CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

GASIC N° 15- Versión 0.1 - 2025

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N° 15

DICCIONARIO DE TÉRMINOS Y CONCEPTOS SOBRE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno, el Consejo de Auditoría Interna General de Gobierno (CAIGG), en su calidad de entidad asesora del Supremo Gobierno en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza, presenta a la Red de Auditoría Gubernamental la GASIC N° 15: Diccionario de Términos y Conceptos sobre Seguridad de la Información y Ciberseguridad.

Esta guía forma parte de una iniciativa del CAIGG orientada a fortalecer las competencias de la función de auditoría interna del sector público en materia de Seguridad de la Información y Ciberseguridad. Su propósito es proporcionar a los Auditores Internos y a los Servicios Públicos herramientas e instrumentos técnicos que les permitan analizar y evaluar los sistemas de información conforme a las mejores prácticas internacionales y a la legislación vigente.

Santiago, noviembre de 2025.

Daniella Caldana Fulss

Auditora General de Gobierno

INTRODUCCIÓN

En un entorno cada vez más digitalizado, donde los riesgos asociados a la Seguridad de la Información y la Ciberseguridad son cada vez más complejos y frecuentes, el fortalecimiento de las capacidades institucionales para enfrentarlos se ha convertido en una prioridad estratégica para el Estado. En este contexto, el Consejo de Auditoría Interna General de Gobierno (CAIGG) ha impulsado una serie de herramientas técnicas orientadas a robustecer la función de auditoría interna en el sector público.

La GASIC N° 15: Diccionario de Términos y Conceptos sobre Seguridad de la Información y Ciberseguridad se enmarca en esta estrategia y constituye un instrumento fundamental para homogeneizar el lenguaje técnico, fortalecer la comprensión especializada y facilitar la evaluación y auditoría de riesgos tecnológicos emergentes en las instituciones públicas. Este documento entrega definiciones relevantes que permiten alinear criterios y enfoques entre los distintos actores responsables de auditar, gestionar y supervisar la seguridad de los activos de información del Estado.

Esta guía es complementaria a las demás GASIC desarrolladas por el CAIGG, que abordan temáticas específicas como gobernanza, seguridad en redes, gestión de accesos, continuidad del negocio, computación en la nube, desarrollo seguro y otros aspectos clave del ecosistema digital.

Así, la GASIC N° 15 aporta valor no solo como diccionario técnico en materia de sistemas de información, sino también como pieza integradora de un marco de fortalecimiento institucional más amplio, alineado con los principios de gobernanza, transparencia y responsabilidad pública que rigen la Administración del Estado.

— A —

1. ACK piggybacking:

El ACK piggybacking es la práctica de enviar un ACK dentro de otro paquete que va al mismo destino. *(Fuente: SANS:)*

2. ACL Reflexivas (Cisco):

Las ACL reflexivas para routers Cisco son un paso para hacer que el router funcione como un firewall con estado. El router tomará decisiones de filtrado basándose en si las conexiones son parte del tráfico ya establecido o no. *(Fuente: SANS:)*

3. ACLs Estándar (Cisco):

Las ACLs estándar en routers Cisco toman decisiones de filtrado de paquetes basándose solo en la dirección IP de origen. *(Fuente: SANS:)*

4. ACLs Extendidas (Cisco):

Las ACLs extendidas son una forma más poderosa de las ACLs estándar en routers Cisco. Pueden tomar decisiones de filtrado basadas en direcciones IP (origen o destino), puertos (origen o destino), protocolos, y si una sesión está establecida. *(Fuente: SANS:)*

5. AIaaS:

un servicio en la nube que ofrece subcontratación de inteligencia artificial (IA) *(Fuente: NICSS:)*

6. ARPANET:

Red de la Agencia de Proyectos de Investigación Avanzada, una red pionera de conmutación por paquetes construida a inicios de los años 70 por contrato con el Gobierno de EE. UU., que condujo al desarrollo de Internet y fue desmantelada en junio de 1990. *(Fuente: SANS:)*

7. Acceso:

La capacidad y los medios para comunicarse o interactuar con un sistema, usar recursos del sistema para manejar información, obtener conocimiento de la información contenida o controlar componentes y funciones del sistema. *(Fuente: NICSS:)*

8. Acceso no autorizado:

Cualquier acceso que viole la política de seguridad establecida. *(Fuente: NICSS:)*

9. Acción Correctiva:

Acción para eliminar la causa de una no conformidad y evitar que vuelva a ocurrir. *(Fuente: ISO 22.300:)*

Acción para eliminar la causa de una no conformidad y prevenir que vuelva a ocurrir. *(Fuente: ISO 27.000:)*

10. Acción Preventiva:

Acción realizada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable. *(Fuente: ISO 22.300:)*

11. Aceptación Del Riesgo:

Decisión informada en favor de tomar un riesgo particular. *(Fuente: ISO 27.000:)*

Decisión informada en favor de tomar un riesgo particular. *(Fuente: ISO 22.300:)*

12. Activación:

Acto de declarar que las medidas de continuidad del negocio de una organización se tienen que aplicar para poder continuar la entrega/prestación de productos o servicios clave. *(Fuente: ISO 22.300:)*

13. Actividad:

Proceso o conjunto de procesos llevados a cabo por una organización (o en su nombre) que producen o ayudan a producir uno o más productos o servicios. *(Fuente: ISO 22.300:)*

<gestión de proyectos> El menor objeto de trabajo identificado en un proyecto. *(Fuente: ISO 9.000:)*

14. Actividad Prioritaria:

Actividad a la que se ha dado prioridad a raíz de un incidente para mitigar los impactos. *(Fuente: ISO 22.300:)*

15. Activo:

Cualquier cosa útil que contribuya al éxito de algo, como una misión organizacional; los activos son cosas valiosas o propiedades a las que se les puede asignar valor. *(Fuente: NICSS:)*

Cualquier cosa que tenga valor para una organización. *(Fuente: ISO 22.300:)*

16. Acuerdo De Ayuda Mutua:

Acuerdo preestablecido entre dos o más entidades para prestarse asistencia entre sí. *(Fuente: ISO 22.300:)*

17. Adiestramiento:

Actividad con la que se practica una habilidad concreta y que con frecuencia implica repetir varias veces la misma cosa. *(Fuente: ISO 22.300:)*

18. Administración De Las Evidencias Electrónicas:

Proceso de generación, almacenamiento, transmisión, recuperación (extracción y exportación), tratamiento (consolidación, agregación, correlación) y comunicación de las evidencias electrónicas. *(Fuente: UNE 71.505:)*

19. Administración de datos:

En el marco NICE, trabajo de ciberseguridad donde una persona: desarrolla y administra bases de datos y/o sistemas de gestión de datos que permiten el almacenamiento, consulta y utilización de datos. *(Fuente: NICSS:)*

20. Administración de sistemas:

En el marco NICE, trabajo en ciberseguridad donde una persona: instala, configura, soluciona problemas y mantiene configuraciones de servidores (hardware y software) para garantizar su confidencialidad, integridad y disponibilidad; también gestiona cuentas, firewalls y parches responsables del control de acceso, contraseñas y creación y administración de cuentas. *(Fuente: NICSS:)*

21. Adquisición De Competencia:

Proceso para alcanzar competencia. *(Fuente: ISO 9.000:)*

22. Adversario:

Una persona, grupo, organización o gobierno que realiza o tiene la intención de realizar actividades perjudiciales. *(Fuente: NICSS:)*

23. Agente de amenaza:

Un individuo, grupo, organización o gobierno que realiza o tiene la intención de realizar actividades dañinas. *(Fuente: NICSS:)*

24. Agotamiento de recursos:

Los ataques de agotamiento de recursos implican ocupar recursos finitos en un sistema, haciéndolos indisponibles para otros. *(Fuente: SANS:)*

25. Agregación de Datos:

La agregación de datos es la capacidad de obtener una imagen más completa de la información al analizar varios tipos diferentes de registros a la vez. *(Fuente: SANS:)*

26. Agregación de datos:

La nueva información es más sensible que los elementos de datos individuales por sí solos, y la persona que agrega los datos no tenía autorización para acceder a la totalidad de la información. *(Fuente: NICSS:)*

27. Aguas Abajo:

Manipulación, procesado y movimiento de bienes cuando estos ya no se encuentran bajo la custodia de la organización en la cadena de suministro. *(Fuente: ISO 22.300:)*

28. Aguas Arriba:

Manipulación, procesado y movimiento de bienes que tiene lugar antes de que la organización en la cadena de suministro se haga cargo de la custodia de los bienes. *(Fuente: ISO 22.300:)*

29. Alcance De La Auditoría:

Extensión y límites de una auditoría. *(Fuente: ISO 27.000:)*

Extensión y límites de una auditoría. *(Fuente: ISO 9.000:)*

30. Alcance Del Ejercicio:

Magnitud, recursos y dimensión que reflejan las necesidades y los objetivos. *(Fuente: ISO 22.300:)*

31. Alcance Del Servicio:

Función o funciones que desempeña una organización en la cadena de suministro y dónde las desempeña. *(Fuente: ISO 22.300:)*

32. Alerta:

Parte de un aviso al público que capta la atención de los primeros intervinientes y personas en riesgo en una situación de emergencia en evolución. *(Fuente: ISO 22.300:)*

Una notificación de que se ha detectado un ataque específico o que este ha sido dirigido contra los sistemas de información de una organización. *(Fuente: NICSS:)*

33. Algoritmo:

Un conjunto finito de instrucciones paso a paso para un procedimiento de resolución de problemas o de cómputo, especialmente uno que puede ser implementado por una computadora. *(Fuente: SANS:)*

34. Algoritmo criptográfico:

Procedimiento computacional bien definido que toma entradas variables, incluida una clave criptográfica, y produce una salida. *(Fuente: NICSS:)*

35. Algoritmo de Retroceso Exponencial:

Un algoritmo de retroceso exponencial se usa para ajustar los valores de timeout TCP dinámicamente para que los dispositivos de red no sigan agotando el tiempo de espera al enviar datos sobre enlaces saturados. *(Fuente: SANS:)*

36. Algoritmo de firma digital (DSA):

Un algoritmo criptográfico asimétrico que produce una firma digital en forma de un par de números grandes. La firma se calcula utilizando reglas y parámetros que permiten verificar la identidad del firmante y la integridad de los datos firmados. *(Fuente: SANS:)*

37. Algoritmo o Hash Criptográfico:

Un algoritmo que emplea la ciencia de la criptografía, incluyendo algoritmos de cifrado, algoritmos hash criptográficos, algoritmos de firma digital y algoritmos de acuerdo de clave. *(Fuente: SANS:)*

38. Alianza:

Asociarse con otros en una actividad o área de interés común para alcanzar unos objetivos individuales y colectivos. *(Fuente: ISO 22.300:)*

39. Almacenamiento de datos:

El almacenamiento de datos es la consolidación de varias bases de datos previamente independientes en una sola ubicación. *(Fuente: SANS:)*

40. Almacenamiento y Reenvío:

Almacenamiento y reenvío es un método de conmutación donde un switch lee el paquete completo para determinar si está intacto antes de reenviarlo. *(Fuente: SANS:)*

41. Almacenes de claves:

Repositorios que contienen artefactos criptográficos como certificados y claves privadas que se usan para protocolos criptográficos como TLS. *(Fuente: NICSS:)*

42. Alta Dirección:

Persona o grupo de personas que dirigen y controlan una organización al más alto nivel. *(Fuente: ISO 27.000:)*

Persona o grupo de personas que dirige y controla una organización al más alto nivel. *(Fuente: ISO 22.300:)*

43. Ambiente De Trabajo:

Conjunto de condiciones bajo las cuales se realiza el trabajo. *(Fuente: ISO 22.300:)*

44. Amenaza:

Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. *(Fuente: ISO 27.000:)*

Potencial de violación de la seguridad, que existe cuando hay una circunstancia, capacidad, acción o evento que podría vulnerar la seguridad y causar daño. *(Fuente: SANS:)*

Incluye a un individuo o grupo de individuos, entidad como una organización o una nación, acción o suceso. *(Fuente: NICSS:)*

Causa potencial de un incidente indeseado, que puede provocar un daño a personas, activos, un sistema o una organización, el medio ambiente o la comunidad. *(Fuente: ISO 22.300:)*

45. Amenaza en la cadena de suministro TIC:

Una amenaza provocada por humanos mediante la explotación de la cadena de suministro del sistema de tecnologías de la información y comunicación, incluidos los procesos de adquisición. *(Fuente: NICSS:)*

46. Amenaza externa:

Una persona o grupo de personas externas a una organización que no están autorizadas para acceder a sus activos y representan un riesgo potencial para la organización y sus activos. *(Fuente: NICSS:)*

47. Amenaza interna:

Una o más personas con acceso y/o conocimiento interno de una empresa, organización o entidad que les permita explotar las vulnerabilidades de la seguridad, sistemas, servicios, productos o instalaciones de esa entidad con la intención de causar daño. *(Fuente: NICSS:)*

48. Amenaza persistente avanzada:

Un adversario con altos niveles de experiencia y recursos significativos, capaz de crear oportunidades para alcanzar sus objetivos usando múltiples vectores de ataque (por ejemplo, cibernético, físico y engaño). *(Fuente: NICSS:)*

49. Amenazas cibernéticas:

Una amenaza cibernética es algo que puede o no suceder, pero que tiene el potencial de causar daños graves. Las amenazas cibernéticas pueden dar lugar a ataques a sistemas informáticos, redes y más. *(Fuente: NICSS:)*

50. Analizar:

Categoría del marco NICE que abarca áreas especializadas encargadas de revisar y evaluar información entrante de ciberseguridad para determinar su utilidad para inteligencia. *(Fuente: NICSS:)*

51. Ancho de banda:

Comúnmente se usa para referirse a la capacidad de un canal de comunicación para transmitir datos a través del canal en un período de tiempo determinado. Usualmente se expresa en bits por segundo. *(Fuente: SANS:)*

52. Anonimadores:

Un proxy anónimo es una herramienta que intenta hacer que la actividad en Internet no se pueda rastrear. *(Fuente: NICSS:)*

53. Anti-CSRF:

pares de tokens relacionados entregados a los usuarios para validar sus solicitudes y evitar que los atacantes emitan solicitudes a través de la víctima. *(Fuente: NICSS:)*

54. Anti-suplantación:

En un ataque de suplantación, la dirección de origen de un paquete entrante se modifica para que parezca provenir de una fuente confiable. Se usa para ataques DoS, explotar vulnerabilidades y acceder sin autorización. *(Fuente: NICSS:)*

55. Análisis De Criticidad:

Proceso diseñado para identificar y valorar sistemáticamente los activos de una organización sobre la base de la importancia de su misión o función, el grupo de personas en riesgo o la trascendencia de un evento indeseable o una disrupción sobre su capacidad para cumplir las previsiones. *(Fuente: ISO 22.300:)*

56. Análisis De Impacto; Análisis De Consecuencias:

Proceso de análisis de todas las funciones operativas y el efecto que una interrupción de las operaciones puede tener sobre ellas. *(Fuente: ISO 22.300:)*

57. Análisis De La Amenaza:

Proceso para identificar, cualificar y cuantificar la causa potencial de un evento indeseado, que puede provocar un daño a personas, activos, un sistema o una organización, el medio ambiente o la comunidad. *(Fuente: ISO 22.300:)*

58. Análisis De Riesgos De Derechos Humanos:

Proceso para identificar, analizar, valorar y documentar los riesgos relativos a los derechos humanos y sus impactos, con el fin de gestionar el riesgo y mitigar o evitar impactos negativos en los derechos humanos e infracciones legales. *(Fuente: ISO 22.300:)*

59. Análisis Del Impacto Sobre El Negocio:

Proceso de análisis de las actividades y el efecto que la disrupción del negocio puede tener sobre ellas. *(Fuente: ISO 22.300:)*

60. Análisis Del Riesgo:

Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. *(Fuente: ISO 27.000:)*

Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. *(Fuente: ISO 22.300:)*

61. Análisis Forense:

Metodología científica que permite autenticar bienes materiales mediante la confirmación de un elemento de autenticación o un atributo intrínseco con el uso de equipos especializados por parte de un experto cualificado con conocimientos específicos. *(Fuente: ISO 22.300:)*

62. Análisis costo-beneficio:

Un análisis costo-beneficio compara el costo de implementar contramedidas con el valor de la reducción del riesgo. *(Fuente: SANS:)*

63. Análisis de Emisiones:

Obtener conocimiento directo de datos comunicados monitoreando y resolviendo una señal que es emitida por un sistema y que contiene los datos pero que no está destinada a comunicar los datos. *(Fuente: SANS:)*

64. Análisis de Impacto en el Negocio (BIA):

Un Análisis de Impacto en el Negocio determina qué niveles de impacto sobre un sistema son tolerables. *(Fuente: SANS:)*

65. Análisis de Señales:

Obtener conocimiento indirecto de datos comunicados mediante la supervisión y análisis de una señal emitida por un sistema que contiene los datos pero no está destinada a comunicar dichos datos. *(Fuente: SANS:)*

66. Análisis de amenazas:

En el marco NICE, trabajo en ciberseguridad donde una persona: identifica y evalúa las capacidades y actividades de ciberdelincuentes o entidades de inteligencia extranjera, produce hallazgos para ayudar a iniciar o apoyar investigaciones o actividades de cumplimiento de la ley y contrainteligencia. *(Fuente: NICSS:)*

67. Análisis de defensa de redes informáticas:

En el Marco NICE, trabajo de ciberseguridad donde una persona usa medidas defensivas e información de diversas fuentes para identificar, analizar e informar sobre eventos que ocurren o podrían ocurrir en la red para proteger la información y sistemas. *(Fuente: NICSS:)*

68. Análisis de explotación:

En el marco NICE, trabajo de ciberseguridad en el que una persona analiza información recolectada para identificar vulnerabilidades y posibilidades de explotación. *(Fuente: NICSS:)*

69. Análisis de regresión:

El uso de pruebas automatizadas que se emplean para testear el software con todas las posibles entradas que se esperan. Normalmente los desarrolladores crean un conjunto de pruebas de regresión que se ejecutan antes de liberar una nueva versión. Ver también "fuzzing". *(Fuente: SANS:)*

70. Análisis de riesgo:

Examen sistemático de los componentes y características del riesgo. *(Fuente: NICSS:)*

71. Análisis de seguridad de sistemas:

En el marco NICE, trabajo en ciberseguridad donde una persona: realiza la integración/pruebas, operaciones y mantenimiento de la seguridad de sistemas. *(Fuente: NICSS:)*

72. Apetito De Riesgo:

Cantidad y tipo de riesgo que una organización está preparada para buscar o retener. *(Fuente: ISO 22.300:)*

73. Aplicación de parches:

Aplicar parches es el proceso de actualizar software a una versión diferente. *(Fuente: SANS:)*

74. AppSec:

el proceso de encontrar, corregir y prevenir vulnerabilidades de seguridad a nivel de aplicación, como parte del desarrollo de software *(Fuente: NICSS:)*

75. Applet:

Programas Java; una aplicación que usa el navegador web del cliente para proporcionar una interfaz de usuario. *(Fuente: SANS:)*

76. Applet malicioso:

Un pequeño programa de aplicación que se descarga y ejecuta automáticamente y que realiza una función no autorizada en un sistema de información. *(Fuente: NICSS:)*

77. Apreciación Del Riesgo:

Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo. *(Fuente: ISO 27.000:)*

78. Aprendizaje automático y evolución:

Un campo dedicado al diseño y desarrollo de algoritmos de inteligencia artificial para el descubrimiento automatizado de conocimiento e innovación por parte de sistemas de información. *(Fuente: NICSS:)*

79. Archivos de Contraseña Shadow:

Un archivo del sistema donde las contraseñas de usuario encriptadas se almacenan para que no estén disponibles para personas que intenten acceder ilegalmente al sistema. *(Fuente: SANS:)*

80. Armamento:

Un atacante crea malware o cargas maliciosas para usar contra un objetivo diseñando nuevas formas de malware o modificando programas existentes para que se adapten mejor a las vulnerabilidades que intentan explotar. *(Fuente: NICSS:)*

81. Arquitectura de seguridad de sistemas:

En el marco NICE, trabajo en ciberseguridad donde una persona: desarrolla conceptos de sistemas y trabaja en las fases de capacidades del ciclo de vida del desarrollo de sistemas, traduce la tecnología y condiciones ambientales (por ejemplo, leyes y regulaciones) en diseños y procesos de sistemas y seguridad. *(Fuente: NICSS:)*

82. Aseguramiento De La Calidad:

Parte de la gestión de la calidad orientada a proporcionar confianza en que se cumplirán los requisitos de la calidad. *(Fuente: ISO 9.000:)*

83. Aseguramiento cibernético:

el proceso de reforzar tecnologías, procesos y controles para proteger sistemas, redes, programas, dispositivos y datos de ataques cibernéticos *(Fuente: NICSS:)*

84. Aseguramiento de la información:

Las medidas que protegen y defienden la información y los sistemas de información asegurando su disponibilidad, integridad y confidencialidad. *(Fuente: NICSS:)*

85. Aseguramiento de software:

El nivel de confianza de que el software está libre de vulnerabilidades, ya sea intencionalmente diseñadas en el software o insertadas accidentalmente en cualquier momento durante su ciclo de vida, y que el software funciona de la manera prevista. *(Fuente: NICSS:)*

86. Aseguramiento de software e ingeniería de seguridad:

En el marco NICE, trabajo de ciberseguridad donde una persona: desarrolla y escribe/codifica nuevas aplicaciones de computadora, software o programas utilitarios especializados siguiendo las mejores prácticas de aseguramiento de software. *(Fuente: NICSS:)*

87. Asesoría legal y defensa legal:

En el marco NICE, trabajo de ciberseguridad donde una persona: proporciona consejos y recomendaciones legalmente fundamentadas a la dirección y personal sobre diversos temas relevantes dentro del dominio pertinente; promueve cambios legales y de políticas y representa al cliente mediante una amplia gama de productos escritos y orales, incluyendo escritos legales y procedimientos. *(Fuente: NICSS:)*

88. Asociación:

Relación organizada entre dos entidades (pública-pública, pública-privada, privada-privada) que establece el alcance, los roles, los procedimientos y las herramientas para prevenir y gestionar cualquier incidente que tenga un impacto sobre la seguridad y la resiliencia de acuerdo con la legislación aplicable. *(Fuente: ISO 22.300:)*

<satisfacción del cliente> Organización formada por organizaciones o personas miembro. *(Fuente: ISO 9.000:)*

89. Aspectos De Seguridad:

Característica, elemento o propiedad que reduce el riesgo de crisis y disastres causados de forma fortuita, intencionada o natural que provoquen una disrupción y tengan consecuencias en los productos o servicios, el funcionamiento, los activos críticos y la continuidad de una organización y de sus partes interesadas. *(Fuente: ISO 22.300:)*

90. Atacante:

Parte que actúa con intención maliciosa para comprometer un sistema de información. *(Fuente: NICSS:)*

91. Ataque:

Intento o intentos exitosos o fracasados de sortear una solución de autenticación, incluidos los intentos de imitar, producir o reproducir los elementos de autenticación. *(Fuente: ISO 22.300:)*

El acto intencional de intentar eludir uno o más servicios o controles de seguridad de un sistema de información. *(Fuente: NICSS:)*

Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo. *(Fuente: ISO 27.000:)*

92. Ataque Interno:

Ataque perpetrado por personas o entidades vinculadas directa o indirectamente al fabricante, originador de los bienes o tenedor de derechos legítimos (personal del tenedor de derechos, subcontratista, proveedor, etc.). *(Fuente: ISO 22.300:)*

93. Ataque SYN Flood:

Un ataque de denegación de servicio que envía a un host más paquetes TCP SYN (solicitud para sincronizar números de secuencia, usada al abrir una conexión) de los que la implementación del protocolo puede manejar. *(Fuente: SANS:)*

94. Ataque Smurf:

El ataque Smurf funciona falsificando la dirección objetivo y enviando un ping a la dirección de difusión de una red remota, lo que resulta en que se envíe una gran cantidad de respuestas de ping al objetivo. *(Fuente: SANS:)*

95. Ataque activo:

Un ataque real perpetrado por una fuente de amenaza intencional que intenta alterar un sistema, sus recursos, sus datos o sus operaciones. *(Fuente: NICSS:)*

96. Ataque de día cero:

Un ataque o amenaza de día cero es una amenaza informática que intenta explotar vulnerabilidades en aplicaciones desconocidas para otros o no divulgadas al desarrollador del software. Los exploits de día cero (código que puede usar la vulnerabilidad para realizar un ataque) son usados o compartidos por atacantes antes que el desarrollador se entere de la vulnerabilidad. *(Fuente: SANS:)*

97. Ataque de fragmento pequeño:

Con muchas implementaciones IP es posible imponer un tamaño de fragmento inusualmente pequeño en paquetes salientes. Si el tamaño del fragmento es lo suficientemente pequeño para forzar que algunos campos del encabezado TCP de un paquete TCP queden en el segundo fragmento, las reglas de filtro que especifican patrones para esos campos no coincidirán. Si la implementación de filtrado no hace cumplir un tamaño mínimo de fragmento, un paquete no permitido podría pasar porque no coincidió con el filtro. STD 5, RFC 791 indica: Cada módulo de Internet debe ser capaz de reenviar un datagrama de 68 octetos sin más fragmentación. Esto es porque un encabezado de Internet puede tener hasta 60 octetos, y el fragmento mínimo es de 8 octetos. *(Fuente: SANS:)*

98. Ataque de intermediario (MitM):

Un ataque de intermediario es un tipo de ciberataque en el que el atacante intercepta y retransmite mensajes secretamente entre dos partes que creen que están comunicándose directamente entre sí. El ataque es un tipo de espionaje en el que el atacante intercepta y luego controla toda la conversación. *(Fuente: SANS:)*

99. Ataque de secuestro:

Una forma de escucha activa en la que el atacante toma control de una asociación de comunicación previamente establecida. *(Fuente: SANS:)*

100. Ataque de superposición de fragmentos:

Un ataque de fragmentación TCP/IP posible porque IP permite que los paquetes se dividan en fragmentos para un transporte más eficiente a través de varios medios. El paquete TCP (y su encabezado) se transporta en el paquete IP. En este ataque, el segundo fragmento contiene

un desplazamiento incorrecto. Cuando el paquete se reconstruye, el número de puerto es sobrescrito. *(Fuente: SANS:)*

101. Ataque de suplantación:

Un tipo de ataque en el que una entidad del sistema asume ilegítimamente la identidad de otra entidad. *(Fuente: SANS:)*

102. Ataque hombre en el medio (MitM):

Un ataque man-in-the-middle es un ciberataque donde el atacante retransmite secreta y posiblemente altera las comunicaciones entre dos partes que creen estar comunicándose directamente. *(Fuente: NICSS:)*

103. Ataque híbrido:

Un ataque híbrido se basa en el método de ataque de diccionario añadiendo números y símbolos a las palabras del diccionario. *(Fuente: SANS:)*

104. Ataque pasivo:

Un ataque real perpetrado por una fuente de amenaza intencional que intenta aprender o usar información de un sistema, pero no intenta alterar el sistema, sus recursos, datos u operaciones. *(Fuente: NICSS:)*

105. Ataque por diccionario:

Un ataque que prueba todas las frases o palabras de un diccionario, intentando descifrar una contraseña o clave. Un ataque por diccionario usa una lista predefinida de palabras, a diferencia de un ataque de fuerza bruta que intenta todas las combinaciones posibles. *(Fuente: SANS:)*

106. Ataque por fuerza bruta:

Método de ataque que usa prueba y error para descifrar contraseñas, credenciales de acceso y claves de cifrado. *(Fuente: NICSS:)*

107. Ataque por inferencia:

Los ataques por inferencia se basan en que el usuario haga conexiones lógicas entre piezas de información aparentemente no relacionadas. *(Fuente: SANS:)*

108. Ataques de validación de entrada:

Los ataques de validación de entrada ocurren cuando un atacante envía intencionalmente entradas inusuales con la esperanza de confundir una aplicación. *(Fuente: SANS:)*

109. Ataques por Fallas de Línea:

Los ataques por fallas de línea usan debilidades entre interfaces de sistemas para explotar brechas en la cobertura. *(Fuente: SANS:)*

110. Atributo:

Propiedad o característica de un objeto que es cuantitativa o cualitativamente distinguible por medios humanos o automáticos. *(Fuente: ISO 27.000:)*

111. Auditado:

Organización que es auditada. *(Fuente: ISO 9.000:)*

112. Auditor:

Persona que lleva a cabo una auditoría. *(Fuente: ISO 22.300:)*

113. Auditoría:

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría. *(Fuente: ISO 27.000:)*

