. INCIBE

13. Minería de datos, Big Data y Seguridad. INCIBE

14. Thinking in Big (Data) y la seguridad industrial. INCIBE

15. WP 251 Guidelines on Automated individual decisión-making and Profiling for the purposes of Regulation 2016/679

16. Riesgos de la utilización de redes sociales en la organización. INCIBE

17. Ciberseguridad y la identidad online de tu empresa. INCIBE

18. Web tracking e identificación de usuarios en Internet. INCIBE

19. Construyendo comunicaciones seguras. Blockchain en la industria 4.0. INCIBE

20. ¿Protege blockchain mi información personal?. Jesús Díaz Vico. INCIBE

21. ¿Qué son los “smart contracts”: cinco preguntas clave. BBVA

22. Guía sobre el uso de las Cookies aepd