La auditoría es la recopilación y análisis de información sobre los activos para garantizar cosas como el cumplimiento de políticas y la seguridad frente a vulnerabilidades. *(Fuente: SANS:)*

Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y valorarlas de manera objetiva con el fin de determinar el grado en el que cumplen los criterios de auditoría. *(Fuente: ISO 22.300:)*

114. Auditoría Combinada:

Auditoría llevada a cabo conjuntamente a un único auditado en dos o más sistemas de gestión. *(Fuente: ISO 9.000:)*

115. Auditoría Conjunta:

Auditoría llevada a cabo a un único auditado por dos o más organizaciones auditoras. *(Fuente: ISO 9.000:)*

116. Auditoría Interna:

Auditoría realizada por la propia organización, o en su nombre, para la revisión por la dirección y otros fines internos, y que puede constituir la base para la autodeclaración de conformidad de una organización. *(Fuente: ISO 22.300:)*

117. Autenticación:

Acción y efecto de autenticar. *(Fuente: UNE 71.505:)*

Proceso de corroboración de una entidad o de atributos con un nivel de garantía especificado o entendido. *(Fuente: ISO 22.300:)*

Aportación de garantías de que son correctas las características que una entidad reivindica para sí misma. *(Fuente: ISO 27.000:)*

La autenticación es el proceso de confirmar la validez de la identidad declarada. *(Fuente: SANS:)*

También es el proceso de verificar la fuente y la integridad de los datos. *(Fuente: NICSS:)*

118. Autenticación basada en certificados:

La Autenticación basada en certificados es el uso de SSL y certificados para autenticar y cifrar el tráfico HTTP. *(Fuente: SANS:)*

119. Autenticación basada en formularios:

La autenticación basada en formularios utiliza formularios en una página web para pedir al usuario que ingrese su nombre de usuario y contraseña. *(Fuente: SANS:)*

120. Autenticación básica:

La autenticación básica es el esquema más simple de autenticación basada en la web que funciona enviando el nombre de usuario y la contraseña con cada solicitud. *(Fuente: SANS:)*

121. Autenticación por resumen:

La autenticación por resumen permite a un cliente web calcular hashes MD5 de la contraseña para demostrar que la posee. *(Fuente: SANS:)*

122. Autenticidad:

Propiedad consistente en que una entidad es lo que dice ser. *(Fuente: ISO 27.000:)*

La autenticidad es la validez y conformidad de la información original. *(Fuente: SANS:)*

Propiedad lograda mediante métodos criptográficos que garantiza que algo es genuino, verificable y confiable, generando confianza en su validez. *(Fuente: NICSS:)*

123. Automatización de seguridad:

El uso de tecnología de la información en lugar de procesos manuales para la respuesta y gestión de incidentes cibernéticos. *(Fuente: NICSS:)*

124. Autorización:

La autorización es la aprobación, permiso o facultad para que alguien o algo realice una acción. *(Fuente: SANS:)*

El proceso o acto de conceder privilegios de acceso, o los privilegios de acceso otorgados. *(Fuente: NICSS:)*

125. Aversion al riesgo:

Evitar riesgos incluso si esto conduce a la pérdida de una oportunidad. Por ejemplo, usar una llamada telefónica (más cara) en vez de enviar un correo electrónico para evitar riesgos asociados al correo puede considerarse "Aversion al riesgo". *(Fuente: SANS:)*

126. Aviso Al Público:

Mensajes de notificación y alerta difundidos como medida de respuesta a un incidente para permitir al personal de primera intervención y a las personas en riesgo adoptar medidas de seguridad. *(Fuente: ISO 22.300:)*

— B —

127. BCrypt:

Función de hash de contraseñas basada en el cifrado Blowfish y presentada en USENIX en 1999. *(Fuente: NICSS:)*

128. BIND:

BIND significa Berkeley Internet Name Domain y es una implementación de DNS. DNS se utiliza para la resolución de nombres de dominio a direcciones IP. *(Fuente: SANS:)*

129. Backdoor:

Un backdoor es una herramienta instalada después de una vulneración para dar al atacante un acceso más fácil al sistema comprometido, eludiendo cualquier mecanismo de seguridad existente. *(Fuente: SANS:)*

130. Banner:

Un banner es la información que se muestra a un usuario remoto que intenta conectarse a un servicio. Esto puede incluir información de versión, información del sistema o una advertencia sobre el uso autorizado. *(Fuente: SANS:)*

131. Barrido Ping:

Un ataque que envía solicitudes ICMP echo ("pings") a un rango de direcciones IP, con el objetivo de encontrar hosts que pueden ser examinados en busca de vulnerabilidades. *(Fuente: SANS:)*

132. Bastion Host:

Un bastion host ha sido reforzado en previsión de vulnerabilidades que aún no han sido descubiertas. *(Fuente: SANS:)*

133. Biblioteca de Enlace Dinámico:

Una colección de pequeños programas, cualquiera de los cuales puede ser llamado cuando se necesita por un programa mayor que está ejecutándose en la computadora. El pequeño programa que permite que el programa mayor se comunique con un dispositivo específico como una impresora o escáner a menudo está empaquetado como un programa DLL (usualmente referido como un archivo DLL). *(Fuente: SANS:)*

134. Bien Material:

Producto fabricado, cultivado o proporcionado por la naturaleza. *(Fuente: ISO 22.300:)*

135. Bien Material Auténtico:

Bien material producido bajo el control del fabricante legítimo, el originador de los bienes o el tenedor de derechos. *(Fuente: ISO 22.300:)*

136. Bienes (Preferido); Mercancías:

Artículos o material que, tras la realización de una orden de compra, son fabricados, manipulados, procesados o transportados en la cadena de suministro para uso o consumo de su comprador. *(Fuente: ISO 22.300:)*

137. Biohacking:

Realizar pequeños cambios estratégicos en hábitos y comportamientos para mejorar funciones cognitivas y manejo del peso, entre otros. *(Fuente: NICSS:)*

138. Biométricos:

Los biométricos usan características físicas de los usuarios para determinar el acceso. *(Fuente: SANS:)*

139. Biosupervisión:

Proceso sistemático de recopilación de información biológica en casi tiempo real para detectar, monitorear y caracterizar amenazas a la salud humana, animal, vegetal y ambiental, permitiendo alertas tempranas e identificación de brotes. *(Fuente: NICSS:)*

140. Bit:

La unidad más pequeña de almacenamiento de información; una contracción del término "binary digit"; uno de dos símbolos: "0" (cero) y "1" (uno), que se utilizan para representar números binarios. *(Fuente: SANS:)*

141. Blockchain:

Seguimiento de transacciones: Blockchain puede rastrear pedidos, pagos, cuentas y más. *(Fuente: NICSS:)*

142. Bluejacking:

Ataque en el que alguien envía mensajes no solicitados a un dispositivo habilitado para Bluetooth. *(Fuente: NICSS:)*

143. Bluesnarfing:

Técnica de hacking en la que un atacante accede a un dispositivo inalámbrico a través de una conexión Bluetooth. *(Fuente: NICSS:)*

144. Bolsa de emergencia:

Una bolsa que contiene todos los elementos necesarios para responder a un incidente, para ayudar a mitigar los efectos de reacciones demoradas. *(Fuente: SANS:)*

145. Bomba Fork:

Un Fork Bomb funciona usando la llamada fork() para crear un nuevo proceso que es una copia del original. Al hacerlo repetidamente, todos los procesos disponibles en la máquina pueden ser ocupados. *(Fuente: SANS:)*

146. Bombas lógicas:

Las bombas lógicas son programas o fragmentos de código que se ejecutan cuando ocurre un evento predefinido. Las bombas lógicas también pueden configurarse para activarse en una fecha determinada o cuando se cumplen ciertas circunstancias. *(Fuente: SANS:)*

147. Bootkit:

Tipo de malware que infecta el proceso de arranque de un ordenador, otorgando al atacante el control del sistema. Son una amenaza grave porque pueden eludir las medidas de seguridad estándar y permanecer ocultos. *(Fuente: NICSS:)*

148. Bosque:

Un bosque es un conjunto de dominios de Active Directory que replican sus bases de datos entre sí. *(Fuente: SANS:)*

149. Bot:

Un miembro de una colección más grande de computadoras comprometidas conocida como botnet. *(Fuente: NICSS:)*

150. Botnet:

Una botnet es una gran cantidad de computadoras comprometidas que se utilizan para crear y enviar spam o virus, o saturar una red con mensajes como ataque de denegación de servicio. *(Fuente: SANS:)*

Conjunto de computadoras comprometidas por código malicioso y controladas a través de una red. *(Fuente: NICSS:)*

151. Bucle de enrutamiento:

Un bucle de enrutamiento ocurre cuando dos o más routers mal configurados intercambian repetidamente el mismo paquete una y otra vez. *(Fuente: SANS:)*

152. Byte:

Una unidad fundamental de almacenamiento de computadora; la unidad direccionable más pequeña en la arquitectura de una computadora. Usualmente contiene un carácter de información y usualmente equivale a ocho bits. *(Fuente: SANS:)*

153. Búsqueda directa:

La búsqueda directa usa un nombre de dominio de Internet para encontrar una dirección IP. *(Fuente: SANS:)*

154. Búsqueda en la Basura:

Búsqueda en la basura es obtener contraseñas y directorios corporativos buscando en medios descartados. *(Fuente: SANS:)*

155. Búsqueda inversa:

Averiguar el nombre de host que corresponde a una dirección IP particular. La búsqueda inversa usa una dirección IP para encontrar un nombre de dominio. *(Fuente: SANS:)*

— C —

156. Caballo de Troya:

Programa de computadora que aparenta tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad del sistema que invoca el programa. *(Fuente: SANS:)*

Un programa informático que parece tener una función útil, pero que también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad del sistema que invoca el programa. *(Fuente: NICSS:)*

157. Cable Cruzado:

Un cable cruzado invierte los pares de cables en el otro extremo y puede usarse para conectar dispositivos directamente entre sí. *(Fuente: SANS:)*

158. Cable Directo:

Un cable directo es aquel en que los pines de un lado del conector están cableados a los mismos pines en el otro extremo. Se usa para interconectar nodos en la red. *(Fuente: SANS:)*

159. Cache:

Se pronuncia “cash”, un mecanismo especial de almacenamiento de alta velocidad. Puede ser una sección reservada de la memoria principal o un dispositivo de almacenamiento independiente y rápido. En computadoras personales, se usan comúnmente dos tipos de caché: caché de memoria y caché de disco. *(Fuente: SANS:)*

160. Cache Cramming:

Cache Cramming es la técnica de engañar a un navegador para que ejecute código Java en caché desde el disco local, en lugar de desde la zona de Internet, de modo que se ejecute con permisos menos restrictivos. *(Fuente: SANS:)*

161. Cadena De Suministro:

Relación bidireccional de las organizaciones, las personas, los procesos, la logística, la información, la tecnología y los recursos involucrados en las actividades y la creación de valor desde el aprovisionamiento de los materiales hasta la entrega/prestación de los productos o servicios. *(Fuente: ISO 22.300:)*

162. Cadena De Suministro Internacional:

Cadena de suministro que en algún momento cruza una frontera internacional o económica. *(Fuente: ISO 22.300:)*

163. Cadena de Custodia:

Cadena de Custodia es la aplicación importante de las reglas federales de evidencia y su manejo. *(Fuente: SANS:)*

164. Cadena de suministro:

Un sistema de organizaciones, personas, actividades, información y recursos, para crear y mover productos incluyendo componentes del producto y/o servicios desde proveedores hasta sus clientes. *(Fuente: NICSS:)*

165. Caja negra:

Forma de prueba realizada sin conocimiento de la estructura interna del sistema objetivo. *(Fuente: NICSS:)*

166. Calidad:

Grado en el que un conjunto de características inherentes de un objeto cumple con los requisitos. *(Fuente: ISO 9.000:)*

167. Canales Ocultos:

Los canales ocultos son los medios por los cuales la información puede ser comunicada entre dos partes de manera encubierta usando operaciones normales del sistema. Por ejemplo, cambiando la cantidad de espacio disponible en disco duro en un servidor de archivos puede usarse para comunicar información. *(Fuente: SANS:)*

168. Capa de Conexión Segura (SSL):

Un protocolo desarrollado por Netscape para transmitir documentos privados vía Internet. SSL funciona usando una clave pública para encriptar los datos que se transfieren a través de la conexión SSL. *(Fuente: SANS:)*

169. Capacidad:

Los medios para llevar a cabo una misión, función u objetivo. *(Fuente: NICSS:)*

Combinación de todas las fortalezas y recursos disponibles en una organización, comunidad o sociedad que puede reducir el nivel de riesgo o los efectos de una crisis. *(Fuente: ISO 22.300:)*

Aptitud de un objeto para realizar una salida que cumplirá los requisitos para esa salida. *(Fuente: ISO 9.000:)*

170. Capas OSI:

La idea principal en OSI es que el proceso de comunicación entre dos puntos finales en una red de telecomunicaciones puede dividirse en capas, donde cada capa añade su propio conjunto de funciones especiales y relacionadas. Cada usuario o programa comunicante se encuentra en una computadora equipada con estas siete capas de función. Así, en un mensaje entre usuarios, habrá un flujo de datos que pasa por cada capa en un extremo, bajando por las capas en esa computadora y, en el otro extremo, cuando el mensaje llega, otro flujo de datos sube por las capas en la computadora receptora y finalmente al usuario o programa final. La programación y el hardware que proporcionan estas siete capas generalmente son una combinación del sistema operativo de la computadora, aplicaciones (como tu navegador web), TCP/IP o protocolos alternativos de transporte y red, y el software y hardware que permiten enviar una señal por una de las líneas conectadas a tu computadora. OSI divide las telecomunicaciones en siete capas. Las capas están en dos grupos. Las cuatro capas superiores se usan siempre que un mensaje pasa desde o hacia un usuario. Las tres capas

inferiores (hasta la capa de red) se usan cuando cualquier mensaje pasa a través del equipo anfitrión o router. Los mensajes destinados a esta computadora pasan a las capas superiores. Los mensajes destinados a otro host no se pasan a las capas superiores sino que se reenvían a otro host. Las siete capas son: Capa 7: La capa de aplicación... Es la capa en la que se identifican los socios de comunicación, se identifica la calidad del servicio, se consideran la autenticación del usuario y la privacidad, y se identifican restricciones en la sintaxis de datos. (Esta capa no es la aplicación en sí, aunque algunas aplicaciones pueden realizar funciones de la capa de aplicación.) Capa 6: La capa de presentación... Esta es una capa, usualmente parte del sistema operativo, que convierte datos entrantes y salientes de un formato de presentación a otro (por ejemplo, de un flujo de texto a una ventana emergente con el texto recién llegado). A veces llamada capa de sintaxis. Capa 5: La capa de sesión... Esta capa establece, coordina y termina conversaciones, intercambios y diálogos entre las aplicaciones en cada extremo. Maneja la coordinación de sesión y conexión. Capa 4: La capa de transporte... Esta capa gestiona el control de extremo a extremo (por ejemplo, determinar si todos los paquetes han llegado) y la verificación de errores. Asegura la transferencia completa de datos. Capa 3: La capa de red... Esta capa maneja el enrutamiento de los datos (enviándolos en la dirección correcta al destino correcto en transmisiones salientes y recibiendo transmisiones entrantes a nivel de paquete). La capa de red realiza enrutamiento y reenvío. Capa 2: La capa de enlace de datos... Esta capa proporciona sincronización para el nivel físico y realiza bit-stuffing para cadenas de 1s en exceso de 5. Proporciona conocimiento y gestión del protocolo de transmisión. Capa 1: La capa física... Esta capa transmite el flujo de bits a través de la red a nivel eléctrico y mecánico. Proporciona los medios hardware para enviar y recibir datos sobre un portador. *(Fuente: SANS:)*

171. Captura de contraseñas:

Escucha pasiva, usualmente en una red de área local, para obtener conocimiento de contraseñas. *(Fuente: SANS:)*

172. Capturador de Paquetes (Sniffer):

Un sniffer es una herramienta que monitorea el tráfico de red conforme se recibe en una interfaz de red. *(Fuente: SANS:)*

173. Característica:

Rasgo diferenciador. *(Fuente: ISO 9.000:)*

174. Característica De La Calidad:

Característica inherente a un objeto relacionada con un requisito. *(Fuente: ISO 9.000:)*

175. Característica Metrológica:

Característica que puede influir sobre los resultados de la medición. *(Fuente: ISO 9.000:)*

176. Carga útil:

La carga útil es el dato real de la aplicación que contiene un paquete. *(Fuente: SANS:)*

177. Carácter no imprimible:

Un carácter que no tiene una letra correspondiente a su código ASCII. Ejemplos son el salto de línea (código ASCII 10 decimal), el retorno de carro (13 decimal), o el sonido de campana (7 decimal). En PC, a menudo se pueden agregar caracteres no imprimibles manteniendo presionada la tecla Alt y escribiendo el valor decimal (ej., Alt-007 para la campana). Existen otros esquemas de codificación, pero ASCII es el más prevalente. *(Fuente: SANS:)*

178. Caso Específico:

<plan de la calidad> Tema del plan de la calidad. *(Fuente: ISO 9.000:)*

179. Catphish:

Creación de una identidad falsa en línea por parte de un ciberdelincuente con fines de engaño, fraude o explotación. *(Fuente: NICSS:)*

180. Certificado De Seguridad:

Proceso de verificación de la fiabilidad de las personas que tendrán acceso a información sensible para la seguridad. *(Fuente: ISO 22.300:)*

181. Certificado digital:

Un certificado digital es una "tarjeta de crédito" electrónica que establece tus credenciales al hacer negocios u otras transacciones en la Web. Es emitido por una autoridad de certificación. Contiene tu nombre, un número de serie, fechas de expiración, una copia de la clave pública del titular (utilizada para cifrar mensajes y firmas digitales), y la firma digital de la autoridad emisora para que el receptor pueda verificar que el certificado es auténtico. *(Fuente: SANS:)*

182. Ciberataque:

Un ciberataque es cualquier intento no autorizado de acceder, interrumpir, robar o dañar sistemas informáticos, redes o datos. *(Fuente: SANS:)*

un intento malicioso y deliberado de vulnerar el sistema de información *(Fuente: NICSS:)*

183. Ciberbioseguridad:

un campo emergente que aborda la intersección entre la ciberseguridad y la bioseguridad, enfocándose en proteger datos, procesos y sistemas biológicos de amenazas cibernéticas y actividades maliciosas *(Fuente: NICSS:)*

184. Cibercrimen:

Actividad criminal que implica el uso de computadoras o redes como Internet. *(Fuente: NICSS:)*

185. Ciberespionaje:

o espionaje cibernético, es un tipo de ciberataque en el que un usuario no autorizado intenta acceder a datos sensibles o clasificados o propiedad intelectual (IP) con fines de ganancia económica, ventaja competitiva o razones políticas *(Fuente: NICSS:)*

186. Ciberseguridad:

Estrategia, políticas y estándares relacionados con la seguridad y operaciones en el ciberespacio, y que abarcan toda la gama de reducción de amenazas, reducción de vulnerabilidades, disuasión, compromiso internacional, respuesta a incidentes, resiliencia y actividades de recuperación, incluyendo operaciones de redes informáticas, garantía de la información, cumplimiento de la ley, diplomacia, misiones militares y de inteligencia en

relación con la seguridad y estabilidad de la infraestructura global de información y comunicaciones. *(Fuente: NICSS:)*

187. Ciclo De Vida De Un Bien Material:

Las etapas de la vida de un bien material incluidas la concepción, el diseño, la fabricación, el almacenamiento, mantenimiento, la reventa y la eliminación. *(Fuente: ISO 22.300:)*

188. Cifra:

Un algoritmo criptográfico para cifrado y descifrado. *(Fuente: SANS:)*

189. Cifrado:

Conversión de datos a una forma que no puede ser comprendida fácilmente por personas no autorizadas. *(Fuente: NICSS:)*

Transformación criptográfica de datos (llamados "texto claro") en una forma (llamada "texto cifrado") que oculta el significado original de los datos para evitar que sea conocido o utilizado. *(Fuente: SANS:)*

190. Cifrado de clave pública:

Sinónimo popular de "criptografía asimétrica". *(Fuente: SANS:)*

191. Cifrado híbrido:

Una aplicación de la criptografía que combina dos o más algoritmos de cifrado, particularmente una combinación de cifrado simétrico y asimétrico. *(Fuente: SANS:)*

192. Cifrado por Flujo:

Un cifrado por flujo funciona cifrando un mensaje un bit, byte o palabra de computadora a la vez. *(Fuente: SANS:)*

193. Cifrado por bloques:

Un cifrado por bloques encripta un bloque de datos a la vez. *(Fuente: SANS:)*

194. Cifrado unidireccional:

Transformación irreversible de texto plano a texto cifrado, de modo que el texto plano no puede ser recuperado del texto cifrado excepto mediante procedimientos exhaustivos, incluso si se conoce la clave criptográfica. *(Fuente: SANS:)*

195. Cifrar (encipher):

Convertir texto plano a texto cifrado mediante un sistema criptográfico. *(Fuente: NICSS:)*

196. Cifrar (encrypt):

Término genérico que abarca cifrar (encipher) y codificar (encode). *(Fuente: NICSS:)*

197. Clase:

Categoría o rango dado a diferentes requisitos para un objeto que tienen el mismo uso funcional. *(Fuente: ISO 9.000:)*

198. Clave Dividida:

Una clave criptográfica que está dividida en dos o más partes separadas que individualmente no proporcionan conocimiento sobre la clave completa que resulta de combinar esas partes. *(Fuente: SANS:)*

199. Clave de Sesión:

En el contexto de la encriptación simétrica, una clave que es temporal o se usa por un período relativamente corto. Usualmente, una clave de sesión se usa por un período definido de comunicación entre dos computadoras, como durante la duración de una conexión o conjunto de transacciones, o en una aplicación que protege grandes cantidades de datos y, por lo tanto, requiere cambios frecuentes de clave. *(Fuente: SANS:)*

200. Clave privada:

La parte secreta de un par de claves asimétricas que está asociada de manera única con una entidad. *(Fuente: NICSS:)*

201. Clave pública:

El componente divulgado públicamente de un par de claves criptográficas usado para criptografía asimétrica. *(Fuente: SANS:)*

La parte pública de un par de claves asimétricas que está asociada de manera única con una entidad y que puede ser hecha pública. *(Fuente: NICSS:)*

202. Clave secreta:

También, un algoritmo criptográfico que utiliza una sola clave (es decir, una clave secreta) tanto para el cifrado de texto plano como para el descifrado de texto cifrado. *(Fuente: NICSS:)*

203. Clave simétrica:

También, un algoritmo criptográfico que usa una sola clave (es decir, una clave secreta) tanto para el cifrado de texto plano como para la descifrado de texto cifrado. *(Fuente: NICSS:)*

Una clave criptográfica usada en un algoritmo criptográfico simétrico. *(Fuente: SANS:)*

204. Cliente:

Una entidad del sistema que solicita y usa un servicio provisto por otra entidad del sistema, llamada "servidor". En algunos casos, el servidor puede ser a su vez cliente de otro servidor. *(Fuente: SANS:)*

Entidad que contrata, ha contratado en el pasado, o tiene la intención de contratar a una organización para realizar operaciones de seguridad en su nombre, incluyendo, cuando proceda, el caso de que dicha organización contrate externamente a otra empresa o a fuerzas locales. *(Fuente: ISO 22.300:)*

Persona u organización que podría recibir o que recibe un producto o un servicio destinado a esa persona u organización o requerido por ella. *(Fuente: ISO 9.000:)*

205. Cliente Certificado:

Organización cuyo sistema de gestión de la seguridad de la cadena de suministro ha sido certificado/registrado por un tercero cualificado. *(Fuente: ISO 22.300:)*

206. Cliente Crítico:

Entidad cuya pérdida como cliente supondría una amenaza para la supervivencia de una organización. *(Fuente: ISO 22.300:)*

207. Cliente De La Auditoría:

Organización o persona que solicita una auditoría. *(Fuente: ISO 9.000:)*

208. Cliente Honey:

Ver Honeymonkey. *(Fuente: SANS:)*

209. Codificar:

Convertir texto plano a texto cifrado mediante un código. *(Fuente: NICSS:)*

210. Colaborativo (crowdsourced):

Proyecto basado en colaboración masiva en línea, en el que los participantes no siempre son remunerados; un ejemplo bien conocido es Wikipedia. *(Fuente: NICSS:)*

211. Colectivo Que Comparte Información:

Grupo de organizaciones que acuerdan compartir información. *(Fuente: ISO 27.000:)*

212. Colisión:

Una colisión ocurre cuando múltiples sistemas transmiten simultáneamente en el mismo cable. *(Fuente: SANS:)*

213. Compartición Del Riesgo (Preferido); Reparto Del Riesgo (Desaconsejado):

Forma de tratamiento del riesgo que implica una distribución acordada del riesgo con otras partes. *(Fuente: ISO 22.300:)*

214. Compartición No Protegida:

En terminología de Windows, una "compartición" es un mecanismo que permite a un usuario conectarse a sistemas de archivos e impresoras en otros sistemas. Una "compartición no protegida" es aquella que permite que cualquiera se conecte a ella. *(Fuente: SANS:)*

215. Competencia:

Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos. *(Fuente: ISO 22.300:)*

Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos. *(Fuente: ISO 27.000:)*

216. Completitud:

Cualidad que responde a una representación completa de las operaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores operaciones o actividades. *(Fuente: UNE 71.505:)*

217. Comportamiento:

Grado en que una persona practica varias medidas de ciberseguridad para evitar o reducir los tipos de amenazas cibernéticas a las que es vulnerable. *(Fuente: NICSS:)*

218. Compromiso:

Participación activa en, y contribución a, las actividades para lograr objetivos compartidos. *(Fuente: ISO 9.000:)*

219. Computación en la nube:

Modelo que permite el acceso bajo demanda a un conjunto compartido de recursos o capacidades informáticas configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que se pueden aprovisionar y liberar rápidamente. *(Fuente: NICSS:)*

Utilización de servidores remotos en el centro de datos de un proveedor de nube para almacenar, gestionar y procesar tus datos en lugar de usar sistemas informáticos locales. *(Fuente: SANS:)*

220. Comunicación Del Riesgo:

Intercambio o compartición de información sobre el riesgo entre quien toma las decisiones y otras partes interesadas. *(Fuente: ISO 22.300:)*

221. Comunicación Y Consulta:

Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las partes interesadas y otros, en relación con la gestión del riesgo. *(Fuente: ISO 22.300:)*

222. Comunicación Y Consulta Del Riesgo:

Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las partes interesadas, en relación con la gestión del riesgo. *(Fuente: ISO 27.000:)*

223. Comunidad:

Grupo de organizaciones asociadas, personas y grupos que comparten intereses comunes. *(Fuente: ISO 22.300:)*

224. Concesión:

Autorización para utilizar o liberar un producto o servicio que no es conforme con los requisitos especificados. *(Fuente: ISO 9.000:)*

225. Conciencia situacional:

En ciberseguridad, comprender el estado actual y la postura de seguridad respecto a la disponibilidad, confidencialidad e integridad de redes, sistemas, usuarios y datos, así como proyectar estados futuros de estos. *(Fuente: NICSS:)*

226. Conclusiones De La Auditoría:

Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría. *(Fuente: ISO 9.000:)*

227. Condición de carrera:

Una condición de carrera explota la pequeña ventana de tiempo entre la aplicación de un control de seguridad y cuando el servicio es utilizado. *(Fuente: SANS:)*

228. Confiabilidad:

Capacidad para desempeñar cómo y cuándo se requiera. *(Fuente: ISO 9.000:)*

Propiedad de la información que asegura los procesos y resultados de la autenticación, la integridad, disponibilidad y completitud de la misma, y garantiza que esa información se ha obtenido y gestionado conforme a procedimientos. previamente planificados. En el caso de las evidencias electrónicas, estos procedimientos son los propios de un sistema de gestión de evidencias electrónicas. *(Fuente: UNE 71.505:)*

229. Confianza:

La confianza determina qué permisos y qué acciones otros sistemas o usuarios pueden realizar en máquinas remotas. *(Fuente: SANS:)*

230. Confidencialidad:

Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. *(Fuente: ISO 27.000:)*

La confidencialidad es la necesidad de asegurar que la información sea revelada solo a quienes están autorizados a verla. *(Fuente: SANS:)*

Preservar las restricciones autorizadas sobre el acceso y divulgación de información, incluyendo la protección de la privacidad personal y la información propietaria. *(Fuente: NICSS:)*

Propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados. *(Fuente: UNE 71.505:)*

231. Configuración:

Características funcionales y físicas interrelacionadas de un producto o servicio definidas en la información sobre configuración del producto. *(Fuente: ISO 9.000:)*

232. Configuración De Referencia:

Información sobre configuración del producto aprobada, que establece las características de un producto o servicio en un punto determinado en el tiempo, que sirve como referencia para actividades durante todo el ciclo de vida del producto o servicio. *(Fuente: ISO 9.000:)*

233. Confirmación Metrológica:

Conjunto de operaciones necesarias para asegurarse de que el equipo de medición es conforme con los requisitos para su uso previsto. *(Fuente: ISO 9.000:)*

234. Conflicto:

<satisfacción del cliente> Desacuerdo, que surge de una queja presentada a un proveedor de PRC. *(Fuente: ISO 9.000:)*

235. Conforme a FedRAMP:

Programa a nivel gubernamental que proporciona un enfoque estandarizado para la evaluación de seguridad, autorización y monitoreo continuo de productos y servicios en la nube. *(Fuente: NICSS:)*

236. Conformidad:

Cumplimiento de un requisito. *(Fuente: ISO 22.300:)*

Cumplimiento de un requisito. *(Fuente: ISO 27.000:)*

237. Consciente de la ciberseguridad:

saber cuáles son las amenazas a la seguridad y actuar de manera responsable para evitar riesgos potenciales. *(Fuente: NICSS:)*

238. Consecuencia:

Resultado de un evento que afecta a los objetivos. *(Fuente: ISO 22.300:)*

En ciberseguridad, es el efecto de la pérdida de confidencialidad, integridad o disponibilidad de la información o de un sistema sobre las operaciones de una organización, sus activos, individuos, otras organizaciones o intereses nacionales. *(Fuente: NICSS:)*

Resultado de un suceso que afecta a los objetivos. *(Fuente: ISO 27.000:)*

239. Consulta En Sistemas De Gestión Y/O Valoración De Riesgos Asociados:

Participación en el diseño, implementación o mantenimiento de una cadena de suministro, sistema de gestión de la seguridad y en la realización de evaluaciones del riesgo. *(Fuente: ISO 22.300:)*

240. Consultor Del Sistema De Gestión De La Calidad:

Persona que ayuda a la organización en la realización de un sistema de gestión de la calidad, dando asesoramiento o información. *(Fuente: ISO 9.000:)*

241. Contenido activo:

Código de programa incrustado en el contenido de una página web. Cuando la página es accedida por un navegador, el código se descarga y ejecuta automáticamente en la estación de trabajo del usuario. Ej. Java, ActiveX (MS) *(Fuente: SANS:)*

Software que puede ejecutar o activar acciones automáticamente sin la intervención explícita del usuario. *(Fuente: NICSS:)*

242. Contexto De La Organización:

Combinación de cuestiones internas y externas que pueden tener un efecto en el enfoque de la organización para el desarrollo y logro de sus objetivos. *(Fuente: ISO 9.000:)*

243. Contexto Externo:

Entorno externo en el que la organización busca alcanzar sus objetivos. *(Fuente: ISO 27.000:)*

244. Contexto Interno:

Entorno interno en el que la organización busca alcanzar sus objetivos. *(Fuente: ISO 27.000:)*

245. Contingencia:

Posible evento, condición o eventualidad futuro. *(Fuente: ISO 22.300:)*

246. Continuidad:

Capacidad estratégica y táctica, previamente aprobada por la dirección1), de una organización para planificar y responder a condiciones, situaciones y eventos con el fin de que las operaciones continúen a un nivel aceptable predefinido. *(Fuente: ISO 22.300:)*

247. Continuidad De La Seguridad De La Información:

Procesos y procedimientos para asegurar la continuidad de las actividades relacionadas con la seguridad de la información. *(Fuente: ISO 27.000:)*

248. Continuidad Del Negocio:

Capacidad de una organización para continuar la entrega/prestación de productos o servicios a niveles predefinidos aceptables después de una disrupción. *(Fuente: ISO 22.300:)*

249. Continuo Del Uso De La Fuerza:

Aumento o disminución del nivel de fuerza aplicado como un continuo en relación con la respuesta del adversario, usando la cantidad de fuerza razonable y necesaria. *(Fuente: ISO 22.300:)*

250. Contrainteligencia:

Monitoreo de otras organizaciones competidoras o naciones para recopilar información. *(Fuente: NICSS:)*

251. Contramedida:

Métodos reactivos usados para prevenir que un exploit ocurra exitosamente una vez que se ha detectado una amenaza. Los Sistemas de Prevención de Intrusiones (IPS) comúnmente emplean contramedidas para evitar que intrusos obtengan mayor acceso a una red informática. Otras contramedidas son parches, listas de control de acceso y filtros de malware. *(Fuente: SANS:)*

Medida adoptada para disminuir la probabilidad de que un escenario de amenaza para la seguridad logre sus objetivos, o para reducir las consecuencias probables de dicho escenario. *(Fuente: ISO 22.300:)*

252. Contraseña:

Una cadena de caracteres (letras, números y otros símbolos) usada para autenticar una identidad o verificar la autorización de acceso. *(Fuente: NICSS:)*

253. Contraseñas en Custodia:

Las contraseñas en custodia son contraseñas que se escriben y almacenan en un lugar seguro (como una caja fuerte) que son usadas por personal de emergencia cuando el personal privilegiado no está disponible. *(Fuente: SANS:)*

254. Contratación Externa:

Contratación de una parte externa para que satisfaga una obligación derivada de un contrato vigente. *(Fuente: ISO 22.300:)*

255. Contratar Externamente:

Establecer un acuerdo mediante el cual una organización externa realiza parte de una función o proceso de una organización. *(Fuente: ISO 22.300:)*

256. Contratar Externamente (Verbo):

Establecer un acuerdo mediante el cual una organización externa realiza parte de una función o proceso de una organización. *(Fuente: ISO 27.000:)*

257. Contrato:

Acuerdo vinculante. *(Fuente: ISO 9.000:)*

258. Control:

Medida que modifica un riesgo. *(Fuente: ISO 27.000:)*

259. Control De Acceso:

Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad. *(Fuente: ISO 27.000:)*

260. Control De Cambios:

<gestión de la configuración> Actividades para controlar las salidas después de la aprobación formal de su información sobre configuración del producto. *(Fuente: ISO 9.000:)*

261. Control De La Calidad:

Parte de la gestión de la calidad orientada al cumplimiento de los requisitos de la calidad. *(Fuente: ISO 9.000:)*

262. Control de Acceso Basado en Conjunto de Reglas (RSBAC):

El Control de Acceso Basado en Conjunto de Reglas dirige acciones basadas en reglas para entidades que operan sobre objetos. *(Fuente: SANS:)*

263. Control de Admisión de Llamadas (CAC):

La inspección y control de toda la actividad de red de voz entrante y saliente mediante un firewall de voz basado en políticas definidas por el usuario. *(Fuente: SANS:)*

264. Control de acceso:

El control de acceso garantiza que los recursos solo se otorguen a aquellos usuarios que tienen derecho a ellos. *(Fuente: SANS:)*

El proceso de conceder o denegar solicitudes específicas o intentos de: 1) obtener y usar información y servicios relacionados, y 2) ingresar a instalaciones físicas específicas. *(Fuente: NICSS:)*

265. Control de acceso basado en listas:

El control de acceso basado en listas asocia una lista de usuarios y sus privilegios con cada objeto. *(Fuente: SANS:)*

266. Control de acceso basado en roles:

El control de acceso basado en roles asigna usuarios a roles basados en sus funciones organizacionales y determina la autorización basándose en esos roles. *(Fuente: SANS:)*

267. Control de acceso basado en token:

El control de acceso basado en token asocia una lista de objetos y sus privilegios con cada usuario. (Lo opuesto al basado en lista.) *(Fuente: SANS:)*

268. Control de acceso discrecional (DAC):

El Control de Acceso Discrecional consiste en algo que el usuario puede gestionar, como una contraseña de documento. *(Fuente: SANS:)*

269. Control de acceso obligatorio (MAC):

El control de acceso obligatorio es cuando el sistema controla el acceso a los recursos basado en niveles de clasificación asignados tanto a los objetos como a los usuarios. Estos controles no pueden ser cambiados por nadie. *(Fuente: SANS:)*

270. Control supervisivo y adquisición de datos:

Nombre genérico para un sistema computarizado capaz de recolectar y procesar datos y aplicar controles operacionales a activos geográficamente dispersos a largas distancias. *(Fuente: NICSS:)*

271. Convertir en arma:

Desarrollar un exploit contra una vulnerabilidad en una herramienta de ataque que puede ser desplegada contra un objetivo. *(Fuente: NICSS:)*

272. Cookie:

Datos intercambiados entre un servidor HTTP y un navegador (cliente del servidor) para almacenar información de estado en el lado cliente y recuperarla después para uso del servidor. Un servidor HTTP, al enviar datos a un cliente, puede enviar una cookie, que el cliente retiene después de cerrar la conexión HTTP. Un servidor puede usar este mecanismo para mantener información persistente de estado del lado cliente para aplicaciones basadas en HTTP, recuperando esta información en conexiones posteriores. *(Fuente: SANS:)*

273. Cooperación:

Proceso de trabajo o actuación conjuntos por intereses y valores comunes sobre la base de un acuerdo. *(Fuente: ISO 22.300:)*

274. Coordinación:

Manera en la que organizaciones diferentes (públicas o privadas) o partes de la misma organización trabajan o actúan juntas para conseguir un objetivo común. *(Fuente: ISO 22.300:)*

275. Coordinador De Ejercicios:

Persona responsable de la planificación, la dirección y la valoración de las actividades de los ejercicios. *(Fuente: ISO 22.300:)*

276. Copia De Custodia:

Duplicado que está supeditado a la fuente autorizada. *(Fuente: ISO 22.300:)*

277. Copias de seguridad incrementales:

Las copias de seguridad incrementales solo respaldan los archivos que han sido modificados desde la última copia de seguridad. Si se usan niveles de volcado (dump levels), las copias incrementales solo respaldan archivos cambiados desde la última copia de seguridad de un nivel de volcado inferior. *(Fuente: SANS:)*

278. Corrección:

Acción para eliminar una no conformidad detectada. *(Fuente: ISO 27.000:)*

Acción para eliminar una no conformidad detectada. *(Fuente: ISO 22.300:)*

279. Corrupción:

Una acción de amenaza que altera indeseablemente la operación del sistema modificando negativamente funciones o datos del sistema. *(Fuente: SANS:)*

280. Cortafuegos:

Dispositivo de hardware/software o programa que limita el tráfico de red según un conjunto de reglas sobre qué acceso está permitido o autorizado. *(Fuente: NICSS:)*

281. Cortafuegos personales:

Los cortafuegos personales son aquellos que se instalan y ejecutan en computadoras individuales. *(Fuente: SANS:)*

282. Crimeware:

Un tipo de malware usado por ciberdelincuentes. El malware está diseñado para permitir al ciberdelincuente ganar dinero con el sistema infectado (como recolectando pulsaciones de teclas, usando los sistemas infectados para lanzar ataques de denegación de servicio, etc.). *(Fuente: SANS:)*

283. Cripto-malware:

Tipo de malware que cifra los datos del dispositivo víctima y exige un rescate para restaurarlos. *(Fuente: NICSS:)*

284. Criptoanálisis:

Estudio de técnicas matemáticas para intentar romper o eludir métodos criptográficos y/o la seguridad de los sistemas de información. *(Fuente: NICSS:)*

La ciencia matemática que se ocupa del análisis de un sistema criptográfico para obtener el conocimiento necesario para romper o eludir la protección que el sistema está diseñado para proporcionar. En otras palabras, convertir el texto cifrado en texto plano sin conocer la clave. *(Fuente: SANS:)*

285. Criptografía:

Arte o ciencia que trata sobre los principios, medios y métodos para convertir texto plano en texto cifrado y para restaurar el texto cifrado en texto plano. *(Fuente: NICSS:)*

286. Criptografía asimétrica:

Criptografía de clave pública; una rama moderna de la criptografía en la cual los algoritmos emplean un par de claves (una pública y una privada) y usan un componente diferente del par para distintos pasos del algoritmo. *(Fuente: SANS:)*

287. Criptografía de clave pública:

Rama de la criptografía en la que un sistema o algoritmo criptográfico utiliza dos claves vinculadas de forma única: una clave pública y una privada (un par de claves). *(Fuente: NICSS:)*

288. Criptografía simétrica:

Rama de la criptografía que involucra algoritmos que usan la misma clave para dos pasos diferentes del algoritmo (como cifrado y descifrado, o creación y verificación de firma). La criptografía simétrica a veces se llama "criptografía de clave secreta" (en contraste con la criptografía de clave pública) porque las entidades comparten la clave. *(Fuente: SANS:)*

Una rama de la criptografía en la que un sistema o algoritmos criptográficos usan la misma clave secreta (una clave secreta compartida). *(Fuente: NICSS:)*

289. Criptología:

Ciencia matemática que abarca el criptoanálisis y la criptografía. *(Fuente: NICSS:)*

290. Criptomineros:

Amenaza en línea que se oculta en un dispositivo y utiliza sus recursos para minar criptomonedas. *(Fuente: NICSS:)*

291. Criptomoneda:

Moneda digital en la que las transacciones se verifican y los registros se mantienen mediante un sistema descentralizado que utiliza criptografía, en lugar de una autoridad central. *(Fuente: NICSS:)*

292. Crisis:

Situación inestable que implica un cambio abrupto o sustancial inminente que exige una atención y acciones urgentes para proteger la vida, los activos, los bienes o el medio ambiente. *(Fuente: ISO 22.300:)*

293. Criterios De Auditoría:

Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia objetiva. *(Fuente: ISO 9.000:)*

294. Criterios De Decisión:

Umbrales, objetivos o patrones que se utilizan para determinar la necesidad de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado. *(Fuente: ISO 27.000:)*

295. Criterios De Riesgo:

Términos de referencia respecto a los que se evalúa la importancia de un riesgo. *(Fuente: ISO 22.300:)*

Términos de referencia respecto a los que se evalúa la importancia de un riesgo. *(Fuente: ISO 27.000:)*

296. Cron:

Cron es una aplicación Unix que ejecuta trabajos para usuarios y administradores en horarios programados del día. *(Fuente: SANS:)*

297. Cryptojacking:

Tipo de ciberdelito que consiste en el uso no autorizado de dispositivos (computadoras, teléfonos, tabletas o servidores) para minar criptomonedas. *(Fuente: NICSS:)*

298. Cumplimiento del aseguramiento de la información:

En el marco NICE, trabajo de ciberseguridad donde una persona: supervisa, evalúa y apoya los procesos de documentación, validación y acreditación necesarios para asegurar que los nuevos sistemas de TI cumplan con los requisitos de aseguramiento de la información y seguridad de la organización, asegurando un tratamiento adecuado del riesgo, cumplimiento y aseguramiento desde perspectivas internas y externas. *(Fuente: NICSS:)*

299. Custodia:

Periodo de tiempo durante el que una organización en la cadena de suministro controla directamente la fabricación, la manipulación, el procesado y el transporte de bienes y su información de expedición pertinente en la cadena de suministro. *(Fuente: ISO 22.300:)*

300. Custodio de datos:

Un Custodio de datos es la entidad que actualmente está utilizando o manipulando los datos y, por lo tanto, asume temporalmente la responsabilidad de los datos. *(Fuente: SANS:)*

301. Cut-Through:

Cut-Through es un método de conmutación donde sólo se lee el encabezado de un paquete antes de ser enviado a su destino. *(Fuente: SANS:)*

302. Célula:

Una célula es una unidad de datos transmitida a través de una red ATM. *(Fuente: SANS:)*

303. Código De Colores:

Conjunto de colores usados de manera simbólica para denotar unos significados específicos. *(Fuente: ISO 22.300:)*

304. Código De Conducta De La Satisfacción Del Cliente:

Promesas hechas a los clientes por una organización relacionadas con su comportamiento, orientadas a aumentar la satisfacción del cliente y las disposiciones relacionadas. *(Fuente: ISO 9.000:)*

305. Código malicioso:

Software (p. ej., caballo de Troya) que parece realizar una función útil o deseable, pero en realidad obtiene acceso no autorizado a los recursos del sistema o engaña a un usuario para ejecutar otra lógica maliciosa. *(Fuente: SANS:)*

Incluye software, firmware y scripts. *(Fuente: NICSS:)*

— D —

306. DBaaS (Base de Datos como Servicio):

una oferta de base de datos en la nube que proporciona a los clientes acceso a una base de datos sin tener que implementar ni gestionar la infraestructura subyacente. *(Fuente: NICSS:)*

307. DDoS (Denegación de Servicio Distribuida):

un delito cibernético en el que el atacante satura un objetivo con tráfico de Internet para impedir que los usuarios accedan a servicios y sitios en línea conectados. *(Fuente: NICSS:)*

308. DNSTwist:

Genera una lista de nombres de dominio visualmente similares a un dominio dado y realiza consultas DNS sobre ellos (A, AAAA, NS y MX), lo cual puede usarse para interceptar tráfico mal dirigido. *(Fuente: NICSS:)*

309. DPIA:

Las DPIA son herramientas importantes para mitigar riesgos y demostrar cumplimiento con el RGPD. *(Fuente: NICSS:)*

310. Daltonismo:

Incapacidad total o parcial de una persona para diferenciar entre ciertas tonalidades. *(Fuente: ISO 22.300:)*

311. DataOps:

una práctica colaborativa de gestión de datos enfocada en mejorar la comunicación, integración y automatización de los flujos de datos entre los gestores de datos y los consumidores de datos en toda una organización *(Fuente: NICSS:)*

312. Datagrama:

El RFC 1594 dice: "una entidad de datos autónoma e independiente que lleva suficiente información para ser enviada desde el origen al computador de destino sin depender de intercambios previos entre este origen y destino ni de la red de transporte." El término ha sido reemplazado generalmente por el término paquete. Los datagramas o paquetes son las unidades de mensaje con las que trata el Protocolo de Internet y que transporta Internet. Un datagrama o paquete debe ser autónomo y no depender de intercambios previos porque no existe una conexión de duración fija entre los dos puntos de comunicación como ocurre, por ejemplo, en la mayoría de las conversaciones telefónicas de voz. (Este tipo de protocolo se denomina no orientado a conexión.) *(Fuente: SANS:)*

313. Datos:

Hechos sobre un objeto. *(Fuente: ISO 9.000:)*

Conjunto de valores asociados a medidas básicas, medidas derivadas y/o indicadores. *(Fuente: ISO 27.000:)*

314. Debilidad:

Una deficiencia o imperfección en código de software, diseño, arquitectura o despliegue que, bajo condiciones adecuadas, podría convertirse en una vulnerabilidad o contribuir a la introducción de vulnerabilidades. *(Fuente: NICSS:)*

315. Declaración De Seguridad:

Compromiso documentado adquirido por un socio comercial, que especifica las medidas de seguridad que este ha implemento, incluyendo, como mínimo, la manera en la que se protegen los bienes y los instrumentos físicos de comercio internacional, así como la información asociada, y se demuestran y verifican las medidas de seguridad. *(Fuente: ISO 22.300:)*

316. Decodificar:

Convertir texto codificado a texto plano mediante un código. *(Fuente: NICSS:)*

317. Deepfake:

medios sintéticos que han sido manipulados digitalmente para reemplazar de forma convincente la apariencia de una persona con la de otra. *(Fuente: NICSS:)*

318. Defecto:

No conformidad relativa a un uso previsto o especificado. *(Fuente: ISO 9.000:)*

319. Defensa de objetivo móvil:

La presentación de una superficie de ataque dinámica, aumentando el factor de trabajo necesario para que un adversario pueda sondear, atacar o mantener presencia en un objetivo cibernético. *(Fuente: NICSS:)*

320. Defensa de redes informáticas:

Acciones tomadas para defenderse de actividades no autorizadas dentro de redes informáticas. *(Fuente: NICSS:)*

321. Defensa en profundidad:

La defensa en profundidad es el enfoque de usar múltiples capas de seguridad para proteger contra la falla de un solo componente de seguridad. *(Fuente: SANS:)*

322. Demonio:

Un programa que a menudo se inicia en el arranque del sistema y corre continuamente sin intervención de ninguno de los usuarios en el sistema. El programa demonio envía las solicitudes a otros programas (o procesos) según corresponda. El término demonio es un término Unix, aunque muchos otros sistemas operativos proveen soporte para demonios, aunque a veces se les llama con otros nombres. Windows, por ejemplo, se refiere a demonios como Agentes del Sistema y servicios. *(Fuente: SANS:)*

323. Denegación de servicio:

La prevención del acceso autorizado a un recurso del sistema o el retraso en las operaciones y funciones del sistema. *(Fuente: SANS:)*

Un ataque que impide o afecta el uso autorizado de los recursos o servicios de un sistema de información. *(Fuente: NICSS:)*

324. Denegación de servicio distribuida:

Una técnica de denegación de servicio que utiliza numerosos sistemas para realizar el ataque simultáneamente. *(Fuente: NICSS:)*

325. Des-perimetrización:

una estrategia de seguridad de la información que fortalece la postura de seguridad de una organización mediante la implementación de múltiples niveles de protección, incluidos sistemas y protocolos informáticos inherentemente seguros, cifrado de alto nivel y autenticación. *(Fuente: NICSS:)*

326. Desarrollo de sistemas:

En el marco NICE, trabajo en ciberseguridad donde una persona: trabaja en las fases de desarrollo del ciclo de vida del desarrollo de sistemas. *(Fuente: NICSS:)*

327. Desastre:

Situación en la que se han producido pérdidas humanas, materiales, económicas o medioambientales generalizadas, que exceden la capacidad de la organización, comunidad o sociedad afectada para responder y recuperarse utilizando sus propios recursos. *(Fuente: ISO 22.300:)*

328. Desastre natural:

Cualquier "acto de Dios" (por ejemplo, incendio, inundación, terremoto, rayo o viento) que inhabilita un componente del sistema. *(Fuente: SANS:)*

329. Desautenticación:

Un ataque de desautenticación es un tipo de ataque de denegación de servicio (DoS) y se refiere a la interrupción no autorizada de la conexión entre un dispositivo inalámbrico y su punto de acceso. *(Fuente: NICSS:)*

330. Desbordamiento de búfer:

Un desbordamiento de búfer ocurre cuando un programa o proceso intenta almacenar más datos en un búfer (área de almacenamiento temporal) de lo que se pretendía contener. Como los búferes se crean para contener una cantidad finita de datos, la información extra –que tiene que ir a algún lugar– puede desbordarse hacia búferes adyacentes, corrompiendo o sobrescribiendo los datos válidos que contienen. *(Fuente: SANS:)*

331. Descifrado:

El descifrado es el proceso de transformar un mensaje cifrado en su texto plano original. *(Fuente: SANS:)*

332. Descifrar:

Convertir texto cifrado a texto plano mediante un sistema criptográfico. *(Fuente: NICSS:)*

333. Desecho:

Acción tomada sobre un producto o servicio no conforme para impedir su uso inicialmente previsto. *(Fuente: ISO 9.000:)*

334. Desempeño:

Resultado medible. *(Fuente: ISO 27.000:)*

Resultado medible. *(Fuente: ISO 22.300:)*

335. Desencapsulación:

La desencapsulación es el proceso de eliminar las cabeceras de una capa y pasar el resto del paquete a la siguiente capa superior en la pila de protocolos. *(Fuente: SANS:)*

336. Desencriptación:

El proceso de convertir datos cifrados de nuevo a su forma original, para que puedan ser comprendidos. *(Fuente: NICSS:)*

337. Desencriptador:

Una herramienta, o conjunto de herramientas, utilizada para desencriptar archivos cifrados. Puede utilizarse con fines de recuperación o para combatir el ransomware. *(Fuente: NICSS:)*

338. Desencriptar:

Término genérico que abarca decodificar y descifrar. *(Fuente: NICSS:)*

339. Desensamblado:

El proceso de tomar un programa binario y derivar el código fuente a partir de él. *(Fuente: SANS:)*

340. Desfiguración:

La desfiguración es el método de modificar el contenido de un sitio web de tal manera que se convierte en "vandalizado" o vergonzoso para el propietario del sitio. *(Fuente: SANS:)*

341. Desinformadores:

Persona que propaga desinformación. *(Fuente: NICSS:)*

342. Desplazamiento de fragmento:

El campo de desplazamiento de fragmento indica al emisor dónde se encuentra un fragmento particular en relación con otros fragmentos del paquete original más grande. *(Fuente: SANS:)*

343. Detección de intrusiones:

El proceso y métodos para analizar información de redes y sistemas de información para determinar si ha ocurrido una brecha o violación de seguridad. *(Fuente: NICSS:)*

344. Detección de intrusos:

Un sistema de gestión de seguridad para computadoras y redes. Un IDS recopila y analiza información de varias áreas dentro de una computadora o red para identificar posibles violaciones de seguridad, que incluyen tanto intrusiones (ataques desde fuera de la organización) como abusos (ataques desde dentro de la organización). *(Fuente: SANS:)*

345. Determinación:

Actividad para encontrar una o más características y sus valores característicos. *(Fuente: ISO 9.000:)*

346. DevOps:

la combinación de filosofías culturales, prácticas y herramientas que aumentan la capacidad de una organización para entregar aplicaciones y servicios. *(Fuente: NICSS:)*

347. DevSecOps:

un enfoque de cultura, automatización y diseño de plataformas que integra la seguridad como una responsabilidad compartida a lo largo de todo el ciclo de vida de TI. *(Fuente: NICSS:)*

348. Diffie-Hellman:

Un algoritmo de intercambio de claves publicado en 1976 por Whitfield Diffie y Martin Hellman. Diffie-Hellman establece claves, no cifra. Sin embargo, la clave que produce puede

usarse para cifrado, para otras operaciones de gestión de claves o para cualquier otra criptografía. *(Fuente: SANS:)*

349. Difusión:

Enviar simultáneamente el mismo mensaje a múltiples destinatarios. Un host a todos los hosts de la red. *(Fuente: SANS:)*

350. Diligencia Debida:

La diligencia debida asegura que un nivel mínimo de protección esté implementado de acuerdo con las mejores prácticas de la industria. *(Fuente: SANS:)*

La diligencia debida es el requisito de que las organizaciones deben desarrollar e implementar un plan de protección para prevenir fraudes, abusos, y además desplegar un medio para detectarlos si ocurren. *(Fuente: SANS:)*

351. Direccionamiento privado:

IANA ha reservado tres rangos de direcciones para el uso de redes privadas o no conectadas a Internet. Esto se denomina espacio de direcciones privadas y está definido en RFC 1918. Los bloques reservados son: 10.0.0.0 a 10.255.255.255 (prefijo 10/8), 172.16.0.0 a 172.31.255.255 (prefijo 172.16/12), 192.168.0.0 a 192.168.255.255 (prefijo 192.168/16). *(Fuente: SANS:)*

352. Dirección Ejecutiva:

Persona o grupo de personas en la(s) que los órganos de gobierno han delegado la responsabilidad de implementar estrategias y políticas para alcanzar la misión de la organización. *(Fuente: ISO 27.000:)*

353. Dirección IP:

La dirección inter-red de una computadora asignada para uso del Protocolo de Internet y otros protocolos. Una dirección IP versión 4 se escribe como una serie de cuatro números de 8 bits separados por puntos. *(Fuente: SANS:)*

354. Dirección MAC:

Una dirección física; un valor numérico que identifica de manera única ese dispositivo de red entre todos los demás dispositivos en el planeta. *(Fuente: SANS:)*

355. Dirección Operativa De Incidentes:

Proceso que se lleva a cabo como parte de un sistema de gestión de incidentes, y que evoluciona durante la gestión de un incidente. *(Fuente: ISO 22.300:)*

356. Dirección de difusión:

Una dirección utilizada para difundir un datagrama a todos los hosts en una red dada usando el protocolo UDP o ICMP. *(Fuente: SANS:)*

357. Dirección de loopback:

La dirección de loopback (127.0.0.1) es una dirección IP falsa que siempre se refiere de vuelta al host local y nunca se envía a una red. *(Fuente: SANS:)*

358. Diseño Y Desarrollo:

Conjunto de procesos que transforman los requisitos para un objeto en requisitos más detallados para ese objeto. *(Fuente: ISO 9.000:)*

359. Disponibilidad:

Propiedad de la información de ser accesible y utilizable por una entidad autorizada. *(Fuente: UNE 71.505:)*

En ciberseguridad, se refiere a activos como la información o los sistemas de información. *(Fuente: NICSS:)*

La disponibilidad es la necesidad de garantizar que el propósito empresarial del sistema se pueda cumplir y que esté accesible para quienes necesitan usarlo. *(Fuente: SANS:)*

Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada. *(Fuente: ISO 27.000:)*

360. Dispositivos basados en token:

Un dispositivo basado en token se activa según la hora del día, por lo que cada minuto la contraseña cambia, requiriendo que el usuario tenga el token consigo al iniciar sesión. *(Fuente: SANS:)*

361. Disrupción:

Evento, ya sea esperado (por ejemplo, una huelga laboral o un huracán) o inesperado (por ejemplo, un apagón o un terremoto), que provoca una desviación negativa no planificada de la entrega/prestación prevista de productos o servicios según los objetivos de una organización. *(Fuente: ISO 22.300:)*

362. Distribuciones (Distros):

Una distribución de Linux es un sistema operativo compuesto por una colección de software que incluye el núcleo de Linux y, a menudo, un sistema de gestión de paquetes. *(Fuente: NICSS:)*

363. Documento:

Información y el medio en el que está contenida. *(Fuente: ISO 22.300:)*

364. Documento Electrónico:

Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. *(Fuente: UNE 71.505:)*

365. Dominio:

Una esfera de conocimiento, o una colección de hechos sobre algunas entidades de programa o un número de puntos o direcciones de red, identificados por un nombre. En Internet, un dominio consiste en un conjunto de direcciones de red. En el sistema de nombres de dominio de Internet, un dominio es un nombre con el que se asocian registros de servidores de nombres que describen subdominios u host. En Windows NT y Windows 2000, un dominio es un conjunto de recursos de red (aplicaciones, impresoras, etc.) para un grupo de usuarios.

El usuario solo necesita iniciar sesión en el dominio para acceder a los recursos, que pueden estar ubicados en varios servidores de la red. *(Fuente: SANS:)*

366. Dorking:

Uso de técnicas de búsqueda para hackear sitios vulnerables o buscar información que no está disponible en resultados públicos de búsqueda. *(Fuente: NICSS:)*

367. Dueño Del Riesgo:

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. *(Fuente: ISO 27.000:)*

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. *(Fuente: ISO 22.300:)*

368. DumpSec:

DumpSec es una herramienta de seguridad que extrae una variedad de información sobre los usuarios de un sistema, sistema de archivos, registro, permisos, política de contraseñas y servicios. *(Fuente: SANS:)*

369. Duración Máxima De Interrupción Aceptable; Mao:

Tiempo que tardarían los impactos adversos, que pudieran derivarse de no entregar un producto, prestar un servicio o realizar una actividad en volverse inaceptables. *(Fuente: ISO 22.300:)*

370. Día Cero:

El "Día Cero" o "Zero Day" es el día en que se da a conocer una nueva vulnerabilidad. En algunos casos, una explotación "zero day" se refiere a una para la cual aún no hay un parche disponible. ("día uno" -> día en que el parche está disponible). *(Fuente: SANS:)*

371. Día cero:

El "Día Cero" es el día en que se da a conocer una nueva vulnerabilidad. En algunos casos, un exploit de "día cero" se refiere a un exploit para el cual aún no existe un parche disponible. ("Día uno" es el día en que el parche se hace disponible). *(Fuente: SANS:)*

372. Dúplex completo:

Un tipo de canal de comunicación dúplex que transmite datos en ambas direcciones a la vez. Se refiere a la transmisión de datos en dos direcciones simultáneamente. Comunicación en la que tanto emisor como receptor pueden enviar datos al mismo tiempo. *(Fuente: SANS:)*

— E —

373. ENISA:

Establecida en 2004 y reforzada por la Ley de Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política cibernética de la UE, mejora la confiabilidad de productos, servicios y procesos TIC con esquemas de certificación en ciberseguridad, coopera con los Estados miembros y órganos de la UE, y ayuda a Europa a prepararse para los desafíos cibernéticos del mañana. *(Fuente: NICSS:)*

374. Ecosistema cibernético:

Infraestructura de información interconectada de interacciones entre personas, procesos, datos y tecnologías de información y comunicación, junto con el entorno y condiciones que influyen en dichas interacciones. *(Fuente: NICSS:)*

375. Educación y capacitación:

En el Marco NICE, trabajo en ciberseguridad donde una persona: capacita al personal en dominios temáticos pertinentes, desarrollando, planificando, coordinando, impartiendo y/o evaluando cursos de capacitación, métodos y técnicas según corresponda. *(Fuente: NICSS:)*

376. Eficacia:

Grado en el cual se realizan las actividades planificadas y se logran los resultados planificados. *(Fuente: ISO 27.000:)*

Grado en el que se realizan las actividades planificadas y se logran los resultados planificados. *(Fuente: ISO 22.300:)*

Grado en el que se realizan las actividades planificadas y se logran los resultados planificados. *(Fuente: ISO 9.000:)*

377. Eficiencia:

Relación entre el resultado alcanzado y los recursos utilizados. *(Fuente: ISO 9.000:)*

378. Ejercicio:

Proceso para ejercitar, evaluar, poner en práctica y mejorar el desempeño de una organización. *(Fuente: ISO 22.300:)*

379. Ejercicio A Escala Natural:

Ejercicio que implica a múltiples organizaciones o funciones y que incluye actividades reales. *(Fuente: ISO 22.300:)*

380. Ejercicio Estratégico:

Ejercicio que implica a la alta dirección a nivel estratégico. *(Fuente: ISO 22.300:)*

381. Ejercicio Funcional:

Ejercicio que se realiza para adiestrar, evaluar, practicar y mejorar el desempeño de funciones individuales, diseñado para responder a un evento no deseado y recuperarse de él. *(Fuente: ISO 22.300:)*

382. Ejercicio cibernético:

Evento planificado en el que una organización simula una disrupción cibernética para desarrollar o probar capacidades como la prevención, detección, mitigación, respuesta o recuperación ante dicha disrupción. *(Fuente: NICSS:)*

383. Ejercicio de equipo rojo:

Un ejercicio que refleja condiciones del mundo real, realizado como un intento simulado por un adversario para atacar o explotar vulnerabilidades en los sistemas de información de una empresa. *(Fuente: NICSS:)*

384. Ejercicio de mesa redonda:

Un ejercicio basado en discusión donde el personal se reúne en un aula o grupos pequeños y se les presenta un escenario para validar el contenido de planes, procedimientos, políticas, acuerdos cooperativos u otra información para manejar un incidente. *(Fuente: NICSS:)*

385. Ejercicio operativo:

También referido como ejercicio basado en operaciones. *(Fuente: NICSS:)*

386. Elemento De Autenticación:

Objeto material, característica visual o información asociados a un bien material o su envase que se usa como parte de una solución de autenticación. *(Fuente: ISO 22.300:)*

387. Elemento De Autenticación Controlable Con Herramienta:

Elemento de autenticación que por lo general no perciben los sentidos humanos y que puede ser revelado por una persona con los conocimientos adecuados usando una herramienta o mediante una interpretación automatizada. *(Fuente: ISO 22.300:)*

388. Elemento De Autenticación Controlable Sin Herramienta:

Elemento de autenticación que puede ser detectado y verificado por uno o varios de los sentidos del ser humano sin recurrir a una herramienta (salvo aquellas cotidianas que corrigen defectos de los sentidos, como gafas o audífonos). *(Fuente: ISO 22.300:)*

389. Elemento De Autenticación Integrado:

Elemento de autenticación que se incorpora al bien material. *(Fuente: ISO 22.300:)*

390. Elemento De Autenticación Intrínsico:

Elemento de autenticación que es inherente al bien material. *(Fuente: ISO 22.300:)*

391. Emergencia:

Hecho o evento repentino, urgente y normalmente inesperado que requiere actuar de inmediato. *(Fuente: ISO 22.300:)*

392. Empresa Prestadora De Servicios De Seguridad Privada; Empresa De Seguridad Privada; Psc:

Organización que lleva a cabo o subcontrata operaciones de seguridad y cuya actividad empresarial incluye la prestación de servicios de seguridad ya sea en su nombre o en nombre de otros. *(Fuente: ISO 22.300:)*

393. Encabezado:

Un encabezado es la información extra en un paquete que es necesaria para que la pila de protocolos procese el paquete. *(Fuente: SANS:)*

394. Encapsulación:

La inclusión de una estructura de datos dentro de otra estructura de modo que la primera estructura de datos esté oculta por el momento. *(Fuente: SANS:)*

395. Endurecimiento:

El endurecimiento es el proceso de identificar y corregir vulnerabilidades en un sistema. *(Fuente: SANS:)*

396. Enlace simbólico (Symlink):

Un enlace simbólico en Linux/UNIX que apunta a otro archivo o carpeta en tu computadora o en un sistema de archivos conectado. Windows tiene una funcionalidad similar llamada acceso directo (Shortcut). *(Fuente: NICSS:)*

397. Enlaces simbólicos:

Archivos especiales que apuntan a otro archivo. *(Fuente: SANS:)*

398. Enrutamiento Estático:

El enrutamiento estático significa que las entradas en la tabla de enrutamiento contienen información que no cambia. *(Fuente: SANS:)*

399. Ensayo:

Tipo de ejercicio único y específico, que incluye la expectativa de un elemento de pasa/no pasa en el propósito o los objetivos del ejercicio que se está planificando. *(Fuente: ISO 22.300:)*

Determinación de acuerdo con los requisitos para un uso o aplicación previsto específico. *(Fuente: ISO 9.000:)*

400. Ensayos:

Procedimiento para la valoración; medio de determinar la presencia, calidad o veracidad de algo. *(Fuente: ISO 22.300:)*

401. Entidad:

Algo que tiene una existencia independiente y diferenciada y que se puede identificar en un contexto. *(Fuente: ISO 22.300:)*

402. Entidad De Confianza Para La Comunicación De Información:

Organización independiente que sustenta el intercambio de información dentro de un colectivo que comparte información. *(Fuente: ISO 27.000:)*

403. Envenenamiento de caché:

Datos maliciosos o engañosos de un servidor de nombres remoto son guardados [en caché] por otro servidor de nombres. Se utiliza típicamente en ataques de envenenamiento de caché DNS. *(Fuente: SANS:)*

404. Envenenamiento inverso:

El horizonte dividido con envenenamiento inverso (más simplemente, envenenamiento inverso) incluye esas rutas en las actualizaciones, pero establece sus métricas a infinito. En efecto, anuncia que esas rutas no son alcanzables. *(Fuente: SANS:)*

405. Equipo Auditor:

Una o más personas que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos. *(Fuente: ISO 9.000:)*

406. Equipo Azul:

Las personas que realizan tareas de ciberseguridad defensiva, incluyendo colocar y configurar firewalls, implementar programas de parches, aplicar autenticación fuerte, asegurar que las medidas de seguridad física sean adecuadas y una larga lista de actividades similares. *(Fuente: SANS:)*

407. Equipo De Gestión De Crisis:

Grupo de personas que son funcionalmente responsables de dirigir y llevar a cabo la ejecución de la respuesta y el plan de continuidad de las operaciones, de declarar una disrupción de las operaciones o una situación de emergencia/crisis, y de marcar la dirección a seguir durante el proceso de recuperación, tanto antes como después del incidente disruptivo. *(Fuente: ISO 22.300:)*

408. Equipo De Medición:

Instrumento de medición, software, patrón de medición, material de referencia o equipos auxiliares o combinación de ellos necesarios para llevar a cabo un proceso de medición. *(Fuente: ISO 9.000:)*

409. Equipo De Proyecto De Ejercicios:

Persona responsable de la planificación, la dirección y la valoración de un proyecto de ejercicios. *(Fuente: ISO 22.300:)*

410. Equipo De Respuesta:

Grupo de personas responsable de desarrollar, ejecutar, probar y mantener el plan de respuesta, incluidos sus procesos y procedimientos. *(Fuente: ISO 22.300:)*

411. Equipo azul:

También, grupo que realiza evaluaciones operativas de vulnerabilidades y recomienda técnicas de mitigación a clientes que requieren revisión técnica independiente de su postura de ciberseguridad. *(Fuente: NICSS:)*

412. Equipo blanco:

Grupo responsable de arbitrar un enfrentamiento entre un Equipo Rojo (atacantes simulados) y un Equipo Azul (defensores reales de sistemas de información). *(Fuente: NICSS:)*

413. Equipo de respuesta a emergencias informáticas (CERT):

Una organización que estudia INFOSEC de computadoras y redes para proveer servicios de respuesta a incidentes a víctimas de ataques, publicar alertas sobre vulnerabilidades y amenazas, y ofrecer otra información para ayudar a mejorar la seguridad informática y de redes. *(Fuente: SANS:)*

414. Equipo rojo:

Un grupo autorizado y organizado para emular las capacidades de ataque o explotación de un adversario potencial contra la postura de ciberseguridad de una empresa. *(Fuente: NICSS:)*

415. Error:

Defecto, falla o imperfección inesperada y relativamente pequeña en un sistema de información o dispositivo. *(Fuente: NICSS:)*

416. Escala:

Conjunto ordenado de valores, continuo o discreto, o un conjunto de categorías a las que se asigna el atributo. *(Fuente: ISO 27.000:)*

417. Escaneo Ping:

Un escaneo ping busca máquinas que responden a solicitudes ICMP Echo. *(Fuente: SANS:)*

418. Escaneo TCP Full Open:

El escaneo TCP Full Open verifica cada puerto realizando un apretón de manos completo (three-way handshake) para determinar si está abierto. *(Fuente: SANS:)*

419. Escaneo TCP Half Open:

El escaneo TCP Half Open funciona realizando la primera mitad de un three-way handshake para determinar si un puerto está abierto. *(Fuente: SANS:)*

420. Escaneo UDP:

Los escaneos UDP realizan escaneos para determinar qué puertos UDP están abiertos. *(Fuente: SANS:)*

421. Escaneo de puertos:

Un escaneo de puertos es una serie de mensajes enviados por alguien que intenta entrar en una computadora para saber qué servicios de red ofrece la computadora, cada uno asociado con un número de puerto "bien conocido". El escaneo de puertos, un enfoque favorito de los crackers, da al atacante una idea de dónde buscar vulnerabilidades. Esencialmente, un escaneo de puertos consiste en enviar un mensaje a cada puerto, uno a la vez. El tipo de respuesta indica si el puerto está en uso y por lo tanto puede ser examinado en busca de debilidades. *(Fuente: SANS:)*

422. Escaneos Distribuidos:

Los escaneos distribuidos son escaneos que utilizan múltiples direcciones de origen para recopilar información. *(Fuente: SANS:)*

423. Escaneos RPC:

Los escaneos RPC determinan qué servicios RPC están funcionando en una máquina. *(Fuente: SANS:)*

424. Escenario:

Argumento planificado de antemano que actúa como hilo conductor de un ejercicio, así como de estímulo utilizado para conseguir los objetivos de desempeño de un proyecto de ejercicios. *(Fuente: ISO 22.300:)*

425. Escenario De Amenaza Para La Seguridad:

Medio por el que puede producirse un incidente potencial de seguridad. *(Fuente: ISO 22.300:)*

426. Escucha Ilegal:

Escucha ilegal es simplemente escuchar una conversación privada que puede revelar información que puede proporcionar acceso a una instalación o red. *(Fuente: SANS:)*

427. Escucha Pasiva (Sniffing):

Sinónimo de "intercepción pasiva". *(Fuente: SANS:)*

428. Espacio confiable personalizado:

Un entorno cibernético que proporciona al usuario confianza en su seguridad, usando mecanismos automatizados para determinar las condiciones de seguridad y ajustar el nivel de seguridad basado en el contexto del usuario y frente a una gama cambiante de amenazas. *(Fuente: NICSS:)*

429. Especificación:

Documento que establece requisitos. *(Fuente: ISO 9.000:)*

430. Especificador:

Entidad que define los requisitos para que se aplique una solución de autenticación a un bien material determinado. *(Fuente: ISO 22.300:)*

431. Estado de enlace:

Con estado de enlace, las rutas mantienen información sobre todos los routers y enlaces entre routers dentro de un área geográfica, y crean una tabla de las mejores rutas con esa información. *(Fuente: SANS:)*

432. Esteganalisis:

El esteganalisis es el proceso de detectar y derrotar el uso de la esteganografía. *(Fuente: SANS:)*

433. Esteganografía:

Métodos para ocultar la existencia de un mensaje u otros datos. Esto es diferente de la criptografía, que oculta el significado de un mensaje pero no el mensaje mismo. Un ejemplo de método esteganográfico es la tinta "invisible". *(Fuente: SANS:)*

434. Estrategia:

Plan para lograr un objetivo a largo plazo o global. *(Fuente: ISO 9.000:)*

435. Estructura Lógica:

Configuración de los datos para optimizar su acceso y procesado por parte de un usuario dado (ya sea una persona o una máquina). *(Fuente: ISO 22.300:)*

436. Estándar de Internet:

Una especificación, aprobada por el IESG y publicada como RFC, que es estable y bien comprendida, técnicamente competente, tiene múltiples implementaciones independientes e interoperables con experiencia operativa sustancial, cuenta con apoyo público significativo y es reconocidamente útil en alguna o todas las partes de Internet. *(Fuente: SANS:)*

437. Estándar de cifrado avanzado (AES):

Un estándar de cifrado desarrollado por NIST. Está destinado a especificar un algoritmo de cifrado simétrico no clasificado y públicamente divulgado. *(Fuente: SANS:)*

438. Estándar de cifrado de datos (DES):

Un método de cifrado de datos ampliamente utilizado que usa una clave privada (secreta). Hay 72.000.000.000.000.000 (72 cuatrillones) o más claves de cifrado posibles que se pueden usar. Para cada mensaje dado, la clave se elige al azar entre este enorme número de claves. Como otros métodos criptográficos de clave privada, tanto el emisor como el receptor deben conocer y usar la misma clave privada. *(Fuente: SANS:)*

439. Estándar de firma digital (DSS):

Estándar del gobierno de EE. UU. que especifica el Algoritmo de Firma Digital (DSA), que implica criptografía asimétrica. *(Fuente: SANS:)*

440. Estímulo:

El estímulo es el tráfico de red que inicia una conexión o solicita una respuesta. *(Fuente: SANS:)*

441. Ethernet:

La tecnología LAN más ampliamente instalada. Especificada en un estándar, IEEE 802.3, una LAN Ethernet típicamente usa cable coaxial o cables de par trenzado especiales. Los dispositivos están conectados al cable y compiten por acceso usando un protocolo CSMA/CD. *(Fuente: SANS:)*

442. Evacuación:

Dispersión organizada, escalonada y supervisada de personas que se encuentren en zonas peligrosas o potencialmente peligrosas hacia lugares seguros. *(Fuente: ISO 22.300:)*

443. Evaluación Del Avance:

<gestión de proyectos> Evaluación del progreso en el logro de los objetivos del proyecto. *(Fuente: ISO 9.000:)*

444. Evaluación Del Desempeño:

Proceso para determinar resultados medibles. *(Fuente: ISO 22.300:)*

445. Evaluación Del Riesgo:

Proceso de comparación de los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables. *(Fuente: ISO 27.000:)*

446. Evaluación Del Riesgo (Preferido); Apreciación Del Riesgo (Desaconsejado):

Proceso global que comprende la identificación de riesgos, el análisis del riesgo y la valoración del riesgo. *(Fuente: ISO 22.300:)*

447. Evaluación de Amenazas:

La evaluación de amenazas es la identificación de tipos de amenazas a las que una organización podría estar expuesta. *(Fuente: SANS:)*

448. Evaluación de Riesgo de Ciberseguridad:

Una evaluación de riesgo de ciberseguridad es el proceso sistemático de identificar, analizar y evaluar amenazas potenciales, vulnerabilidades e impactos a los activos digitales de una organización. *(Fuente: SANS:)*

449. Evaluación de amenazas:

El producto o proceso de identificar o evaluar entidades, acciones o sucesos, ya sean naturales o provocados por el hombre, que tienen o indican potencial para dañar la vida, información, operaciones y/o propiedad. *(Fuente: NICSS:)*

450. Evaluación de riesgos:

Evaluación de los riesgos que enfrenta una entidad, activo, sistema o red, operaciones organizacionales, individuos, área geográfica, otras organizaciones o sociedad, e incluye determinar hasta qué punto las circunstancias adversas o eventos podrían resultar en consecuencias dañinas. *(Fuente: NICSS:)*

Una evaluación de riesgos es el proceso mediante el cual se identifican riesgos y se determina el impacto de esos riesgos. *(Fuente: SANS:)*

451. Evaluación y gestión de vulnerabilidades:

En el marco NICE, trabajo en ciberseguridad donde una persona: realiza evaluaciones de amenazas y vulnerabilidades, determina desviaciones de configuraciones aceptables, políticas locales o empresariales, evalúa el nivel de riesgo y desarrolla y/o recomienda contramedidas adecuadas de mitigación en situaciones operativas y no operativas. *(Fuente: NICSS:)*

452. Evento:

Ocurrencia o cambio de un conjunto particular de circunstancias. *(Fuente: ISO 27.000:)*

Un evento es una ocurrencia observable en un sistema o red. *(Fuente: SANS:)*

A veces proporciona una indicación de que está ocurriendo un incidente o al menos genera sospechas de que podría estar ocurriendo. *(Fuente: NICSS:)*

453. Evento (Preferido); Suceso (Desaconsejado):

Ocurrencia o cambio de un conjunto particular de circunstancias. *(Fuente: ISO 22.300:)*

454. Evento De Seguridad De La Información:

Ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación hasta ahora desconocida y que puede ser relevante para la seguridad. *(Fuente: UNE 71.505:)*

455. Evento Indeseable:

Suceso o cambio que tiene el potencial de provocar víctimas mortales, daños a activos materiales e inmateriales o un impacto negativo en los derechos humanos y las libertades fundamentales de partes interesadas internas o externas. *(Fuente: ISO 22.300:)*

456. Evento O Suceso De Seguridad De La Información:

Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles, o una situación desconocida hasta el momento y que puede ser relevante para la seguridad. *(Fuente: ISO 27.000:)*

457. Evidencia:

Cualquier dato o información que puede ser utilizado para determinar la existencia o no de un hecho. *(Fuente: UNE 71.505:)*

458. Evidencia De Falsificación:

Capacidad del elemento de autenticación de mostrar que la autenticidad del bien material se ha visto comprometida. *(Fuente: ISO 22.300:)*

459. Evidencia De La Auditoría:

Registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que es verificable. *(Fuente: ISO 9.000:)*

460. Evidencia Electrónica:

Información en forma electrónica de cualquier naturaleza, identificable y susceptible de ser tratada de manera diferenciada, y generada, tratada, gestionada y/o almacenada de manera que se asegura su confiabilidad y valor probatorio. *(Fuente: UNE 71.505:)*

461. Evidencia Objetiva:

Datos que respaldan la existencia o veracidad de algo. *(Fuente: ISO 9.000:)*

462. Exfiltración:

Transferencia no autorizada de información desde un sistema de información. *(Fuente: NICSS:)*

463. Experto Técnico:

<auditoría> Persona que aporta conocimientos o experiencia específicos al equipo auditor. *(Fuente: ISO 9.000:)*

464. Exploit:

Técnica para violar la seguridad de una red o sistema de información infringiendo la política de seguridad. *(Fuente: NICSS:)*

465. Exploit de día cero:

Un exploit de día cero se refiere a un ciberataque que aprovecha una vulnerabilidad en software, hardware o firmware que es desconocida para el proveedor o el público. *(Fuente: SANS:)*

466. Exposición:

Una acción de amenaza por la cual datos sensibles son directamente liberados a una entidad no autorizada. *(Fuente: SANS:)*

Condición de estar desprotegido, permitiendo así el acceso a información o capacidades que un atacante puede usar para ingresar a un sistema o red. *(Fuente: NICSS:)*

— F —

467. FaaS:

Servicio de computación en la nube que permite a los clientes ejecutar código en respuesta a eventos, sin gestionar la infraestructura compleja. *(Fuente: NICSS:)*

468. Factor Humano:

Característica de una persona que tiene un impacto sobre un objeto bajo consideración. *(Fuente: ISO 9.000:)*

469. Factor de trabajo:

Estimación del esfuerzo o tiempo que necesita un posible adversario, con la experiencia y recursos especificados, para superar una medida protectora. *(Fuente: NICSS:)*

470. Falla:

Incapacidad de un sistema o componente para cumplir sus funciones requeridas dentro de los requisitos de rendimiento especificados. *(Fuente: NICSS:)*

471. Falsificar:

Imitar, reproducir o modificar un bien material o su envase sin autorización. *(Fuente: ISO 22.300:)*

472. Fast Flux:

Método de protección usado por botnets que consiste en un cambio continuo y rápido de los registros DNS para un nombre de dominio a través de diferentes direcciones IP. *(Fuente: SANS:)*

473. Fiabilidad:

Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados. *(Fuente: ISO 27.000:)*

474. Fichero Contenedor:

Fichero que contiene la evidencia electrónica objeto de intercambio o comunicación. *(Fuente: UNE 71.505:)*

475. Filtrado de Salida:

Filtrado de tráfico saliente. *(Fuente: SANS:)*

476. Filtrado de entrada:

El filtrado de entrada es el filtrado del tráfico entrante. *(Fuente: SANS:)*

477. Filtro:

Un filtro se usa para especificar qué paquetes serán o no serán usados. Puede ser usado en sniffers para determinar qué paquetes se muestran, o por firewalls para determinar qué paquetes son bloqueados. *(Fuente: SANS:)*

478. Fin de vida (EoL):

Que la aplicación ha llegado al final de su vida útil. Puede significar que hay una nueva versión que reemplaza al producto existente o que ya no se ofrece soporte para el producto. *(Fuente: NICSS:)*

479. Finger:

Un protocolo para buscar información del usuario en un host dado. Un programa Unix que toma una dirección de correo electrónico como entrada y devuelve información sobre el usuario que posee esa dirección. En algunos sistemas, finger solo informa si el usuario está actualmente conectado. Otros sistemas devuelven información adicional, como el nombre

completo del usuario, dirección y número telefónico. Por supuesto, el usuario debe ingresar primero esta información al sistema. Muchos programas de correo electrónico ahora tienen una utilidad finger integrada. *(Fuente: SANS:)*

480. Fingerprinting:

Enviar paquetes extraños a un sistema para evaluar cómo responde y determinar el sistema operativo. *(Fuente: SANS:)*

481. Firewall:

Una discontinuidad lógica o física en una red para prevenir el acceso no autorizado a datos o recursos. *(Fuente: SANS:)*

482. Firewall de Voz:

Una discontinuidad física en una red de voz que monitorea, alerta y controla la actividad de la red de voz entrante y saliente basada en políticas definidas por el usuario de control de admisión de llamadas (CAC), amenazas a la seguridad de la capa de aplicación de voz o violaciones por uso no autorizado de servicios. *(Fuente: SANS:)*

483. Firma:

Una firma es un patrón distintivo en el tráfico de red que puede ser identificado con una herramienta o exploit específico. *(Fuente: SANS:)*

Tipos de firmas: firma de ataque, firma digital, firma electrónica. *(Fuente: NICSS:)*

484. Firma Electrónica:

Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. *(Fuente: UNE 71.505:)*

485. Firma Electrónica Avanzada:

Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. *(Fuente: UNE 71.505:)*

486. Firma Electrónica Reconocida:

Firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. *(Fuente: UNE 71.505:)*

487. Firma de ataque:

Conjunto automatizado de reglas para identificar una posible amenaza (como una explotación o herramienta de atacante) y posibles respuestas. *(Fuente: NICSS:)*

488. Firma digital:

Una firma digital es un hash de un mensaje que identifica de manera única al remitente y prueba que el mensaje no ha cambiado desde su transmisión. *(Fuente: SANS:)*

Un valor calculado mediante un proceso criptográfico usando una clave privada que se adjunta a un objeto de datos, firmando digitalmente los datos. *(Fuente: NICSS:)*

489. Firma electrónica:

Cualquier marca en forma electrónica asociada a un documento electrónico, aplicada con la intención de firmar dicho documento. *(Fuente: NICSS:)*

490. Flooding:

Un ataque que intenta causar una falla en (especialmente en la seguridad de) un sistema informático u otra entidad de procesamiento de datos, proporcionando más entrada de la que la entidad puede procesar adecuadamente. *(Fuente: SANS:)*

491. Footprinting:

Técnica de hacking ético utilizada para recopilar la mayor cantidad posible de datos sobre un sistema informático específico, una infraestructura y redes, con el fin de identificar oportunidades para penetrarlas. *(Fuente: NICSS:)*

492. Forense:

Relativo a tribunales de justicia o utilizado en ellos. *(Fuente: ISO 22.300:)*

493. Formación:

Actividades concebidas para facilitar el aprendizaje y desarrollo de conocimientos, destrezas y habilidades, así como mejorar el desempeño de tareas y roles concretos. *(Fuente: ISO 22.300:)*

494. Formato De Fichero:

Forma de codificar información para almacenarla en algún medio de escritura que permita ser leído o accedido por un sistema informático. *(Fuente: UNE 71.505:)*

495. Formato De Intercambio De La Evidencia Electrónica:

Conjunto de reglas que definen la estructura y el contenido para el intercambio de evidencias. *(Fuente: UNE 71.505:)*

496. Fragmentación:

El proceso de almacenar un archivo de datos en varios "trozos" o fragmentos en lugar de una secuencia contigua de bits en un solo lugar del medio de almacenamiento. *(Fuente: SANS:)*

497. Fuente Autorizada:

Origen oficial de un atributo que también es responsable de mantenerlo. *(Fuente: ISO 22.300:)*

498. Fuente De Riesgo:

Elemento que, por sí solo o en combinación con otros, presenta el potencial intrínseco de engendrar un riesgo. *(Fuente: ISO 22.300:)*

499. Fuerza De Letalidad Reducida:

Grado de fuerza utilizada que es menos susceptible de provocar la muerte o lesiones graves al responder ante confrontaciones violentas y adecuarse a los niveles de resistencia encontrados. *(Fuente: ISO 22.300:)*

500. Fuerza bruta:

Una técnica de criptoanálisis u otro tipo de método de ataque que implica un procedimiento exhaustivo que intenta todas las posibilidades, una por una. *(Fuente: SANS:)*

501. Fuerza de tarea de ingeniería de Internet (IETF):

El organismo que define los protocolos estándar de operación de Internet como TCP/IP. La IETF está supervisada por la Junta de Arquitectura de Internet (IAB) de la Sociedad de Internet. Los miembros de la IETF provienen de los miembros individuales y organizaciones de la Sociedad de Internet. *(Fuente: SANS:)*

502. Funcionarios De Las Fuerzas Y Cuerpos De Seguridad Y Otros Funcionarios Públicos Competentes:

Personal de las administraciones públicas y las fuerzas y cuerpos de seguridad que tiene competencia legal específica sobre la cadena de suministro internacional o partes de ella. *(Fuente: ISO 22.300:)*

503. Funciones hash:

Las funciones hash (criptográficas) se usan para generar una "suma de verificación" unidireccional para un texto más grande, que no es trivialmente reversible. El resultado de esta función hash puede usarse para validar si un archivo grande ha sido alterado, sin tener que comparar los archivos entre sí. Las funciones hash usadas frecuentemente son MD5 y SHA1. *(Fuente: SANS:)*

504. Función De Autenticación:

Función que lleva a cabo la autenticación. *(Fuente: ISO 22.300:)*

505. Función De Difusión De Los Avisos:

Actividades que permiten emitir mensajes adecuados para las personas en riesgo basados en información constatada recibida de la función de seguimiento de peligros. *(Fuente: ISO 22.300:)*

506. Función De Examen Del Objeto:

Proceso que de búsqueda y determinación del identificador único (UID) o de otros atributos destinados a la autenticación. *(Fuente: ISO 22.300:)*

507. Función De Medición:

Algoritmo o cálculo realizado para combinar dos o más medidas básicas. *(Fuente: ISO 27.000:)*

508. Función De Procesamiento De Consultas De Confianza; Tqpf:

Función que proporciona una pasarela a la función de verificación de confianza y al sistema de gestión de atributos de datos (ADMS). *(Fuente: ISO 22.300:)*

509. Función De Seguimiento De Peligros:

Actividades que permiten obtener información constatada sobre peligros en una zona determinada para tomar decisiones sobre la necesidad de emitir un aviso al público. *(Fuente: ISO 22.300:)*

510. Función De Verificación De Confianza:

Función que verifica si el identificador único (UID) recibido es válido o no y gestiona una respuesta conforme a unas reglas y los derechos de acceso. *(Fuente: ISO 22.300:)*

511. Función Metrológica:

Unidad funcional con responsabilidad administrativa y técnica para definir e implementar el sistema de gestión de las mediciones. *(Fuente: ISO 9.000:)*

512. Función hash:

Un algoritmo que calcula un valor basado en un objeto de datos, mapeando el objeto a un objeto de datos más pequeño. *(Fuente: SANS:)*

513. Función unidireccional:

Una función (matemática) f, que es fácil de calcular la salida con base en una entrada dada. Sin embargo, dado solo el valor de salida, es imposible (excepto por ataque de fuerza bruta) determinar cuál fue la entrada. *(Fuente: SANS:)*

514. Función "Hash":

Secuencia de valores resultado de aplicación de una función hash a un fichero electrónico. *(Fuente: UNE 71.505:)*

515. Fuzzer:

un método automatizado de prueba de software que inyecta entradas inválidas, malformadas o inesperadas en un sistema para revelar defectos y vulnerabilidades del software *(Fuente: NICSS:)*

516. Fuzzing:

Uso de herramientas especiales de pruebas de regresión para generar entradas fuera de especificación para una aplicación con el fin de encontrar vulnerabilidades de seguridad. También ver "pruebas de regresión". *(Fuente: SANS:)*

— G —

517. GNU:

GNU es un sistema operativo similar a Unix que viene con código fuente que puede ser copiado, modificado y redistribuido. El proyecto GNU fue iniciado en 1983 por Richard Stallman y otros, quienes formaron la Free Software Foundation. *(Fuente: SANS:)*

518. GeoIP:

una técnica que permite localizar a un usuario web en función de su dirección IP *(Fuente: NICSS:)*

519. Geolocalización:

Ubicación específica definida por uno de los distintos medios de representar la latitud, la longitud, la altitud sobre el nivel del mar y el sistema de coordenadas. *(Fuente: ISO 22.300:)*

520. Geoperimetraje:

configurar alertas para que, cuando un dispositivo como un teléfono inteligente con conexión a internet entre en un límite geográfico definido, el usuario reciba una alerta *(Fuente: NICSS:)*

521. Georredundancia:

La georredundancia actúa como una medida de seguridad en caso de fallas del sitio principal o en caso de un desastre o interrupción que afecte una región. *(Fuente: NICSS:)*

522. Gerente Del Programa De Ejercicios:

Persona responsable de la planificación y la mejora del programa de ejercicios. *(Fuente: ISO 22.300:)*

523. Gestión:

Actividades coordinadas para dirigir y controlar una organización. *(Fuente: ISO 22.300:)*

524. Gestión De Crisis:

Proceso de gestión integral que identifica los impactos potenciales que amenazan a una organización y facilita un marco para generar resiliencia, con la capacidad de dar una respuesta eficaz que proteja los intereses de las principales partes interesadas, la reputación, la marca y las actividades generadoras de valor, así como restablecer de manera eficaz las capacidades operativas. *(Fuente: ISO 22.300:)*

525. Gestión De Emergencias:

Planteamiento global para prevenir y gestionar las emergencias que puedan ocurrir. *(Fuente: ISO 22.300:)*

526. Gestión De Incidentes De Seguridad De La Información:

Procesos para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de la información. *(Fuente: ISO 27.000:)*

527. Gestión De La Calidad:

Gestión con respecto a la calidad. *(Fuente: ISO 9.000:)*

528. Gestión De La Configuración:

Actividades coordinadas para dirigir y controlar la configuración. *(Fuente: ISO 9.000:)*

529. Gestión De La Continuidad De La Cadena De Suministro, Sccm:

Aplicación de la gestión de la continuidad del negocio a la cadena de suministro. *(Fuente: ISO 22.300:)*

530. Gestión De La Continuidad Del Negocio:

Proceso de gestión integral que identifica las amenazas potenciales para una organización y el impacto que estas pueden tener, en caso de materializarse, sobre las operaciones del negocio, y facilita un marco de referencia para generar resiliencia organizacional con la capacidad de dar una respuesta eficaz que proteja los intereses de las principales partes interesadas, la reputación, la marca y las actividadesgeneradoras de valor. *(Fuente: ISO 22.300:)*

531. Gestión De La Seguridad:

Actividades y prácticas sistemáticas y coordinadas mediante las cuales una organización gestiona de forma óptima sus riesgos, así como las amenazas e impactos potenciales asociados. *(Fuente: ISO 22.300:)*

532. Gestión De Operaciones De Seguridad:

Actividades coordinadas para dirigir y controlar una organización en lo relativo a las operaciones de seguridad. *(Fuente: ISO 22.300:)*

533. Gestión De Proyectos:

Planificación, organización, seguimiento, control e informe de todos los aspectos de un proyecto y la motivación de todos aquellos que están involucrados en él para alcanzar los objetivos del proyecto. *(Fuente: ISO 9.000:)*

534. Gestión Del Riesgo:

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. *(Fuente: ISO 22.300:)*

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. *(Fuente: ISO 27.000:)*

535. Gestión de acceso:

La gestión de acceso es el mantenimiento de la información de acceso, que consta de cuatro tareas: administración de cuentas, mantenimiento, monitoreo y revocación. *(Fuente: SANS:)*

536. Gestión de configuración:

Establecer una condición base conocida y gestionarla. *(Fuente: SANS:)*

537. Gestión de datos basada en riesgos:

Un enfoque estructurado para gestionar riesgos a los datos e información mediante el cual una organización selecciona y aplica controles de seguridad apropiados en cumplimiento con la política y acorde con la sensibilidad y valor de los datos. *(Fuente: NICSS:)*

538. Gestión de derechos digitales:

Una forma de tecnología de control de acceso para proteger y gestionar el uso del contenido o dispositivos digitales conforme a las intenciones del proveedor del contenido o dispositivo. *(Fuente: NICSS:)*

539. Gestión de identidades y accesos:

Los métodos y procesos usados para gestionar sujetos y su autenticación y autorizaciones para acceder a objetos específicos. *(Fuente: NICSS:)*

540. Gestión de incidentes:

La gestión y coordinación de actividades asociadas con la ocurrencia real o potencial de un evento que puede resultar en consecuencias adversas para la información o sistemas de información. *(Fuente: NICSS:)*

541. Gestión de programas de seguridad:

En el marco NICE, trabajo de ciberseguridad donde una persona: administra las implicancias de la seguridad de la información dentro de la organización, programa específico u otra área de responsabilidad, incluyendo estrategia, personal, infraestructura, cumplimiento de

políticas, planificación de emergencias, concienciación de seguridad y otros recursos (por ejemplo, el rol de un Oficial Principal de Seguridad de la Información). *(Fuente: NICSS:)*

542. Gestión de riesgos:

Incluye: 1) realizar una evaluación de riesgos 2) implementar estrategias para mitigar riesgos 3) monitoreo continuo del riesgo a lo largo del tiempo y 4) documentar el programa general de gestión de riesgos. *(Fuente: NICSS:)*

543. Gestión de riesgos empresariales:

Implica identificar dependencias de la misión sobre capacidades empresariales, identificar y priorizar riesgos debidos a amenazas definidas, implementar contramedidas para proporcionar tanto una postura de riesgo estática como una respuesta dinámica efectiva a amenazas activas, y evaluar el desempeño empresarial frente a amenazas ajustando contramedidas según sea necesario. *(Fuente: NICSS:)*

544. Gestión del conocimiento:

En el marco NICE, trabajo de ciberseguridad donde una persona: gestiona y administra procesos y herramientas que permiten a la organización identificar, documentar y acceder al capital intelectual y contenido informativo. *(Fuente: NICSS:)*

545. Gestión del riesgo en la cadena de suministro:

El proceso de identificar, analizar y evaluar el riesgo en la cadena de suministro y aceptarlo, evitarlo, transferirlo o controlarlo a un nivel aceptable considerando los costos y beneficios asociados a las acciones tomadas. *(Fuente: NICSS:)*

546. Gestión integrada de riesgos:

El enfoque estructurado que permite a una empresa u organización compartir información y análisis de riesgos y sincronizar estrategias de gestión de riesgos independientes pero complementarias para unificar esfuerzos a lo largo de toda la empresa. *(Fuente: NICSS:)*

547. Gnutella:

Una utilidad de intercambio de archivos en Internet. Gnutella actúa como servidor para compartir archivos mientras simultáneamente actúa como cliente que busca y descarga archivos de otros usuarios. *(Fuente: SANS:)*

548. Gobernanza De La Seguridad De La Información:

Sistema mediante el cual una organización dirige y supervisa las actividades de seguridad de la información. *(Fuente: ISO 27.000:)*

549. Grupo Objetivo:

Personas u organizaciones sometidas a los ejercicios. *(Fuente: ISO 22.300:)*

550. Grupo Vulnerable:

Personas que comparten una a varias características que constituyen la base de una discriminación o de unas circunstancias desfavorables de carácter social, económico, cultural, político o en lo referente a la salud y que provoca que no cuenten con los medios para hacer efectivos sus derechos ni tampoco para disfrutar de las mismas oportunidades. *(Fuente: ISO 22.300:)*

551. Guerra asimétrica:

La guerra asimétrica es el hecho de que una pequeña inversión, correctamente aprovechada, puede producir resultados increíbles. *(Fuente: SANS:)*

552. Guerra cibernética:

típicamente definida como un conjunto de acciones por parte de una nación u organización para atacar los sistemas de redes informáticas de países o instituciones con la intención de interrumpir, dañar o destruir infraestructura mediante virus informáticos o ataques de denegación de servicio. *(Fuente: NICSS:)*

553. Guerra de la información:

La guerra de la información es la competencia entre actores ofensivos y defensivos por los recursos de información. *(Fuente: SANS:)*

554. Guerrero cibernético:

un individuo que participa en la guerra cibernética, motivado por razones personales, patrióticas o religiosas, pero no por una exigencia profesional *(Fuente: NICSS:)*

555. Guion:

Desarrollo de la trama del ejercicio, que permite al personal de dirección entender cómo deberían desarrollarse los eventos durante la realización del ejercicio a medida que se introducen los diversos elementos de los eventos principales. *(Fuente: ISO 22.300:)*

556. Gusano:

Programa auto-replicante, auto-propagante y autónomo que utiliza mecanismos de red para propagarse. *(Fuente: NICSS:)*

Un programa de computadora que puede ejecutarse independientemente, puede propagarse copiándose completamente a otros hosts en una red, y puede consumir recursos computacionales de manera destructiva. *(Fuente: SANS:)*

557. Gusano Morris:

Un programa gusano escrito por Robert T. Morris, Jr. que inundó la ARPANET en noviembre de 1988, causando problemas para miles de hosts. *(Fuente: SANS:)*

558. Guía:

<auditoría> Persona designada por el auditado para asistir al equipo auditor. *(Fuente: ISO 9.000:)*

— H —

559. HTTPS:

Cuando se usa en la primera parte de una URL (la parte que precede dos puntos y especifica un esquema de acceso o protocolo), este término especifica el uso de HTTP mejorado por un mecanismo de seguridad, que generalmente es SSL. *(Fuente: SANS:)*

560. Hackathon:

una reunión de personas de diversos orígenes y diferentes etapas de sus carreras (desde aficionados hasta profesionales) para resolver problemas de interés común *(Fuente: NICSS:)*

561. Hacker:

Un usuario no autorizado que intenta acceder o accede a un sistema de información. *(Fuente: NICSS:)*

562. Hallazgos De La Auditoría:

Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría. *(Fuente: ISO 9.000:)*

563. Hash o hashing:

Mapear una cadena de bits de longitud arbitraria a una cadena de bits de longitud fija para producir el valor hash. *(Fuente: NICSS:)*

564. Herramienta De Autenticación:

Conjunto de hardware y/o software que forma parte de una solución contra la falsificación y se usa para controlar el elemento de autenticación. *(Fuente: ISO 22.300:)*

565. Herramienta De Autenticación Autónoma:

Herramienta de autenticación que se utiliza para revelar un elemento de autenticación que los sentidos humanos no pueden percibir en una verificación realizada por una persona o que integra las funciones necesarias para poder verificar el elemento de autenticación de manera independiente. *(Fuente: ISO 22.300:)*

566. Herramienta De Autenticación Disponible Comercialmente:

Herramienta de autenticación que puede adquirirse a través de redes de venta libre. *(Fuente: ISO 22.300:)*

567. Herramienta De Autenticación En Línea:

Herramienta de autenticación que requiere una conexión en línea en tiempo real para poder interpretar el elemento de autenticación de forma local. *(Fuente: ISO 22.300:)*

568. Herramienta De Autenticación Hecha A Medida:

Herramienta de autenticación destinada a una solución de autenticación específica. *(Fuente: ISO 22.300:)*

569. Hipervínculo:

En hipertexto o hipermedia, un objeto de información (como una palabra, frase o imagen; usualmente resaltado con color o subrayado) que apunta (indica cómo conectar) a información relacionada que se encuentra en otro lugar y puede ser recuperada activando el enlace. *(Fuente: SANS:)*

570. Historial De Accesos Del Inspector:

Registros de acceso que detallan cuándo se han verificado identificadores únicos (UID) y, de forma opcional, por qué inspector (con derechos de acceso) y desde qué ubicación específica. *(Fuente: ISO 22.300:)*

571. Honeymonkey:

Sistema automatizado que simula un usuario navegando sitios web. El sistema típicamente está configurado para detectar sitios web que explotan vulnerabilidades en el navegador. También conocido como Cliente Honey. *(Fuente: SANS:)*

572. Honeypot:

Programas que simulan uno o más servicios de red que designas en los puertos de tu computadora. Un atacante asume que estás ejecutando servicios vulnerables que pueden usarse para acceder a la máquina. Un honeypot puede registrar intentos de acceso a esos puertos, incluyendo las pulsaciones del atacante. Esto puede darte una advertencia anticipada de un ataque más concertado. *(Fuente: SANS:)*

573. Horizonte Dividido:

Horizonte dividido es un algoritmo para evitar problemas causados por incluir rutas en actualizaciones enviadas al gateway desde el cual se aprendieron dichas rutas. *(Fuente: SANS:)*

574. Host:

Cualquier computadora que tenga acceso bidireccional completo a otras computadoras en Internet. O una computadora con un servidor web que sirve las páginas para uno o más sitios web. *(Fuente: SANS:)*

575. Hub:

Un hub es un dispositivo de red que opera repitiendo los datos que recibe en un puerto a todos los demás puertos. Como resultado, los datos transmitidos por un host se retransmiten a todos los demás hosts conectados al hub. *(Fuente: SANS:)*

576. Huella Digital:

Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información. *(Fuente: UNE 71.505:)*

577. Huella TCP:

La huella TCP es el uso de combinaciones extrañas en los encabezados de paquetes para determinar el sistema operativo remoto. *(Fuente: SANS:)*

— I —

578. IDS basado en host:

Los sistemas de detección de intrusiones basados en host usan información de los registros de auditoría del sistema operativo para vigilar todas las operaciones que ocurren en el host donde está instalado el software de detección de intrusiones. Estas operaciones se comparan con una política de seguridad predefinida. Este análisis del rastro de auditoría impone una posible sobrecarga significativa en el sistema debido a la mayor cantidad de procesamiento requerida por el sistema de detección de intrusiones. Dependiendo del tamaño del rastro de auditoría y la capacidad de procesamiento del sistema, la revisión de los datos de auditoría podría resultar en la pérdida de la capacidad de análisis en tiempo real. *(Fuente: SANS:)*

579. IDS basado en red:

Un sistema IDS basado en red monitorea el tráfico en su segmento de red como fuente de datos. Esto se logra generalmente poniendo la tarjeta de interfaz de red en modo promiscuo para capturar todo el tráfico que cruza su segmento de red. El tráfico en otros segmentos y otros medios de comunicación (como líneas telefónicas) no puede ser monitoreado. El IDS basado en red observa los paquetes en la red a medida que pasan por un sensor, que solo puede ver los paquetes del segmento de red al que está conectado. Los paquetes son de interés si coinciden con una firma. La detección de intrusiones basada en red monitorea pasivamente la actividad para indicar ataques y ofrece varias ventajas sobre los IDS basados en host, detectando ataques que podrían pasar desapercibidos. *(Fuente: SANS:)*

580. IDaaS:

una gestión de identidad y acceso (IAM) basada en la nube ofrecida por un proveedor extern *(Fuente: NICSS:)*

581. IPSec:

El Protocolo de Internet (IP) es el estándar común que determina cómo viajan los datos por internet. IPSec agrega cifrado y autenticación para hacer el protocolo más seguro. *(Fuente: NICSS:)*

582. ISO:

Organización Internacional de Normalización, una organización voluntaria, no gubernamental ni de tratado, establecida en 1947, con miembros con derecho a voto que son organismos de normalización designados de naciones participantes y observadores sin voto. *(Fuente: SANS:)*

583. Identidad:

La identidad es quién es alguien o qué es algo, por ejemplo, el nombre por el cual se conoce algo. *(Fuente: SANS:)*

Conjunto de atributos que está asociado a una entidad. *(Fuente: ISO 22.300:)*

584. Identificación:

Proceso de reconocimiento de los atributos que identifican a la entidad. *(Fuente: ISO 22.300:)*

585. Identificación De Riesgos:

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos. *(Fuente: ISO 22.300:)*

586. Identificación Del Riesgo:

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos. *(Fuente: ISO 27.000:)*

587. Identificador:

Conjunto determinado de atributos que se asigna a una entidad a efectos de identificación. *(Fuente: ISO 22.300:)*

588. Identificador Uniforme de Recursos (URI):

El término genérico para todo tipo de nombres y direcciones que se refieren a objetos en la World Wide Web. *(Fuente: SANS:)*

589. Identificador Único; UID:

Código que representa un conjunto único y específico de atributos relativos a un objeto o a una clase de objetos durante toda su vida en el ámbito y alcance concretos de un sistema de identificación de objetos. *(Fuente: ISO 22.300:)*

590. Impacto:

Consecuencia valorada de un resultado concreto. *(Fuente: ISO 22.300:)*

591. Imparcialidad:

Existencia real o percibida de objetividad. *(Fuente: ISO 22.300:)*

592. Improvisación:

Acto de idear, formular o ejecutar con poca o ninguna preparación una reacción a lo imprevisto. *(Fuente: ISO 22.300:)*

593. Incidente:

Una ocurrencia que constituye una violación o amenaza inminente de violación de políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. *(Fuente: NICSS:)*

Situación que puede ser, o podría provocar, una disrupción, una pérdida, una emergencia o una crisis. *(Fuente: ISO 22.300:)*

Un incidente es un evento adverso en una red, sistema de información o la amenaza de la ocurrencia de tal evento. *(Fuente: SANS:)*

594. Incidente De Seguridad De La Información:

Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información. *(Fuente: ISO 27.000:)*

Propiedad de salvaguardar que los activos son exactos y completos. *(Fuente: UNE 71.505:)*

595. Indicador:

Medida que proporciona una estimación o una evaluación de determinados atributos usando un modelo analítico para satisfacer unas determinadas necesidades de información. *(Fuente: ISO 27.000:)*

Una ocurrencia o señal de que un incidente puede haber ocurrido o puede estar en progreso. *(Fuente: NICSS:)*

596. Indicador De Desempeño; Kpi:

Medida cuantificable que una organización usa para valorar o comparar el desempeño en cuanto al cumplimiento de los objetivos estratégicos y operativos. *(Fuente: ISO 22.300:)*

597. Indicador de ataque (IoA):

Una pista de que una entidad maliciosa ha obtenido o está intentando obtener acceso no autorizado a la red o a activos conectados a la red. *(Fuente: NICSS:)*

598. Indicador de compromiso (IoC):

pistas y evidencias de una violación de datos *(Fuente: NICSS:)*

599. Indicadores de ataque (IoAs):

Los indicadores de ataque no son tanto una descripción estática del atacante, sino un perfil dinámico de cómo un atacante interactúa con tus tecnologías y usuarios. *(Fuente: NICSS:)*

600. Inetd (xinetd):

Inetd (o Internet Daemon) es una aplicación que controla servicios de internet menores como telnet, ftp y POP. *(Fuente: SANS:)*

601. Infección del registro de arranque:

Una infección del registro de arranque es un tipo de malware que inserta código malicioso en el sector de arranque de un disco. *(Fuente: SANS:)*

602. Infectador de programas:

Un infectador de programas es un tipo de malware que se adjunta a archivos de programas existentes. *(Fuente: SANS:)*

603. Información:

Datos procesados, organizados y correlacionados para darles sentido. *(Fuente: ISO 22.300:)*

Datos que poseen significado. *(Fuente: ISO 9.000:)*

604. Información Documentada:

Información que una organización tiene que controlar y mantener, y el medio en el que está contenida. *(Fuente: ISO 27.000:)*

Información que una organización tiene que controlar y mantener, y el medio que la contiene. *(Fuente: ISO 22.300:)*

605. Información Operativa:

Información que se ha contextualizado y analizado para poder comprender la situación y su posible evolución. *(Fuente: ISO 22.300:)*

606. Información Sensible:

Información sensible, según la definición del gobierno federal, es cualquier información no clasificada que, si es comprometida, podría afectar negativamente el interés nacional o la ejecución de iniciativas federales. *(Fuente: SANS:)*

Información protegida de su divulgación pública porque tendría un efecto negativo sobre una organización, la seguridad nacional o la seguridad pública. *(Fuente: ISO 22.300:)*

607. Información Sensible Para La Seguridad; Documentación Sensible Para La Seguridad:

Información o material, producidos por el proceso de seguridad de la cadena de suministro o incorporados a él, que contiene información sobre los procesos, envíos o directivas gubernamentales de seguridad que no estaría a disposición del público y que resultaría útil para alguien que quisiera iniciar un incidente de seguridad. *(Fuente: ISO 22.300:)*

608. Información Sobre Configuración Del Producto:

Requisito u otra información para el diseño, la realización, la verificación, el funcionamiento y el soporte de un producto. *(Fuente: ISO 9.000:)*

609. Información personal identificable:

La información que permite inferir directa o indirectamente la identidad de un individuo. *(Fuente: NICSS:)*

610. Información propietaria:

Información propietaria es aquella información única para una empresa y su capacidad para competir, como listas de clientes, datos técnicos, costos de productos y secretos comerciales. *(Fuente: SANS:)*

611. Informe Posterior A Una Acción:

Documento que registra, describe y analiza el ejercicio, apoyándose en los informes de los observadores, y extrae lecciones del mismo. *(Fuente: ISO 22.300:)*

612. Informática forense:

En el marco NICE, trabajo de ciberseguridad donde una persona: recopila, procesa, preserva, analiza y presenta evidencia relacionada con computadoras en apoyo de investigaciones de vulnerabilidades de red, mitigación y/o investigaciones criminales, de fraude, contrainteligencia o de cumplimiento de la ley. *(Fuente: NICSS:)*

613. Infraestructura:

Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización. *(Fuente: ISO 22.300:)*

<organización> Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización. *(Fuente: ISO 9.000:)*

614. Infraestructura cibernética:

Sistemas y servicios de información y comunicaciones compuestos por todo el hardware y software que procesan, almacenan y comunican información, o cualquier combinación de estos elementos. Incluye la creación, acceso, modificación, destrucción, almacenamiento y distribución de la información. *(Fuente: NICSS:)*

615. Infraestructura crítica:

Sistemas y activos, físicos o virtuales, tan vitales para la sociedad que su incapacidad o destrucción puede tener un impacto devastador en la seguridad, economía, salud pública, medio ambiente o cualquier combinación de estos aspectos. *(Fuente: NICSS:)*

616. Infraestructura de clave pública:

Un marco y servicios para generar, producir, distribuir, controlar, contabilizar y revocar (destruir) certificados de clave pública. *(Fuente: NICSS:)*

617. Infraestructura de clave pública (PKI):

Una PKI (infraestructura de clave pública) permite a usuarios de una red pública básicamente insegura como Internet intercambiar datos y dinero de manera segura y privada mediante el

uso de un par de claves criptográficas pública y privada obtenidas y compartidas a través de una autoridad confiable. La infraestructura de clave pública provee un certificado digital que puede identificar a una persona o una organización y servicios de directorio que pueden almacenar y, cuando sea necesario, revocar los certificados. *(Fuente: SANS:)*

618. Ingeniería Social:

Eufemismo para métodos no técnicos o de baja tecnología —como mentiras, suplantación, trucos, sobornos, chantajes y amenazas— usados para atacar sistemas de información. *(Fuente: SANS:)*

619. Ingeniería inversa:

Obtener datos sensibles desensamblando y analizando el diseño de un componente del sistema. *(Fuente: SANS:)*

620. Ingeniería social:

El uso del engaño para manipular a individuos para que divulguen información confidencial o personal que pueda ser usada para fines fraudulentos. *(Fuente: NICSS:)*

621. Innovación:

Objeto nuevo o cambiado que crea o redistribuye valor. *(Fuente: ISO 9.000:)*

622. Inserto:

Información que sigue un guion y se inserta en un ejercicio y que está concebida para provocar una respuesta o una decisión y facilitar el desarrollo del ejercicio. *(Fuente: ISO 22.300:)*

623. Inspección:

Determinación de la conformidad con los requisitos especificados. *(Fuente: ISO 9.000:)*

624. Inspección Stateful:

También conocido como filtrado dinámico de paquetes. La inspección stateful es una arquitectura de firewall que trabaja en la capa de red. A diferencia del filtrado estático de paquetes, que examina un paquete basándose en la información de su encabezado, la inspección stateful examina no solo la información del encabezado sino también el contenido del paquete hasta la capa de aplicación para determinar más sobre el paquete que solo información de su origen y destino. *(Fuente: SANS:)*

625. Inspector:

Persona que utiliza la función de examen del objeto para valorar un objeto. *(Fuente: ISO 22.300:)*

626. Instalación:

Planta, maquinaria, terreno, edificio, unidades de transporte, puertos marítimos y fluviales, aeropuertos y otros elementos de infraestructura o de una planta y sus sistemas asociados que tienen una función o un servicio claros y cuantificables para el negocio. *(Fuente: ISO 22.300:)*

627. Instituto Nacional de Estándares y Tecnología (NIST):

Instituto Nacional de Estándares y Tecnología, una unidad del Departamento de Comercio de EE.UU. Anteriormente conocido como la Oficina Nacional de Estándares, NIST promueve y mantiene estándares de medición. También tiene programas activos para fomentar y asistir a la industria y la ciencia en el desarrollo y uso de estos estándares. *(Fuente: SANS:)*

628. Integrar la seguridad desde el diseño:

Conjunto de principios, prácticas y herramientas para diseñar, desarrollar y evolucionar sistemas de información y software que refuercen la resistencia a vulnerabilidades, fallos y ataques. *(Fuente: NICSS:)*

629. Integridad:

Propiedad de salvaguardar la exactitud y completitud de los activos. *(Fuente: ISO 22.300:)*

Propiedad de salvaguardar que los activos son exactos y completos. *(Fuente: UNE 71.505:)*

Propiedad de exactitud y completitud. *(Fuente: ISO 27.000:)*

La integridad es la necesidad de asegurar que la información no ha sido cambiada accidental o deliberadamente, y que es precisa y completa. *(Fuente: SANS:)*

Un estado en el que la información se ha mantenido sin alteraciones desde el momento en que fue producida por una fuente, durante la transmisión, almacenamiento y recepción final en el destino. *(Fuente: NICSS:)*

630. Integridad de los datos:

La propiedad de que los datos están completos, intactos y son confiables, y no han sido modificados ni destruidos de manera no autorizada o accidental. *(Fuente: NICSS:)*

631. Integridad del sistema:

Atributo de un sistema de información cuando realiza su función prevista de manera no alterada, libre de manipulación no autorizada deliberada o accidental del sistema. *(Fuente: NICSS:)*

632. Inteligencia competitiva:

La inteligencia competitiva es espionaje usando medios legales, o al menos no obviamente ilegales. *(Fuente: SANS:)*

633. Inteligencia de amenazas cibernéticas (CTI):

La recopilación, procesamiento, organización y análisis de datos en información procesable que se relaciona con capacidades, oportunidades, acciones e intención de adversarios en el dominio cibernético, para cumplir con un requisito específico determinado por e informando a los responsables de la toma de decisiones. *(Fuente: NICSS:)*

634. Inteligencia de todas las fuentes:

En el marco NICE, trabajo en ciberseguridad donde una persona analiza información sobre amenazas de múltiples fuentes, disciplinas y agencias, la contextualiza y extrae implicaciones. *(Fuente: NICSS:)*

635. Intención:

Un estado mental o deseo de alcanzar un objetivo. *(Fuente: NICSS:)*

636. Intercambio de información:

Un intercambio de datos, información y/o conocimiento para gestionar riesgos o responder a incidentes. *(Fuente: NICSS:)*

637. Intercepción de comunicaciones:

Monitoreo y grabación de datos que fluyen entre dos puntos en un sistema de comunicación. *(Fuente: SANS:)*

638. Interfaz Común de Pasarela:

Este mecanismo es usado por servidores HTTP (servidores web) para pasar parámetros a scripts ejecutables con el fin de generar respuestas dinámicamente. *(Fuente: SANS:)*

639. Internet:

Un término para describir la conexión de múltiples redes separadas. *(Fuente: SANS:)*

640. Internet Industrial de las Cosas (IIoT):

La colección de sensores, instrumentos y dispositivos autónomos conectados a través de internet a aplicaciones industriales. *(Fuente: NICSS:)*

641. Interoperabilidad:

Capacidad de varios sistemas y organizaciones de trabajar de forma conjunta. *(Fuente: ISO 22.300:)*

La capacidad de dos o más sistemas o componentes para intercambiar información y usar la información que ha sido intercambiada. *(Fuente: NICSS:)*

642. Interoperabilidad Semántica:

Capacidad de dos o más sistemas o servicios para interpretar y usar automáticamente la información intercambiada con exactitud. *(Fuente: ISO 22.300:)*

643. Interoperabilidad Sintáctica:

Capacidad de dos o más sistemas o servicios de intercambiar información estructurada. *(Fuente: ISO 22.300:)*

644. Interpretación Automatizada:

Proceso que valora de forma automática la autenticidad de uno o más componentes de la solución de autenticación. *(Fuente: ISO 22.300:)*

645. Interpretación Humana:

Autenticidad según la valoración de un inspector. *(Fuente: ISO 22.300:)*

646. Interrupción:

Una circunstancia o evento que interrumpe o impide el funcionamiento correcto de los servicios y funciones del sistema. *(Fuente: SANS:)*

Una interrupción es una señal que informa al sistema operativo que algo ha ocurrido. *(Fuente: SANS:)*

Un evento que causa una interrupción no planificada en operaciones o funciones durante un período inaceptable. *(Fuente: NICSS:)*

647. Intranet:

Una red informática, especialmente basada en tecnología de Internet, que una organización utiliza para sus propios fines internos y usualmente privados, y que está cerrada a personas externas. *(Fuente: SANS:)*

648. Intrusión:

Un acto no autorizado de evadir los mecanismos de seguridad de una red o sistema de información. *(Fuente: NICSS:)*

649. Inundación IP:

Un ataque de denegación de servicio que envía a un host más paquetes de solicitud de eco ("ping") de los que la implementación del protocolo puede manejar. *(Fuente: SANS:)*

650. Investigación:

En el marco NICE, trabajo de ciberseguridad donde una persona: Aplica tácticas, técnicas y procedimientos para un rango completo de herramientas y procesos investigativos que incluyen pero no se limitan a técnicas de entrevista e interrogación, vigilancia, contra vigilancia y detección de vigilancia, y equilibra apropiadamente los beneficios de la prosecución versus la recopilación de inteligencia. *(Fuente: NICSS:)*

651. Investigación y desarrollo tecnológico:

En el marco NICE, trabajo en ciberseguridad donde una persona: conduce procesos de evaluación e integración tecnológica, proporciona y apoya una capacidad prototipo y/o evalúa su utilidad. *(Fuente: NICSS:)*

652. Investigar:

Una categoría del marco NICE que consiste en áreas especializadas responsables de la investigación de eventos cibernéticos y/o delitos en sistemas IT, redes y evidencias digitales. *(Fuente: NICSS:)*

653. Inyección SQL:

La inyección SQL es un tipo de ataque de validación de entrada específico para aplicaciones basadas en bases de datos, donde se inserta código SQL en consultas de la aplicación para manipular la base de datos. *(Fuente: SANS:)*

— J —

654. Jitter:

Jitter o ruido es la modificación de campos en una base de datos mientras se preservan las características agregadas que hacen útil a la base de datos. *(Fuente: SANS:)*

655. Juegos de guerra:

Técnica interactiva que sumerge a posibles respondedores de incidentes cibernéticos en un escenario cibernético simulado. *(Fuente: NICSS:)*

656. Justificación Del Estado De La Configuración:

Registro e informe formalizado de la información sobre configuración del producto , el estado de los cambios propuestos y el estado de la implementación de los cambios aprobados. *(Fuente: ISO 9.000:)*

— K —

657. Kerberos:

Un sistema desarrollado en el Instituto de Tecnología de Massachusetts que depende de contraseñas y criptografía simétrica (DES) para implementar un servicio de autenticación basado en tickets y un servicio de control de acceso distribuido en un entorno de red cliente-servidor. *(Fuente: SANS:)*

— L —

658. LaaS:

Un modelo arquitectónico de TI para la ingesta y recopilación centralizada de cualquier tipo de archivos de registro provenientes de cualquier fuente o ubicación, como servidores, aplicaciones y dispositivos. *(Fuente: NICSS:)*

659. Lado del cliente:

Incluye lo que el usuario ve, como texto, imágenes y el resto de la interfaz de usuario, junto con cualquier acción que realiza una aplicación dentro del navegador del usuario. *(Fuente: NICSS:)*

660. LangSec:

Una filosofía de diseño y programación que se centra en el manejo formalmente correcto y verificable de entradas a lo largo de todas las fases del ciclo de vida del desarrollo de software. *(Fuente: NICSS:)*

661. Legion:

Software para detectar recursos compartidos no protegidos. *(Fuente: SANS:)*

662. Legítima Defensa:

Protección de uno mismo o de sus propiedades frente a un intento de lesión o daño por parte de otra persona. *(Fuente: ISO 22.300:)*

663. Lenguaje de marcas de hipertexto (HTML):

El conjunto de símbolos o códigos de marcado insertados en un archivo destinado a mostrarse en una página de navegador web. *(Fuente: SANS:)*

664. Lenguaje práctico de extracción y reporte (Perl):

Un lenguaje de programación de scripts que es similar en sintaxis al lenguaje C e incluye una serie de utilidades populares de Unix como sed, awk y tr. *(Fuente: SANS:)*

665. Liberación:

Autorización para proseguir con la siguiente etapa de un proceso o el proceso siguiente. *(Fuente: ISO 9.000:)*

666. Lista de bloqueados:

Lista de entidades que están bloqueadas o se les niega el acceso o privilegios. *(Fuente: NICSS:)*

667. Lista de control de acceso (ACL):

Mecanismo que implementa el control de acceso a un recurso del sistema listando las identidades de las entidades del sistema autorizadas para acceder al recurso. *(Fuente: SANS:)*

668. Lista de permitidos:

Una lista de entidades consideradas confiables a las que se les concede acceso o privilegios. *(Fuente: NICSS:)*

669. Localización Escenográfica:

Conjunto de geolocalizaciones que define el perímetro de la escena visible por una cámara. *(Fuente: ISO 22.300:)*

670. Localizador Uniforme de Recursos (URL):

La dirección global de documentos y otros recursos en la World Wide Web. La primera parte de la dirección indica qué protocolo usar, y la segunda parte especifica la dirección IP o el nombre de dominio donde se encuentra el recurso. Por ejemplo, http://www.pcwebopedia.com/ind.... *(Fuente: SANS:)*

671. Lugar De Trabajo Alternativo:

Emplazamiento de trabajo, distinto al emplazamiento principal, que tiene que utilizarse cuando este último es inaccesible. *(Fuente: ISO 22.300:)*

672. Lógica maliciosa:

Hardware, firmware o software que se incluye o inserta intencionalmente en un sistema para realizar una función o proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema de información. *(Fuente: NICSS:)*

— M —

673. Maestro de bots:

El controlador de una botnet que, desde una ubicación remota, dirige a las computadoras comprometidas de la red. *(Fuente: NICSS:)*

674. Malvertising:

un ataque malicioso que implica la inyección de código dañino en redes legítimas de publicidad en línea. *(Fuente: NICSS:)*

675. Malware:

Un término genérico para varios tipos diferentes de código malicioso. *(Fuente: SANS:)*

Software que compromete la operación de un sistema realizando una función o proceso no autorizado. *(Fuente: NICSS:)*

676. Malware de interrupción:

Una categoría de malware diseñada para suspender operaciones dentro de un objetivo mediante el compromiso de la disponibilidad, integridad y confidencialidad de los sistemas, redes y datos. *(Fuente: NICSS:)*

677. Mando Y Control:

Actividades de la toma de decisiones centrada en los objetivos, incluyendo la evaluación de la situación, la planificación, la implementación de las decisiones y el control de los efectos de la implementación sobre el incidente. *(Fuente: ISO 22.300:)*

678. Manejo de incidentes:

El manejo de incidentes es un plan de acción para tratar con intrusiones, ciberrobo, denegación de servicio, incendios, inundaciones y otros eventos relacionados con la seguridad. Comprende un proceso de seis pasos: Preparación, Identificación, Contención, Erradicación, Recuperación y Lecciones aprendidas. *(Fuente: SANS:)*

679. Manipulación de Pila:

La manipulación de pila es la técnica de usar un desbordamiento de buffer para engañar a un ordenador y hacer que ejecute código arbitrario. *(Fuente: SANS:)*

680. Manipulación de marcas de tiempo:

Técnica utilizada en ciberseguridad y análisis forense digital, donde los atacantes modifican las marcas de tiempo de archivos y directorios en un sistema informático para ocultar sus acciones o dificultar las investigaciones. *(Fuente: NICSS:)*

681. Manipular:

Alterar deliberadamente la lógica, datos o información de control de un sistema para hacer que el sistema realice funciones o servicios no autorizados. *(Fuente: SANS:)*

682. Manual De La Calidad:

Especificación para el sistema de gestión de la calidad de una organización. *(Fuente: ISO 9.000:)*

683. Mapeo de red:

Compilar un inventario electrónico de los sistemas y servicios en su red. *(Fuente: SANS:)*

684. Marca De Tiempo:

Fecha y hora asignadas por medios electrónicos a un fichero electrónico. *(Fuente: UNE 71.505:)*

685. Marcación Automática (War Dialing):

War dialing es un método simple para intentar identificar módems en una central telefónica que podrían ser susceptibles a compromisos para intentar evadir la seguridad perimetral. *(Fuente: SANS:)*

686. Marcador Automático (War Dialer):

Un programa de computadora que marca automáticamente una serie de números telefónicos para encontrar líneas conectadas a sistemas computacionales y cataloga esos números para que un cracker pueda intentar acceder a los sistemas. *(Fuente: SANS:)*

687. Matriz de acceso:

Una matriz de acceso usa filas para representar sujetos y columnas para representar objetos, con privilegios listados en cada celda. *(Fuente: SANS:)*

688. Mecanismo:

Es el conjunto de procedimientos técnicos y algoritmos (principalmente criptográficos) que se emplean para generar una evidencia electrónica. *(Fuente: UNE 71.505:)*

689. Mecanismo de control de acceso:

Medidas de seguridad diseñadas para detectar y denegar accesos no autorizados y permitir el acceso autorizado a un sistema de información o a una instalación física. *(Fuente: NICSS:)*

690. Medición:

Proceso para determinar un valor. *(Fuente: ISO 22.300:)*

Proceso para determinar un valor. *(Fuente: ISO 27.000:)*

691. Medida:

Variable a la que se le asigna un valor como resultado de una medición. *(Fuente: ISO 27.000:)*

692. Medida Básica:

Medida definida por medio de un atributo y el método para cuantificarlo. *(Fuente: ISO 27.000:)*

693. Medida Derivada:

Medida que se define en función de dos o más valores de medidas básicas. *(Fuente: ISO 27.000:)*

694. Medidas de efectividad (MOE):

Las medidas de efectividad son un modelo probabilístico basado en conceptos de ingeniería que permite aproximar el impacto que una acción dada tendrá en un entorno. En la guerra de información es la capacidad de atacar o defender dentro de un entorno de Internet. *(Fuente: SANS:)*

695. Medio De Transporte:

Instrumento físico del comercio internacional que transporta mercancías de un lugar a otro. *(Fuente: ISO 22.300:)*

696. Mejora:

Actividad para mejorar el desempeño. *(Fuente: ISO 9.000:)*

697. Mejora Continua:

Actividad recurrente para mejorar el desempeño. *(Fuente: ISO 27.000:)*

Actividad recurrente para mejorar el desempeño. *(Fuente: ISO 22.300:)*

698. Mejora De La Calidad:

Parte de la gestión de la calidad orientada a aumentar la capacidad de cumplir con los requisitos de la calidad. *(Fuente: ISO 9.000:)*

699. Mejorar habilidades:

Proveer a alguien, como un empleado, de habilidades más avanzadas mediante educación y capacitación adicional. *(Fuente: NICSS:)*

700. Meta:

Requisito de desempeño detallado aplicable a la organización o a partes de ella, que tiene su origen en los objetivos y que es necesario establecer y cumplir para alcanzar dichos objetivos. *(Fuente: ISO 22.300:)*

701. Meta De Gestión De La Seguridad:

Grado específico de desempeño que se requiere para lograr un objetivo de la gestión de la seguridad. *(Fuente: ISO 22.300:)*

702. Metadato:

Información que describe el contenido de un dato. *(Fuente: UNE 71.505:)*

703. Metadato Dinámico:

Información asociada a una imagen digital, aparte de los valores de píxeles, que puede cambiar en cada fotograma de una secuencia de vídeo. *(Fuente: ISO 22.300:)*

704. Metadatos:

Información que permite describir el contenido y la esencia de un material audiovisual en un formato definido. *(Fuente: ISO 22.300:)*

705. Metadatos Estáticos:

Información asociada a una imagen digital, aparte de los valores de píxeles, que no cambia con el tiempo (o al menos no cambia a lo largo de la secuencia en cuestión). *(Fuente: ISO 22.300:)*

706. Metaverso:

Un espacio virtual 3D compartido, inmersivo y persistente donde los humanos experimentan la vida de maneras que no podrían en el mundo físico. *(Fuente: NICSS:)*

707. Minería de datos:

La minería de datos es una técnica utilizada para analizar información existente, generalmente con la intención de explorar nuevas vías para hacer negocios. *(Fuente: SANS:)*

El proceso o las técnicas utilizadas para analizar grandes conjuntos de información existente y descubrir patrones o correlaciones previamente no reveladas. *(Fuente: NICSS:)*

708. Misión:

<organización> Propósito de la existencia de la organización, tal como lo expresa la alta dirección. *(Fuente: ISO 9.000:)*

709. Mitigación:

Implementación de controles apropiados para la reducción de riesgos basados en prioridades de gestión de riesgos y análisis de alternativas. *(Fuente: NICSS:)*

Limitación de cualquier consecuencia negativa de un incidente determinado. *(Fuente: ISO 22.300:)*

710. Modelo Analítico:

Algoritmo o cálculo que combina una o más medidas básicas y/o derivadas siguiendo los criterios de decisión asociados a las mismas. *(Fuente: ISO 27.000:)*

711. Modelo de amenaza:

Un modelo de amenaza se usa para describir una amenaza dada y el daño que podría causar a un sistema si tiene una vulnerabilidad. *(Fuente: SANS:)*

712. Modo promiscuo:

Cuando una máquina lee todos los paquetes de la red, independientemente de a quién estén dirigidos. Esto es usado por administradores de red para diagnosticar problemas de red, pero también por personas malintencionadas que intentan escuchar el tráfico de red (que puede contener contraseñas u otra información). *(Fuente: SANS:)*

713. Monitoreo de radiación:

El monitoreo de radiación es el proceso de recibir imágenes, datos o audio de una fuente no protegida escuchando señales de radiación. *(Fuente: SANS:)*

714. Monitores de actividad:

Los monitores de actividad buscan prevenir infecciones por virus monitoreando actividades maliciosas en un sistema, y bloqueándolas cuando sea posible. *(Fuente: SANS:)*

715. Monocultura:

La monocultura es el caso en que un gran número de usuarios ejecutan el mismo software y son vulnerables a los mismos ataques. *(Fuente: SANS:)*

716. Multi-homed:

Se dice que eres "multi-homed" si tu red está conectada directamente a dos o más proveedores de servicios de Internet (ISP). *(Fuente: SANS:)*

717. Multidifusión:

Transmisión desde un host a un conjunto determinado de hosts. *(Fuente: SANS:)*

718. Multiplexación:

Combinar múltiples señales de fuentes posiblemente distintas para transmitirlas por un único canal. *(Fuente: SANS:)*

719. Máquina de Estados:

Un sistema que avanza a través de una serie de condiciones progresivas. *(Fuente: SANS:)*

720. Máscara de Subred:

Una máscara de subred (o número) se usa para determinar la cantidad de bits usados para las partes de subred y host de la dirección. La máscara es un valor de 32 bits que usa unos para las partes de red y subred y ceros para la parte del host. *(Fuente: SANS:)*

721. Máscara de red:

Número de 32 bits que indica el rango de direcciones IP que residen en una única red/subred/superred IP. Esta especificación muestra las máscaras de red como números hexadecimales. Por ejemplo, la máscara de red para una red IP clase C se muestra como 0xffffff00. Esta máscara a menudo se muestra en otros lugares como 255.255.255.0. *(Fuente: SANS:)*

722. Método De Medición:

Secuencia lógica de operaciones, descritas genéricamente, utilizada en la cuantificación de un atributo con respecto a una escala especificada. *(Fuente: ISO 27.000:)*

723. Método de ataque:

La forma, técnica o medio que un adversario puede utilizar en un ataque contra información o un sistema de información. *(Fuente: NICSS:)*

724. Mínimo privilegio:

Mínimo privilegio es el principio de permitir a los usuarios o aplicaciones la menor cantidad de permisos necesarios para realizar su función prevista. *(Fuente: SANS:)*

725. Módulos de núcleo cargables (LKM):

Los módulos de núcleo cargables permiten agregar funcionalidad adicional directamente en el núcleo mientras el sistema está en ejecución. *(Fuente: SANS:)*

— N —

726. NAT:

Traducción de direcciones de red. Se usa para compartir una o pocas direcciones IP públicas entre un mayor número de hosts. A los hosts se les asignan direcciones IP privadas, que luego se "traducen" a una de las direcciones IP públicas. Normalmente, redes domésticas o pequeñas empresas usan NAT para compartir una sola dirección IP de un módem DSL o cable. En algunos casos se usa NAT en servidores como capa adicional de protección. *(Fuente: SANS:)*

727. NCCoE:

Una asociación público-privada del NIST que permite la creación de soluciones prácticas de ciberseguridad para industrias específicas o desafíos tecnológicos amplios y multisectoriales. *(Fuente: NICSS:)*

728. Navegador:

Un programa cliente que puede recuperar y mostrar información de servidores en la World Wide Web. *(Fuente: SANS:)*

729. Necesidades De Información:

Conocimiento necesario para gestionar los objetivos,, las metas, el riesgo y los problemas. *(Fuente: ISO 27.000:)*

730. Neuroergonomía:

El campo emergente que estudia cómo el cerebro se relaciona con el desempeño en entornos cotidianos y laborales, integrando neurociencia y ergonomía para diseñar sistemas más seguros y eficientes y entender las relaciones cerebro-desempeño. *(Fuente: NICSS:)*

731. Neuromórfico:

La computación neuromórfica es un método de computación que usa neuronas artificiales para imitar la estructura y función del cerebro humano. La palabra "neuromórfico" significa "característico de la forma del cerebro o de las neuronas". *(Fuente: NICSS:)*

732. NewSQL:

Sistema de bases de datos relacional que cierra la brecha entre SQL y NoSQL. Las bases de datos NewSQL buscan escalar y mantenerse consistentes. *(Fuente: NICSS:)*

733. Nivel De Riesgo:

Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad. *(Fuente: ISO 27.000:)*

734. No Conformidad:

Incumplimiento de un requisito. *(Fuente: ISO 22.300:)*

Incumplimiento de un requisito. *(Fuente: ISO 27.000:)*

735. No Repudio:

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron. *(Fuente: ISO 27.000:)*

736. No repudio:

El no repudio es la capacidad de un sistema para probar que un usuario específico y solo ese usuario envió un mensaje y que este no ha sido modificado. *(Fuente: SANS:)*

Proporciona la capacidad de determinar si un individuo en particular realizó una acción específica, como crear información, enviar un mensaje, aprobar información o recibir un mensaje. *(Fuente: NICSS:)*

737. Nombre de Dominio:

Un nombre de dominio localiza una organización u otra entidad en Internet. Por ejemplo, el nombre de dominio "www.sans.org" localiza una dirección de Internet para "sans.org" en el punto de Internet 199.0.0.2 y un servidor host particular llamado "www". La parte "org" del nombre de dominio refleja el propósito de la organización o entidad (en este ejemplo, "organización") y se llama dominio de nivel superior. La parte "sans" del nombre de dominio define la organización o entidad y junto con el nivel superior se llama dominio de segundo nivel. *(Fuente: SANS:)*

738. Nombre de dominio completamente calificado:

Un nombre de dominio completamente calificado es un nombre de servidor con un nombre de host seguido por el nombre completo del dominio. *(Fuente: SANS:)*

739. Norma Británica 7799:

Un código estándar de buenas prácticas que proporciona orientación sobre cómo asegurar un sistema de información. Incluye el marco de gestión, los objetivos y los requisitos de control para los sistemas de gestión de seguridad de la información. *(Fuente: SANS:)*

740. Norma De Implementación De La Seguridad:

Documento que especifica las formas autorizadas para satisfacer las necesidades de seguridad. *(Fuente: ISO 27.000:)*

741. Notificación:

Parte de un aviso al público que da información a las personas en riesgo sobre las decisiones y acciones necesarias para hacer frente a una situación de emergencia. *(Fuente: ISO 22.300:)*

742. Novato:

Una persona inexperta en una esfera o actividad particular, especialmente relacionada con la informática. *(Fuente: NICSS:)*

743. Núcleo:

El centro esencial de un sistema operativo, el núcleo que provee servicios básicos para todas las demás partes del sistema operativo. Un sinónimo es núcleo. Un kernel se puede contrastar con un shell, la parte más externa de un sistema operativo que interactúa con los comandos del usuario. Los términos kernel y shell se usan más frecuentemente en Unix y algunos otros sistemas operativos que en sistemas mainframe IBM. *(Fuente: SANS:)*

— O —

744. OAuth:

Un protocolo o marco de autorización de estándar abierto que proporciona a las aplicaciones la capacidad de acceso designado seguro. *(Fuente: NICSS:)*

745. OSI:

OSI (Interconexión de Sistemas Abiertos) es una descripción estándar o "modelo de referencia" para cómo los mensajes deben transmitirse entre dos puntos en una red de telecomunicaciones. Su propósito es guiar a los desarrolladores para que sus productos funcionen consistentemente con otros. El modelo define siete capas de funciones que ocurren en cada extremo de la comunicación. Aunque no siempre se cumple estrictamente, muchos productos lo usan para describirse. Es valioso como referencia común para educación y discusión. *(Fuente: SANS:)*

746. Objetivo:

Resultado a lograr. *(Fuente: ISO 27.000:)*

Resultado a lograr. *(Fuente: ISO 22.300:)*

747. Objetivo De Control:

Declaración que describe lo que se quiere lograr como resultado de la implementación de controles. *(Fuente: ISO 27.000:)*

748. Objetivo De La Calidad:

Objetivo relativo a la calidad. *(Fuente: ISO 9.000:)*

749. Objetivo De La Gestión De La Seguridad:

Resultado o logro específico requerido en cuanto a seguridad para cumplir la política de gestión de la seguridad. *(Fuente: ISO 22.300:)*

750. Objetivo De La Revisión:

Declaración que describe lo que se quiere lograr como resultado de una revisión. *(Fuente: ISO 27.000:)*

751. Objetivo De Las Operaciones De Seguridad:

Objetivo que se persigue o pretende con relación a las operaciones de seguridad. *(Fuente: ISO 22.300:)*

752. Objetivo Mínimo De Continuidad Del Negocio:

Nivel mínimo de servicios y/o productos que resulta aceptable para que la organización alcance sus objetivos de negocio durante una disrupción. *(Fuente: ISO 22.300:)*

753. Objetivos:

En el marco NICE, trabajo en ciberseguridad donde una persona: aplica conocimiento actual de una o más regiones, países, entidades no estatales y/o tecnologías. *(Fuente: NICSS:)*

754. Objeto:

Entidad única y diferenciada que puede ser identificada. *(Fuente: ISO 22.300:)*

Elemento caracterizado por medio de la medición de sus atributos. *(Fuente: ISO 27.000:)*

Una entidad pasiva relacionada con sistemas de información que contiene o recibe información. *(Fuente: NICSS:)*

755. Objeto De La Configuración:

Objeto dentro de una configuración que satisface una función de uso final. *(Fuente: ISO 9.000:)*

756. Objeto En Revisión:

Elemento específico que está siendo revisado. *(Fuente: ISO 27.000:)*

757. Objeto; entidad; ítem:

Cualquier cosa que puede percibirse o concebirse. *(Fuente: ISO 9.000:)*

758. Observador:

Participante que observa el ejercicio, permaneciendo separado de las actividades del ejercicio. *(Fuente: ISO 22.300:)*

<auditoría> Persona que acompaña al equipo auditor pero que no actúa como un auditor. *(Fuente: ISO 9.000:)*

759. Octeto:

Una secuencia de ocho bits. Un octeto es un byte de ocho bits. *(Fuente: SANS:)*

760. Ocultamiento (Stealthing):

Stealthing es un término que se refiere a las técnicas usadas por código malicioso para ocultar su presencia en el sistema infectado. *(Fuente: SANS:)*

761. OffSec:

El enfoque proactivo para asegurar redes y sistemas contra ataques mediante la búsqueda activa de vulnerabilidades y debilidades. *(Fuente: NICSS:)*

762. Oficial de Seguridad del Sistema (SSO):

Persona responsable de la aplicación o administración de la política de seguridad que aplica al sistema. *(Fuente: SANS:)*

763. Open Shortest Path First (OSPF):

Open Shortest Path First es un algoritmo de enrutamiento de estado de enlace usado en enrutamiento de puerta de enlace interior. Los routers mantienen una base de datos de todos los routers en el sistema autónomo con enlaces entre routers, costos de enlace y estados de enlace (arriba y abajo). *(Fuente: SANS:)*

764. OpenIOC:

Un esquema XML extensible que permite describir las características técnicas que identifican una amenaza conocida, la metodología de un atacante u otra evidencia de compromiso. *(Fuente: NICSS:)*

765. Operaciones cibernéticas:

En el marco NICE, trabajo de ciberseguridad en el que una persona realiza actividades para reunir evidencia sobre entidades criminales o de inteligencia extranjera, con el fin de mitigar amenazas reales o potenciales, proteger contra espionaje, sabotaje extranjero, terrorismo internacional o apoyar otras actividades de inteligencia. *(Fuente: NICSS:)*

766. Operaciones de recopilación:

En el Marco NICE, trabajo de ciberseguridad donde una persona ejecuta la recopilación utilizando estrategias apropiadas y dentro de las prioridades establecidas por el proceso de gestión de recolección. *(Fuente: NICSS:)*

767. Operaciones de seguridad de sistemas de información:

En el marco NICE, trabajo de ciberseguridad donde una persona: supervisa el programa de aseguramiento de la información de un sistema de información dentro o fuera del entorno de red, puede incluir deberes de adquisición (por ejemplo, Oficina de Seguridad de Sistemas de Información). *(Fuente: NICSS:)*

768. Operación De Seguridad:

Actividad y función relativa a la protección de personas y activos materiales e inmateriales. *(Fuente: ISO 22.300:)*

769. Operador Económico Autorizado:

Parte que interviene en el traslado internacional de mercancías con cualquier capacidad que le haya sido reconocida por una administración nacional aduanera, o en su nombre, que cumple con las normas de seguridad de la cadena de suministro. *(Fuente: ISO 22.300:)*

770. Operar y mantener:

Una categoría del Marco NICE que consiste en áreas especializadas responsables de proveer soporte, administración y mantenimiento necesarios para asegurar un desempeño y seguridad efectivos y eficientes del sistema TI. *(Fuente: NICSS:)*

771. Organización:

Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus objetivos. *(Fuente: ISO 27.000:)*

Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos. *(Fuente: ISO 22.300:)*

772. Organización En La Cadena De Suministro:

Entidad que:

– tras realizarse una orden de compra, fabrica, manipula, procesa, carga, consolida, descarga o recepciona bienes que en algún momento cruzan una frontera internacional o económica;

– transporta mercancías por cualquier medio en la cadena de suministro internacional con independencia de que su parte concreta de la cadena de suministro cruce fronteras nacionales (o económicas) o no; o – provee, gestiona o lleva a cabo la elaboración, la

distribución o el flujo de la información de expedición utilizada por las autoridades aduaneras o en la práctica comercial. *(Fuente: ISO 22.300:)*

773. Organización Mundial De Aduanas; Oma:

Organismo intergubernamental independiente cuya misión es mejorar la eficacia y eficiencia de las administraciones aduaneras. *(Fuente: ISO 22.300:)*

— P —

774. PIV (Identificación de Personal):

Una tarjeta de identificación emitida por una agencia federal que contiene un chip informático, que permite recibir, almacenar, recuperar y enviar información de manera segura. *(Fuente: NICSS:)*

775. PTaaS:

Solución híbrida que combina la amplitud de la automatización con la profundidad de la evaluación humana, integrada con gestión avanzada de vulnerabilidades y análisis. *(Fuente: NICSS:)*

776. PaaS (Plataforma como servicio):

Un modelo de computación en la nube donde un proveedor externo entrega herramientas de hardware y software a los usuarios a través de internet. *(Fuente: NICSS:)*

777. Panorama de amenazas:

El espectro de posibles amenazas en ciberseguridad. *(Fuente: NICSS:)*

778. Paquete:

Una parte de un mensaje transmitido a través de una red conmutada por paquetes. Una de las características clave de un paquete es que contiene la dirección de destino además de los datos. En redes IP, los paquetes a menudo se llaman datagramas. *(Fuente: SANS:)*

779. Par de Sockets:

Una manera de especificar de forma única una conexión, es decir, dirección IP de origen, puerto de origen, dirección IP de destino, puerto de destino. *(Fuente: SANS:)*

780. Parche:

Un parche es una pequeña actualización lanzada por un fabricante de software para corregir errores en programas existentes. *(Fuente: SANS:)*

781. Parte Interesada:

Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad. *(Fuente: ISO 27.000:)*

Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. *(Fuente: ISO 22.300:)*

Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad. *(Fuente: ISO 27.000:)*

782. Particiones:

Divisiones principales del espacio físico total del disco duro. *(Fuente: SANS:)*

783. Participación Activa:

Tomar parte en una actividad, evento o situación. *(Fuente: ISO 9.000:)*

784. Participante:

Persona u organización que desempeña una función relativa a un ejercicio. *(Fuente: ISO 22.300:)*

785. Patrón de ataque:

En software, descripciones de métodos comunes para explotar sistemas de software. *(Fuente: NICSS:)*

786. Peligro:

Una fuente o causa natural o provocada por el hombre de daño o dificultad. *(Fuente: NICSS:)*

Fuente de un daño potencial. *(Fuente: ISO 22.300:)*

787. Penetración:

Obtener acceso lógico no autorizado a datos sensibles al eludir las protecciones de un sistema. *(Fuente: SANS:)*

788. Pentester:

Un experto en seguridad informática que realiza pruebas de penetración. *(Fuente: NICSS:)*

789. Permiso De Desviación:

Autorización para apartarse de los requisitos originalmente especificados de un producto o servicio, antes de su realización. *(Fuente: ISO 9.000:)*

790. Permutación:

La permutación mantiene las mismas letras pero cambia la posición dentro de un texto para codificar el mensaje. *(Fuente: SANS:)*

791. Personal:

Personas que trabajan para una organización y están bajo su control. *(Fuente: ISO 22.300:)*

792. Personal De Operaciones De Seguridad:

Personas que trabajan en nombre de una organización y que participan directa o indirectamente en operaciones de seguridad. *(Fuente: ISO 22.300:)*

793. Personal De Seguridad:

Personas de una organización en la cadena de suministro a las que se han asignado funciones relacionadas con la seguridad. *(Fuente: ISO 22.300:)*

794. Personas En Riesgo:

Personas que se encuentran en una zona en la que pueden verse afectadas por un incidente. *(Fuente: ISO 22.300:)*

795. PhaaS:

Un modelo donde ciberdelincuentes ofrecen herramientas y recursos preempaquetados para phishing, como plantillas de correos maliciosos, páginas de aterrizaje y hosting, reduciendo la barrera para lanzar campañas de phishing. *(Fuente: NICSS:)*

796. Pharming:

Esta es una forma más sofisticada de ataque MITM (hombre en el medio). La sesión de un usuario es redirigida a un sitio web que se hace pasar por otro. Esto se logra corrompiendo un servidor DNS en Internet y apuntando una URL a la IP del sitio web falso. Casi todos los usuarios usan una URL como www.worldbank.com en lugar de la IP real (192.86.99.140) del sitio. Cambiando los punteros en un servidor DNS, la URL puede ser redirigida para enviar tráfico a la IP del sitio falso. En el sitio falso, las transacciones pueden ser simuladas y se puede recopilar información como credenciales de inicio de sesión. Con esto, el atacante puede acceder al sitio real www.worldbank.com y realizar transacciones usando las credenciales de un usuario válido de ese sitio. *(Fuente: SANS:)*

797. Phishing:

El uso de correos electrónicos que parecen originarse en una fuente confiable para engañar a un usuario y que ingrese credenciales válidas en un sitio web falso. Normalmente, el correo y el sitio web parecen ser parte de un banco con el que el usuario realiza negocios. *(Fuente: SANS:)*

Una forma digital de ingeniería social para engañar a individuos y obtener información sensible. *(Fuente: NICSS:)*

798. Pilas de protocolos (OSI):

Un conjunto de capas de protocolos de red que trabajan juntas. *(Fuente: SANS:)*

799. Ping de la muerte:

Un ataque que envía un paquete ICMP echo request (ping) de tamaño incorrectamente grande con la intención de desbordar los búferes de entrada de la máquina destino y hacer que se bloquee. *(Fuente: SANS:)*

800. Plan Anual De Ejercicios:

Documento en el que el plan en materia de política de ejercicios se ha traducido en metas y ejercicios, y que recoge el programa de ejercicios para un determinado año. *(Fuente: ISO 22.300:)*

801. Plan De Auditoría:

Descripción de las actividades y de los detalles acordados de una auditoría. *(Fuente: ISO 9.000:)*

802. Plan De Continuidad Del Negocio:

Procedimientos documentados que sirven de guía a una organización para responder a una disrupción y recuperar, reanudar y restablecer un nivel predefinido de actividad tras ella. *(Fuente: ISO 22.300:)*

803. Plan De Gestión:

Plan de acción claramente definido y documentado, que normalmente abarca el personal, los recursos, los servicios y las acciones clave que se necesitan para implementar el proceso de gestión. *(Fuente: ISO 22.300:)*

804. Plan De Gestión De Proyecto:

Documento que especifica qué es necesario para cumplir los objetivos del proyecto. *(Fuente: ISO 9.000:)*

805. Plan De La Calidad:

Especificación de los procedimientos y recursos asociados a aplicar, cuándo deben aplicarse y quién debe aplicarlos a un objeto específico. *(Fuente: ISO 9.000:)*

806. Plan De Respuesta:

Recopilación documentada de procedimientos e información que se elabora, recaba y mantiene actualizada para su rápida aplicación en caso de un incidente. *(Fuente: ISO 22.300:)*

807. Plan De Seguridad:

Medidas planificadas para garantizar que la seguridad se gestiona de manera adecuada. *(Fuente: ISO 22.300:)*

808. Plan de Contingencia del Usuario:

El plan de contingencia del usuario es el conjunto de métodos alternativos para continuar las operaciones comerciales si los sistemas de TI no están disponibles. *(Fuente: SANS:)*

809. Plan de Continuidad del Negocio (BCP):

Un Plan de Continuidad del Negocio es el plan para respuesta a emergencias, operaciones de respaldo y pasos de recuperación post-desastre que asegurarán la disponibilidad de recursos críticos y facilitarán la continuidad de las operaciones en una situación de emergencia. *(Fuente: SANS:)*

810. Plan de continuidad de operaciones:

Documento que establece los procedimientos para el desempeño continuo de capacidades clave y operaciones críticas durante una interrupción o posible interrupción. *(Fuente: NICSS:)*

811. Plan de recuperación ante desastres (DRP):

Un Plan de Recuperación ante Desastres es el proceso de recuperación de los sistemas de TI en caso de una interrupción o desastre. *(Fuente: SANS:)*

812. Plan de respuesta a incidentes:

Un conjunto de procedimientos predeterminados y documentados para detectar y responder a un incidente cibernético. *(Fuente: NICSS:)*

813. Planificación:

Parte de la gestión centrada en establecer los objetivos de las operaciones de seguridad y especificar los procesos operativos necesarios y los recursos asociados para cumplir los objetivos de las operaciones de seguridad. *(Fuente: ISO 22.300:)*

814. Planificación De La Calidad:

Parte de la gestión de la calidad orientada a establecer los objetivos de la calidad y a la especificación de los procesos operativos necesarios y de los recursos relacionados para lograr los objetivos de la calidad. *(Fuente: ISO 9.000:)*

815. Planificación de operaciones cibernéticas:

En el marco NICE, trabajo de ciberseguridad en el que una persona: realiza un proceso de planificación y selección conjunta en profundidad. Recolecta información y desarrolla planes operativos y órdenes detalladas que respaldan los requisitos. Lleva a cabo planificación estratégica y operativa en toda la gama de operaciones para operaciones integradas de información y ciberespacio. *(Fuente: NICSS:)*

816. Planificación de requisitos de sistemas:

En el marco NICE, trabajo en ciberseguridad donde una persona: consulta con clientes para recopilar y evaluar requisitos funcionales y traduce esos requisitos en soluciones técnicas, proporcionando orientación sobre la aplicabilidad de sistemas de información para satisfacer necesidades comerciales. *(Fuente: NICSS:)*

817. Planificación estratégica y desarrollo de políticas:

En el marco NICE, trabajo de ciberseguridad donde una persona: aplica conocimiento de prioridades para definir una entidad. *(Fuente: NICSS:)*

818. Plazo Máximo Tolerable De Disrupción:

Tiempo que tardarían los impactos adversos, que pudieran derivarse de no entregar un producto, prestar un servicio o realizar una actividad en volverse inaceptables. *(Fuente: ISO 22.300:)*

819. Poliinestación:

La poliinestación es la capacidad de una base de datos para mantener múltiples registros con la misma clave. Se usa para prevenir ataques por inferencia. *(Fuente: SANS:)*

820. Polimorfismo:

El polimorfismo es el proceso mediante el cual un software malicioso cambia su código subyacente para evitar ser detectado. *(Fuente: SANS:)*

821. Política:

Política relativa a la calidad. *(Fuente: ISO 9.000:)*

Intenciones y dirección de una organización, como las expresa formalmente su alta dirección. *(Fuente: ISO 22.300:)*

Intenciones y dirección de una organización, como las expresa formalmente su alta dirección. *(Fuente: ISO 27.000:)*

822. Política De Gestión De La Seguridad:

Las intenciones y la dirección generales de una organización, con respecto a la seguridad y al marco para el control de los procesos y actividades relativas a la seguridad que se derivan de su política y los requisitos reglamentarios y que están en consonancia con ambos. *(Fuente: ISO 22.300:)*

823. Política De La Calidad:

Política relativa a la calidad. *(Fuente: ISO 9.000:)*

824. Política De Operaciones De Seguridad:

Las intenciones y la dirección generales de una organización con respecto a las operaciones de seguridad expresadas formalmente por la alta dirección. *(Fuente: ISO 22.300:)*

825. Política Específica del Sistema:

Política escrita para un sistema o dispositivo específico. *(Fuente: SANS:)*

826. Política de Seguridad:

Un conjunto de reglas y prácticas que especifican o regulan cómo un sistema u organización provee servicios de seguridad para proteger recursos del sistema sensibles y críticos. *(Fuente: SANS:)*

827. Política de programa:

Una política de programa es una política de alto nivel que establece el tono general del enfoque de seguridad de una organización. *(Fuente: SANS:)*

828. Política de seguridad:

Una regla o conjunto de reglas aplicadas a un sistema de información para proporcionar servicios de seguridad. *(Fuente: NICSS:)*

829. Política de seguridad de la información:

Un conjunto de directivas, regulaciones, normas y prácticas que prescriben cómo una organización gestiona, protege y distribuye la información. *(Fuente: NICSS:)*

830. Política específica:

Una política específica destinada a abordar necesidades concretas dentro de una organización, como una política de contraseñas. *(Fuente: SANS:)*

831. Posesión:

La posesión es la tenencia, control y capacidad de usar información. *(Fuente: SANS:)*

832. Precursor:

Un evento observable o señal que indica que un atacante podría estar preparándose para causar un incidente. *(Fuente: NICSS:)*

833. Preparación:

Actividades para construir, mantener y mejorar capacidades de preparación para prevenir, proteger, responder y recuperarse de incidentes naturales o provocados por el hombre. *(Fuente: NICSS:)*

Actividades, programas y sistemas desarrollados e implementados con anterioridad a un incidente que se pueden utilizar para apoyar y reforzar la prevención, la protección, la respuesta y la recuperación ante disrupciones, emergencias o desastres, así como su mitigación. *(Fuente: ISO 22.300:)*

834. Preparación De La Respuesta A Incidentes:

Actividades que se realizan para preparar una respuesta a incidentes. *(Fuente: ISO 22.300:)*

835. Pretty Good Privacy (PGP)TM:

Marca registrada de Network Associates, Inc., que se refiere a un programa informático (y protocolos relacionados) que utiliza criptografía para proveer seguridad de datos para correo electrónico y otras aplicaciones en Internet. *(Fuente: SANS:)*

836. Prevención:

Medidas que permiten que una organización evite, impida o limite el impacto de un evento indeseable o de una posible disrupción. *(Fuente: ISO 22.300:)*

837. Prevención De Peligros Y Amenazas:

Proceso, prácticas, técnicas, material, productos, servicios o recursos utilizados para evitar, reducir o controlar los peligros y amenazas, así como sus riesgos asociados de todo tipo, con el fin de reducir su probabilidad o sus consecuencias potenciales. *(Fuente: ISO 22.300:)*

838. Prevención de pérdida de datos:

Un conjunto de procedimientos y mecanismos para evitar que los datos sensibles salgan de un límite de seguridad. *(Fuente: NICSS:)*

839. Preámbulo:

Un preámbulo es una señal usada en comunicaciones de red para sincronizar el tiempo de transmisión entre dos o más sistemas. El tiempo adecuado asegura que todos los sistemas interpreten correctamente el inicio de la transferencia de información. Un preámbulo define una serie específica de pulsos de transmisión que los sistemas comunicantes entienden como "alguien está a punto de transmitir datos". Esto asegura que los sistemas receptores interpreten correctamente cuándo comienza la transmisión de datos. Los pulsos usados varían según la tecnología de comunicación en uso. *(Fuente: SANS:)*

840. Privacidad:

La capacidad de los individuos para entender y controlar cómo otros pueden usar la información sobre ellos mismos. *(Fuente: NICSS:)*

841. Probabilidad (Likelihood):

Posibilidad de que algún hecho se produzca. *(Fuente: ISO 27.000:)*

842. Probabilidad <Matemática>:

Medición de la posibilidad de que algo se produzca, expresada como un número comprendido entre 0 y 1, donde 0 es la imposibilidad y 1 la certeza absoluta. *(Fuente: ISO 22.300:)*

843. Probabilidad <Posibilidad>:

Posibilidad de que algún hecho se produzca. *(Fuente: ISO 22.300:)*

844. Procedimiento:

Manera especificada de llevar a cabo una actividad o un proceso. *(Fuente: ISO 22.300:)*

Forma especificada de llevar a cabo una actividad o un proceso. *(Fuente: ISO 9.000:)*

845. Proceso:

Conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto. *(Fuente: ISO 22.300:)*

Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida. *(Fuente: ISO 27.000:)*

846. Proceso De Gestión Del Riesgo:

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo. *(Fuente: ISO 27.000:)*

847. Proceso De Medición:

Conjunto de operaciones que permiten determinar el valor de una magnitud. *(Fuente: ISO 9.000:)*

848. Producto:

Salida de una organización que puede producirse sin que se lleve a cabo ninguna transacción entre la organización y el cliente. *(Fuente: ISO 9.000:)*

849. Producto Falsificado:

Bien material que es una imitación o copia de un bien material auténtico. *(Fuente: ISO 22.300:)*

850. Producto O Servicio:

Resultado proporcionado por una organización para disfrute de sus clientes, destinatarios y partes interesadas. *(Fuente: ISO 22.300:)*

851. Producto O Servicio Crítico:

Recurso obtenido de un proveedor que, de no estar disponible, supondría una disrupción para las actividades críticas de una organización y amenazaría su supervivencia. *(Fuente: ISO 22.300:)*

852. Programa De Continuidad Del Negocio:

Proceso continuo de gestión y gobernanza respaldado por la alta dirección y dotado de los recursos adecuados para implementar y mantener la gestión de la continuidad del negocio. *(Fuente: ISO 22.300:)*

853. Programa De Ejercicios:

Serie de actividades de ejercicios diseñadas para cumplir el objetivo o la meta general. *(Fuente: ISO 22.300:)*

854. Programa De Gestión De La Seguridad:

Proceso por el que se logra un objetivo de la gestión de la seguridad. *(Fuente: ISO 22.300:)*

855. Programa De La Auditoría:

Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico. *(Fuente: ISO 9.000:)*

856. Programa De Operaciones De Seguridad:

Proceso continuo de gestión y gobernanza respaldado por la alta dirección y dotado con los recursos para garantizar que se toman las medidas necesarias para coordinar los esfuerzos encaminados a lograr los objetivos del sistema de gestión de operaciones de seguridad. *(Fuente: ISO 22.300:)*

857. Programa De Respuesta:

Plan, procesos y recursos que permiten llevar a cabo las actividades y los servicios necesarios para preservar y proteger la vida, los bienes, las operaciones y los activos críticos. *(Fuente: ISO 22.300:)*

858. Propiedad Estrella (Star):

En la propiedad estrella, un usuario no puede escribir datos a un nivel de clasificación inferior sin iniciar sesión en ese nivel de clasificación inferior. *(Fuente: SANS:)*

859. Propiedad Estrella Fuerte:

En la propiedad estrella fuerte, un usuario no puede escribir datos en niveles de clasificación superiores ni inferiores al propio. *(Fuente: SANS:)*

860. Propiedad Intrínsicamente Peligrosa:

Propiedad que supondría una amenaza inminente de muerte o lesiones corporales graves en caso de estar en manos de una persona no autorizada. *(Fuente: ISO 22.300:)*

861. Propiedad de Integridad Simple:

En la propiedad de integridad simple un usuario no puede escribir datos en un nivel de integridad superior al propio. *(Fuente: SANS:)*

862. Propiedad de Seguridad Simple:

En la propiedad de seguridad simple un usuario no puede leer datos con una clasificación superior a la propia. *(Fuente: SANS:)*

863. Propiedad estrella de integridad:

En la propiedad estrella de integridad, un usuario no puede leer datos de un nivel de integridad inferior al suyo. *(Fuente: SANS:)*

864. Propietario:

Entidad que controla legalmente los derechos de licencia y usuario y la distribución del objeto asociado al identificador único (UID). *(Fuente: ISO 22.300:)*

865. Propietario de datos:

Un Propietario de datos es la entidad que tiene la responsabilidad y autoridad sobre los datos. *(Fuente: SANS:)*

866. Protección:

Medidas que protegen a una organización de una posible disrupción y le permiten reducir su impacto. *(Fuente: ISO 22.300:)*

867. Protección Civil:

Medidas que se toman y sistemas que se implementan para preservar la vida y la salud de los ciudadanos, sus bienes y su entorno ambiental, ante eventos no deseados. *(Fuente: ISO 22.300:)*

868. Proteger y defender:

Una categoría del Marco NICE que consiste en áreas especializadas responsables de la identificación, análisis y mitigación de amenazas a sistemas o redes internas de TI. *(Fuente: NICSS:)*

869. Protegerse In Situ; Refugiarse In Situ:

Permanecer o refugiarse inmediatamente en un lugar protegido del riesgo. *(Fuente: ISO 22.300:)*

870. Protocolo:

Una especificación formal para comunicarse; un conjunto especial de reglas que los puntos finales en una conexión de telecomunicaciones usan cuando se comunican. Los protocolos existen en varios niveles dentro de una conexión de telecomunicaciones. *(Fuente: SANS:)*

871. Protocolo Ligero de Acceso a Directorios (LDAP):

Un protocolo de software para permitir a cualquiera localizar organizaciones, individuos y otros recursos como archivos y dispositivos en una red, ya sea en Internet pública o en una Intranet corporativa. *(Fuente: SANS:)*

872. Protocolo Punto a Punto (PPP):

Un protocolo para la comunicación entre dos computadoras usando una interfaz serial, típicamente una computadora personal conectada por línea telefónica a un servidor. Empaqueta los paquetes TCP/IP de tu computadora y los envía al servidor donde pueden ser puestos en Internet. *(Fuente: SANS:)*

873. Protocolo Simple de Administración de Red (SNMP):

El protocolo que regula la gestión de red y el monitoreo de dispositivos de red y sus funciones. Un conjunto de protocolos para administrar redes complejas. *(Fuente: SANS:)*

874. Protocolo de Acceso a Mensajes de Internet (IMAP):

Un protocolo que define cómo un cliente debe recuperar correo y devolver correo a un servidor de correo. IMAP está diseñado como un reemplazo o extensión del Protocolo de Oficina de Correos (POP). Está definido en RFC 1203 (v3) y RFC 2060 (v4). *(Fuente: SANS:)*

875. Protocolo de Aplicación Inalámbrica:

Una especificación para un conjunto de protocolos de comunicación que estandarizan la forma en que dispositivos inalámbricos, como teléfonos celulares y transceptores de radio, pueden usarse para acceso a Internet, incluyendo correo electrónico, la World Wide Web, grupos de noticias y chat de Internet Relay. *(Fuente: SANS:)*

876. Protocolo de Autenticación Challenge-Handshake (CHAP):

El Protocolo de Autenticación Challenge-Handshake usa un mecanismo de autenticación de desafío/respuesta donde la respuesta varía en cada desafío para prevenir ataques de repetición. *(Fuente: SANS:)*

877. Protocolo de Autenticación Extensible (EAP):

Un marco que soporta múltiples mecanismos opcionales de autenticación para PPP, incluyendo contraseñas en texto claro, desafío-respuesta, y secuencias arbitrarias de diálogo. *(Fuente: SANS:)*

878. Protocolo de Control de Transmisión (TCP):

Conjunto de reglas (protocolo) usadas junto con el Protocolo de Internet para enviar datos en forma de unidades de mensaje entre computadoras por Internet. Mientras IP se encarga de la entrega real de los datos, TCP se encarga de hacer seguimiento de las unidades individuales de datos (llamados paquetes) en que un mensaje se divide para su enrutamiento eficiente. Mientras el protocolo IP solo maneja paquetes, TCP permite que dos hosts establezcan una conexión e intercambien flujos de datos. TCP garantiza la entrega de datos y que los paquetes lleguen en el mismo orden en que fueron enviados. *(Fuente: SANS:)*

879. Protocolo de Datagramas de Usuario (UDP):

Un protocolo de comunicaciones que, al igual que TCP, funciona sobre redes IP. A diferencia de TCP/IP, UDP/IP proporciona muy pocos servicios de recuperación de errores, ofreciendo en cambio una forma directa de enviar y recibir datagramas sobre una red IP. Se usa principalmente para la transmisión de mensajes en una red. UDP utiliza el Protocolo de Internet para enviar un datagrama de una computadora a otra, pero no divide un mensaje en paquetes (datagramas) ni los reensambla en el destino. Específicamente, UDP no proporciona secuenciación de los paquetes en que llegan los datos. *(Fuente: SANS:)*

880. Protocolo de Enrutamiento Dinámico:

Permite a los dispositivos de red aprender rutas. Ej. RIP, EIGRP. El enrutamiento dinámico ocurre cuando los routers hablan con routers adyacentes, informándose mutuamente sobre a qué redes está conectado cada router. Los routers deben comunicarse usando un protocolo de enrutamiento, de los cuales hay muchos para elegir. El proceso en el router que ejecuta el protocolo de enrutamiento, comunicándose con sus routers vecinos, usualmente se llama demonio de enrutamiento. El demonio de enrutamiento actualiza la tabla de enrutamiento del kernel con la información que recibe de los routers vecinos. *(Fuente: SANS:)*

881. Protocolo de Gateway Exterior (EGP):

Un protocolo que distribuye información de enrutamiento a los routers que conectan sistemas autónomos. *(Fuente: SANS:)*

882. Protocolo de Información de Enrutamiento (RIP):

El Protocolo de Información de Enrutamiento es un protocolo vector-distancia usado para el enrutamiento de puerta de enlace interior, que utiliza el conteo de saltos como la única métrica del costo de una ruta. *(Fuente: SANS:)*

883. Protocolo de Internet (IP):

El método o protocolo mediante el cual se envían datos de una computadora a otra en Internet. *(Fuente: SANS:)*

884. Protocolo de Oficina de Correos, Versión 3 (POP3):

Un protocolo estándar de Internet por el cual una estación cliente puede acceder dinámicamente a un buzón en un servidor para recuperar mensajes de correo que el servidor ha recibido y está manteniendo para el cliente. *(Fuente: SANS:)*

885. Protocolo de Resolución Inversa de Direcciones (RARP):

RARP (Protocolo de Resolución Inversa de Direcciones) es un protocolo por el cual una máquina física en una red local puede solicitar aprender su dirección IP desde la tabla o caché del Protocolo de Resolución de Direcciones del servidor gateway. Un administrador de red crea una tabla en el router gateway de la red local que asigna las direcciones físicas (o direcciones MAC) a las direcciones IP correspondientes. Cuando se configura una nueva máquina, su cliente RARP solicita al servidor RARP en el router que le envíe su dirección IP. Asumiendo que exista una entrada en la tabla del router, el servidor RARP devuelve la dirección IP a la máquina, que puede almacenarla para uso futuro. *(Fuente: SANS:)*

886. Protocolo de Transferencia de Archivos (FTP):

Un protocolo TCP/IP que especifica la transferencia de archivos de texto *(Fuente: SANS:)*

887. Protocolo de Tunelización Punto a Punto (PPTP):

Un protocolo (conjunto de reglas de comunicación) que permite a las corporaciones extender su propia red corporativa a través de "túneles" privados sobre Internet público. *(Fuente: SANS:)*

888. Protocolo de autenticación de contraseña (PAP):

El Protocolo de Autenticación de Contraseña es un mecanismo de autenticación simple y débil donde un usuario ingresa la contraseña que luego se envía a través de la red, usualmente en texto claro. *(Fuente: SANS:)*

889. Protocolo de mensajes de control de Internet (ICMP):

Un protocolo estándar de Internet que se usa para reportar condiciones de error durante el procesamiento de datagramas IP y para intercambiar otra información relativa al estado de la red IP. *(Fuente: SANS:)*

890. Protocolo de puerta de enlace de frontera (BGP):

Un protocolo de enrutamiento entre sistemas autónomos. BGP se utiliza para intercambiar información de enrutamiento en Internet y es el protocolo utilizado entre proveedores de servicios de Internet (ISP). *(Fuente: SANS:)*

891. Protocolo de reenvío de capa 2 (L2F):

Un protocolo de Internet (desarrollado originalmente por Cisco Corporation) que utiliza túneles PPP sobre IP para crear una extensión virtual de un enlace de marcación a través de una red, iniciado por el servidor de marcación y transparente para el usuario de marcación. *(Fuente: SANS:)*

892. Protocolo de resolución de direcciones (ARP):

El Protocolo de resolución de direcciones (ARP) es un protocolo para mapear una dirección IP a una dirección física reconocida en la red local. Se usa una tabla, usualmente llamada caché ARP, para mantener la correlación entre cada dirección MAC y su correspondiente dirección IP. ARP proporciona las reglas del protocolo para hacer esta correlación y convertir direcciones en ambas direcciones. *(Fuente: SANS:)*

893. Protocolo de semáforo:

Un conjunto de designaciones que emplean cuatro colores (ROJO, ÁMBAR, VERDE y BLANCO) usado para asegurar que la información sensible se comparta con la audiencia correcta. *(Fuente: NICSS:)*

894. Protocolo de transferencia de hipertexto (HTTP):

El protocolo en la familia de protocolos Internet Protocol (IP) utilizado para transportar documentos de hipertexto a través de una red. *(Fuente: SANS:)*

895. Protocolo de túnel de capa 2 (L2TP):

Una extensión del Protocolo de Túnel Punto a Punto usada por un proveedor de servicios de Internet para habilitar la operación de una red privada virtual sobre Internet. *(Fuente: SANS:)*

896. Proveedor:

Organización que proporciona un producto o un servicio. *(Fuente: ISO 9.000:)*

897. Proveedor Crítico:

Proveedor de productos o servicios críticos. *(Fuente: ISO 22.300:)*

898. Proveedor De Nivel 1:

Proveedor de productos o servicios a una organización de manera directa normalmente mediante un acuerdo contractual. *(Fuente: ISO 22.300:)*

899. Proveedor De Nivel 2:

Proveedor de productos o servicios a una organización de manera indirecta a través del proveedor de nivel 1. *(Fuente: ISO 22.300:)*

900. Proveedor De Prc; Proveedor De Un Proceso De Resolución De Conflictos:

Persona u organización que provee y opera un proceso de resolución de conflictos externo *(Fuente: ISO 9.000:)*

901. Proveedor Externo:

Proveedor que no es parte de la organización. *(Fuente: ISO 9.000:)*

902. Provisión segura:

Una categoría del marco NICE que consiste en áreas especializadas encargadas de conceptualizar, diseñar y construir sistemas de TI seguros, con responsabilidad sobre algún aspecto del desarrollo de los sistemas. *(Fuente: NICSS:)*

903. Proxy HTTP:

Un Proxy HTTP es un servidor que actúa como intermediario en la comunicación entre clientes y servidores HTTP. *(Fuente: SANS:)*

904. Proxy directo:

Los proxies directos están diseñados para ser el servidor a través del cual se hacen todas las solicitudes. *(Fuente: SANS:)*

905. Proxy inverso:

Los proxies inversos reciben solicitudes HTTP públicas y las pasan a servidores web internos para obtener el contenido, que luego el proxy envía al usuario final. *(Fuente: SANS:)*

906. Proxyjacking:

Técnica maliciosa donde un atacante toma control del servidor proxy de una víctima, permitiéndole interceptar y manipular el tráfico de internet del objetivo. *(Fuente: NICSS:)*

907. Proyecto:

Proceso único, consistente en un conjunto de actividades coordinadas y controladas con fechas de inicio y de finalización, llevadas a cabo para lograr un objetivo conforme con requisitos específicos, incluyendo las limitaciones de tiempo, costo y recursos. *(Fuente: ISO 9.000:)*

908. Proyecto De Sgsi:

Actividades estructuradas llevadas a cabo por una organización para implementar un SGSI. *(Fuente: ISO 27.000:)*

909. Prueba:

Es la demostración en un procedimiento judicial de los hechos que fundamentan la aplicación de requerimientos formales, procesales y/o legales. *(Fuente: UNE 71.505:)*

910. Prueba Electrónica:

Es aquella evidencia electrónica que cumple con los requerimientos formales, procesales y/o legales que establezca, en cada caso, el ordenamiento jurídico aplicable. *(Fuente: UNE 71.505:)*

911. Prueba de caja blanca:

Una forma de prueba que se realiza con conocimiento de los internos de un sistema objetivo. *(Fuente: NICSS:)*

912. Prueba de penetración (pen test):

Término coloquial para test de penetración o prueba de penetración. *(Fuente: NICSS:)*

913. Prueba de penetración (penetration testing):

Una metodología de evaluación mediante la cual los evaluadores buscan vulnerabilidades e intentan evadir las características de seguridad de una red y/o sistema de información. *(Fuente: NICSS:)*

914. Prueba y evaluación:

En el marco NICE, trabajo en ciberseguridad donde una persona: desarrolla y realiza pruebas de sistemas para evaluar el cumplimiento con especificaciones y requisitos aplicando principios y métodos para la planificación rentable, evaluación, verificación y validación de características técnicas, funcionales y de desempeño (incluyendo interoperabilidad) de

sistemas o elementos de sistemas que incorporan tecnología de la información. *(Fuente: NICSS:)*

915. Pruebas de penetración:

Las pruebas de penetración se usan para evaluar la seguridad del perímetro externo de una red o instalación. *(Fuente: SANS:)*

916. Puente:

Un producto que conecta una red de área local (LAN) con otra red de área local que usa el mismo protocolo (por ejemplo, Ethernet o token ring). *(Fuente: SANS:)*

917. Puerta de enlace:

Un punto de red que actúa como entrada a otra red. *(Fuente: SANS:)*

918. Puerta lógica:

Una puerta lógica es un bloque elemental de un circuito digital. La mayoría de las puertas lógicas tienen dos entradas y una salida. Como los circuitos digitales sólo pueden entender binario, las entradas y salidas sólo pueden asumir uno de dos estados, 0 o 1. *(Fuente: SANS:)*

919. Puerta trasera:

Cualquier método por el cual usuarios autorizados o no autorizados pueden eludir las medidas de seguridad normales y obtener acceso de alto nivel. *(Fuente: NICSS:)*

920. Puerto:

Un puerto no es más que un número entero que identifica de forma única un punto final de un flujo de comunicación. Solo un proceso por máquina puede escuchar en el mismo número de puerto. *(Fuente: SANS:)*

921. Puerto Efímero:

También llamado puerto transitorio o temporal. Usualmente está del lado del cliente. Se configura cuando una aplicación cliente quiere conectarse a un servidor y se destruye cuando la aplicación cliente termina. Tiene un número elegido al azar que es mayor que 1023. *(Fuente: SANS:)*

922. Puerto de Espacio (Spanning Port):

Configura el switch para que se comporte como un hub para un puerto específico. *(Fuente: SANS:)*

923. Puerto de Origen:

El puerto que un host usa para conectarse a un servidor. Usualmente es un número mayor o igual a 1024. Se genera aleatoriamente y es diferente cada vez que se establece una conexión. *(Fuente: SANS:)*

924. Puerto de switch:

La apertura física donde se puede conectar un cable de datos. *(Fuente: NICSS:)*

925. Puerto trampa:

un mecanismo de seguridad informática configurado para detectar, desviar o contrarrestar de alguna manera intentos de uso no autorizado de información *(Fuente: NICSS:)*

926. Puertos confiables:

Los puertos confiables son puertos por debajo del número 1024 que usualmente pueden ser abiertos por el usuario root. *(Fuente: SANS:)*

927. Punto De Control Crítico:

Punto, fase o proceso en el que se pueden aplicar los controles y se puede evitar, eliminar o reducir una amenaza o un peligro a niveles aceptables. *(Fuente: ISO 22.300:)*

928. Punto De Recuperación Objetivo, Rpo:

Punto al que se restablece la información utilizada por una actividad para permitir que esta reanude su funcionamiento. *(Fuente: ISO 22.300:)*

929. Pérdida de datos:

El resultado de eliminar datos de forma involuntaria o accidental, olvidar dónde están almacenados o exponerlos a una parte no autorizada. *(Fuente: NICSS:)*

— Q —

930. QAZ:

Un gusano de red. *(Fuente: SANS:)*

931. Queja:

<satisfacción del cliente> Expresión de insatisfacción hecha a una organización, relativa a su producto o servicio, o al propio proceso de tratamiento de quejas, donde explícita o implícitamente se espera una respuesta o resolución. *(Fuente: ISO 9.000:)*

932. RTOS (Sistema operativo en tiempo real):

En un RTOS, las tareas repetidas se ejecutan dentro de un límite de tiempo estricto, mientras que en un sistema operativo de propósito general, esto no necesariamente ocurre. *(Fuente: NICSS:)*

— R —

933. Ransomware:

Malware diseñado para negar a un usuario u organización el acceso a archivos en su computadora. *(Fuente: NICSS:)*

Un tipo de malware que es una forma de extorsión. Funciona cifrando el disco duro de la víctima negándole el acceso a archivos clave. La víctima debe pagar un rescate para descifrar los archivos y obtener acceso nuevamente. *(Fuente: SANS:)*

934. Rastreo (Spidering):

El proceso mediante el cual los hackers se familiarizan con sus objetivos para obtener credenciales basadas en su actividad. *(Fuente: NICSS:)*

935. Realización Del Sistema De Gestión De La Calidad:

Proceso de establecimiento, documentación, implementación, mantenimiento y mejora continua de un sistema de gestión de la calidad. *(Fuente: ISO 9.000:)*

936. Rechazos Falsos:

Los rechazos falsos son cuando un sistema de autenticación no logra reconocer a un usuario válido. *(Fuente: SANS:)*

937. Reciclaje de datos:

Búsqueda en residuos de datos en un sistema para obtener conocimiento no autorizado de datos sensibles. *(Fuente: SANS:)*

938. Reclasificación:

Variación de la clase de un producto o servicio no conforme para hacerlo conforme a requisitos diferentes de los requisitos iniciales. *(Fuente: ISO 9.000:)*

939. Recolección de cuentas:

La recolección de cuentas es el proceso de recopilar todos los nombres de cuentas legítimas en un sistema. *(Fuente: SANS:)*

940. Reconocimiento:

El reconocimiento es la fase de un ataque donde un atacante encuentra nuevos sistemas, mapea redes y explora vulnerabilidades específicas explotables. *(Fuente: SANS:)*

941. Recopilar y operar:

Categoría del Marco NICE que incluye áreas especializadas responsables de operaciones de negación y engaño, y recopilación de información de ciberseguridad para desarrollar inteligencia. *(Fuente: NICSS:)*

942. Recorte de logs:

El recorte de logs es la eliminación selectiva de entradas de registro en un log del sistema para ocultar una vulneración. *(Fuente: SANS:)*

943. Recuperación:

Las actividades posteriores a un incidente o evento para restaurar servicios y operaciones esenciales a corto y mediano plazo, y restaurar completamente todas las capacidades a largo plazo. *(Fuente: NICSS:)*

Restablecimiento y mejora, en su caso, de las operaciones, las instalaciones, los medios de vida o las condiciones de vida de las organizaciones afectadas, incluidas las medidas para reducir los factores de riesgo. *(Fuente: ISO 22.300:)*

944. Recurso:

Activo, instalación, equipo, material, producto o residuo que tiene un valor potencial y puede utilizarse. *(Fuente: ISO 22.300:)*

945. Recurso Compartido:

Un recurso hecho público en una máquina, como un directorio (compartición de archivos) o impresora (compartición de impresoras). *(Fuente: SANS:)*

946. Recursos (Instalaciones) De Tratamiento De Información:

Cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan. *(Fuente: ISO 27.000:)*

947. Red Privada Virtual (VPN):

Una red informática lógica (es decir, artificial o simulada) de uso restringido que se construye a partir de los recursos de sistema de una red física relativamente pública (es decir, real) (como Internet), frecuentemente usando cifrado (ubicado en hosts o gateways) y frecuentemente usando túneles para enlazar la red virtual a través de la red real. Por ejemplo, si una corporación tiene LANs en varios sitios diferentes, cada una conectada a Internet mediante un firewall, la corporación podría crear una VPN (a) usando túneles cifrados para conectar firewall con firewall a través de Internet y (b) no permitiendo otro tráfico a través de los firewalls. Generalmente una VPN es más económica de construir y operar que una red real dedicada, porque la red virtual comparte el costo de recursos con otros usuarios de la red real. *(Fuente: SANS:)*

948. Red conmutada:

Una red de comunicaciones, como la red telefónica pública conmutada, en la que cualquier usuario puede conectarse a otro usuario mediante el uso de conmutación de mensajes, circuitos o paquetes y dispositivos de control. Cualquier red que provea servicio de comunicaciones conmutadas. *(Fuente: SANS:)*

949. Red conmutada por paquetes:

Una red conmutada por paquetes es aquella donde los paquetes individuales siguen sus propios caminos a través de la red desde un punto final a otro. *(Fuente: SANS:)*

950. Red de computadoras:

Una colección de computadoras anfitrionas junto con la subred o interred a través de la cual pueden intercambiar datos. *(Fuente: SANS:)*

951. Red de confianza:

Una red de confianza es la confianza que evoluciona naturalmente cuando un usuario comienza a confiar en las firmas de otros, y en las firmas en las que ellos confían. *(Fuente: SANS:)*

952. Red de conmutación de circuitos:

Una red de conmutación de circuitos es donde un solo circuito físico continuo conecta dos puntos finales y la ruta es inmutable una vez establecida. *(Fuente: SANS:)*

953. Red trampa (honeynetting):

una red configurada con vulnerabilidades intencionales alojadas en un servidor señuelo para atraer hackers *(Fuente: NICSS:)*

954. Reducción Del Riesgo:

Acciones llevadas a cabo para disminuir la probabilidad y/o las consecuencias negativas asociadas a un riesgo. *(Fuente: ISO 22.300:)*

955. Redundancia:

Sistemas, subsistemas, activos o procesos adicionales o alternativos que mantienen un grado de funcionalidad general en caso de pérdida o falla de otro sistema, subsistema, activo o proceso. *(Fuente: NICSS:)*

956. Reenvío IP:

El reenvío IP es una opción del sistema operativo que permite a un host actuar como un router. Un sistema que tiene más de una tarjeta de interfaz de red debe tener activado el reenvío IP para poder actuar como router. *(Fuente: SANS:)*

957. Registrador de teclas (keylogger):

Aunque existen usos legítimos y legales para los registradores de teclas, muchos usos son maliciosos. *(Fuente: NICSS:)*

958. Registro:

El Registro en los sistemas operativos Windows es el conjunto central de configuraciones e información requerida para ejecutar el computador con Windows. *(Fuente: SANS:)*

Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas. *(Fuente: ISO 22.300:)*

959. Registro De Riesgos:

Registro de la información relativa a los riesgos identificados. *(Fuente: ISO 22.300:)*

960. Remoting:

Tecnología que permite que un programa interactúe con los elementos internos de otro programa que se ejecuta en una máquina diferente. *(Fuente: NICSS:)*

961. Reparación:

Acción tomada sobre un producto o servicio no conforme para convertirlo en aceptable para su utilización prevista. *(Fuente: ISO 9.000:)*

962. Repojacking:

Tomar intencionalmente el control de la cuenta de un propietario o mantenedor que hospeda un repositorio. *(Fuente: NICSS:)*

963. Reproceso:

Acción tomada sobre un producto o servicio no conforme para hacerlo conforme con los requisitos. *(Fuente: ISO 9.000:)*

964. Requisito:

Necesidad o expectativa establecida, generalmente implícita u obligatoria. *(Fuente: ISO 22.300:)*

Necesidad o expectativa que está establecida, generalmente implícita u obligatoria. *(Fuente: ISO 27.000:)*

965. Requisito De La Calidad:

Requisito relativo a la calidad. *(Fuente: ISO 9.000:)*

966. Requisito Legal:

Requisito obligatorio especificado por un organismo legislativo. *(Fuente: ISO 9.000:)*

967. Requisito Reglamentario:

Requisito obligatorio especificado por una autoridad que recibe el mandato de un órgano legislativo. *(Fuente: ISO 9.000:)*

968. Resiliencia:

Capacidad que tiene una organización para absorber un entorno cambiante y adaptarse a él. *(Fuente: ISO 22.300:)*

La capacidad de adaptarse a condiciones cambiantes, prepararse para, resistir y recuperarse rápidamente de interrupciones. *(Fuente: NICSS:)*

969. Resiliencia de red:

La capacidad de una red para: (1) proveer operación continua (es decir, altamente resistente a interrupciones y capaz de operar en modo degradado si está dañada), (2) recuperarse efectivamente si ocurre una falla y (3) escalar para satisfacer demandas rápidas o impredecibles. *(Fuente: NICSS:)*

970. Resiliencia del sistema de información:

La capacidad de un sistema de información para: (1) continuar operando bajo condiciones adversas o estrés, incluso si en un estado degradado o debilitado, mientras mantiene capacidades operativas esenciales y (2) recuperarse eficazmente en un tiempo oportuno. *(Fuente: NICSS:)*

971. Responsable De La Resolución De Conflictos:

<satisfacción del cliente> Persona individual designada por un proveedor de PRC para ayudar a las partes en la resolución de un conflicto. *(Fuente: ISO 9.000:)*

972. Responsable De Seguridad Del Ejercicio:

Persona encargada de asegurarse de que cualquier acción durante el ejercicio se realiza de manera segura. *(Fuente: ISO 22.300:)*

973. Respuesta:

Una respuesta es la información enviada en reacción a algún estímulo. *(Fuente: SANS:)*

En ciberseguridad, la respuesta abarca actividades tanto automatizadas como manuales. *(Fuente: NICSS:)*

974. Respuesta A Incidentes:

Acciones llevadas a cabo con objeto de detener las causas de un peligro inminente y/o mitigar las consecuencias de eventos potencialmente desestabilizadores o de disrupciones, así como volver a una situación normal. *(Fuente: ISO 22.300:)*

975. Respuesta Echo:

Una respuesta echo es la respuesta que una máquina que ha recibido una solicitud echo envía sobre ICMP. *(Fuente: SANS:)*

976. Respuesta a incidentes:

En el marco laboral, trabajo de ciberseguridad donde una persona: Responde a crisis o situaciones urgentes dentro del dominio pertinente para mitigar amenazas inmediatas y potenciales, usa enfoques de mitigación, preparación, respuesta y recuperación según sea necesario para maximizar la supervivencia de la vida, preservación de la propiedad y seguridad de la información. Investiga y analiza todas las actividades relevantes de respuesta. *(Fuente: NICSS:)*

La respuesta a incidentes es el proceso estructurado de identificar, gestionar y mitigar los efectos de incidentes de ciberseguridad para minimizar daños, recuperar operaciones y prevenir futuras ocurrencias. *(Fuente: SANS:)*

977. Resultados De Las Mediciones:

Uno o más indicadores y sus correspondientes interpretaciones que abordan una necesidad de información. *(Fuente: ISO 27.000:)*

978. Retroalimentación:

<satisfacción del cliente> Opiniones, comentarios y muestras de interés por un producto, un servicio o un proceso de tratamiento de quejas. *(Fuente: ISO 9.000:)*

979. Revisión:

Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del sistema de gestión y sus componentes para conseguir los objetivos establecidos. *(Fuente: ISO 22.300:)*

Determinación de la conveniencia, adecuación o eficacia de un objeto para lograr unos objetivos establecidos. *(Fuente: ISO 9.000:)*

Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos. *(Fuente: ISO 27.000:)*

980. Riesgo:

Efecto de la incertidumbre sobre la consecución de los objetivos. *(Fuente: ISO 27.000:)*

La posibilidad de un resultado no deseado o adverso resultante de un incidente, evento o suceso, determinado por la probabilidad de que una amenaza particular explote una vulnerabilidad específica, junto con las consecuencias asociadas. *(Fuente: NICSS:)*

Efecto de la incertidumbre sobre los objetivos. *(Fuente: ISO 22.300:)*

Efecto de la incertidumbre. *(Fuente: ISO 9.000:)*

El riesgo es el producto del nivel de amenaza por el nivel de vulnerabilidad. Establece la probabilidad de un ataque exitoso. *(Fuente: SANS:)*

981. Riesgo Residual:

Riesgo remanente después del tratamiento del riesgo. *(Fuente: ISO 27.000:)*

Riesgo remanente después del tratamiento del riesgo. *(Fuente: ISO 22.300:)*

982. Rivest-Shamir-Adleman (RSA):

Un algoritmo para criptografía asimétrica, inventado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman. *(Fuente: SANS:)*

983. Robo de datos:

El acto deliberado o intencional de robar información. *(Fuente: NICSS:)*

984. Robustez:

Capacidad de un sistema para resistir ataques virtuales o físicos, ya sean externos o internos. *(Fuente: ISO 22.300:)*

985. Roles adyacentes a la ciberseguridad:

varios roles que tienen responsabilidades de ciberseguridad que típicamente forman solo una parte de sus responsabilidades generales dentro de una organización. *(Fuente: NICSS:)*

986. Rompimiento de contraseñas:

El rompimiento de contraseñas es el proceso de intentar adivinar contraseñas, dado el archivo de contraseñas. *(Fuente: SANS:)*

987. Root:

Root es el nombre de la cuenta de administrador en sistemas Unix. *(Fuente: SANS:)*

988. Rootkit:

Una colección de herramientas (programas) que un hacker utiliza para ocultar intrusiones y obtener acceso a nivel administrador en una computadora o red informática. *(Fuente: SANS:)*

Conjunto de herramientas de software con privilegios de acceso a nivel administrador instaladas en un sistema de información y diseñadas para ocultar su presencia, mantener los privilegios de acceso y ocultar las actividades realizadas por las herramientas. *(Fuente: NICSS:)*

989. Router:

Los routers interconectan redes lógicas reenviando información a otras redes basándose en direcciones IP. *(Fuente: SANS:)*

990. Router de filtrado:

Un router inter-red que previene selectivamente el paso de paquetes de datos según una política de seguridad. Un router de filtrado puede ser usado como firewall o parte de un firewall. Un router normalmente recibe un paquete de una red y decide a dónde reenviarlo en una segunda red. Un router de filtrado hace lo mismo, pero primero decide si el paquete debe ser reenviado en absoluto, de acuerdo con alguna política de seguridad. La política se implementa mediante reglas (filtros de paquetes) cargadas en el router. *(Fuente: SANS:)*

991. Ruta de ataque:

Los pasos que un adversario toma o puede tomar para planificar, prepararse y ejecutar un ataque. *(Fuente: NICSS:)*

— S —

992. S/Key:

Un mecanismo de seguridad que usa una función hash criptográfica para generar una secuencia de contraseñas de un solo uso de 64 bits para el ingreso remoto de usuarios. El cliente genera una contraseña de un solo uso aplicando la función hash criptográfica MD4 múltiples veces a la clave secreta del usuario. En cada autenticación sucesiva, el número de aplicaciones del hash se reduce en uno. *(Fuente: SANS:)*

993. SECaaS:

Un método basado en la nube para externalizar la ciberseguridad. *(Fuente: NICSS:)*

994. SHA1:

Una función hash criptográfica unidireccional. Véase también "MD5". *(Fuente: SANS:)*

995. SIEM:

Una solución de seguridad que ayuda a las organizaciones a detectar amenazas antes de que interrumpan el negocio. *(Fuente: NICSS:)*

996. SOCKS:

Un protocolo que un servidor proxy puede usar para aceptar solicitudes de usuarios clientes en la red de una empresa y reenviarlas a través de Internet. SOCKS usa sockets para representar y rastrear conexiones individuales. El lado cliente de SOCKS está integrado en ciertos navegadores web y el lado servidor puede añadirse a un servidor proxy. *(Fuente: SANS:)*

997. STaaS (Almacenamiento como servicio):

Una práctica de usar recursos de almacenamiento en la nube pública para guardar sus datos. *(Fuente: NICSS:)*

998. Salida:

Resultado de un proceso. *(Fuente: ISO 9.000:)*

999. Saltos:

Un salto es cada intercambio con una puerta de enlace que toma un paquete en su camino al destino. *(Fuente: SANS:)*

1000. Satisfacción Del Cliente:

Percepción del cliente sobre el grado en que se han cumplido las expectativas de los clientes. *(Fuente: ISO 9.000:)*

1001. Scareware:

Una táctica de ciberataque que asusta a las personas para que visiten sitios web falsificados o infectados o descarguen software malicioso (malware). *(Fuente: NICSS:)*

1002. SecDevOps:

Una metodología de desarrollo de software que coloca las preocupaciones de seguridad como prioridad en la planificación y desarrollo. *(Fuente: NICSS:)*

1003. SecOps:

Una combinación de los términos seguridad y operaciones; es una metodología que los gerentes de TI implementan para mejorar la conexión, colaboración y comunicación entre los equipos de seguridad de TI y operaciones de TI. *(Fuente: NICSS:)*

1004. Secreto:

Datos y/o conocimientos que se encuentran protegidos contra su divulgación a entidades no autorizadas. *(Fuente: ISO 22.300:)*

1005. Secreto hacia adelante de clave pública (PFS):

Para un protocolo de acuerdo de claves basado en criptografía asimétrica, la propiedad que asegura que una clave de sesión derivada de un conjunto de claves públicas y privadas a largo plazo no será comprometida si una de las claves privadas es comprometida en el futuro. *(Fuente: SANS:)*

1006. Secuestro de Dominio:

El secuestro de dominio es un ataque mediante el cual un atacante toma control de un dominio bloqueando primero el acceso al servidor DNS del dominio y luego poniendo su propio servidor en su lugar. *(Fuente: SANS:)*

1007. Secuestro de Sesión:

Tomar control de una sesión que alguien más ha establecido. *(Fuente: SANS:)*

1008. Secure Shell (SSH):

Un programa para iniciar sesión en otro computador a través de una red, ejecutar comandos en una máquina remota y mover archivos de una máquina a otra. *(Fuente: SANS:)*

1009. Segmento:

Segmento es otro nombre para los paquetes TCP. *(Fuente: SANS:)*

1010. Seguimiento:

Determinación del estado de un sistema, un proceso, un producto, un servicio o una actividad. *(Fuente: ISO 22.300:)*

1011. Seguimiento Logístico:

Medio de identificar cada uno de los bienes materiales o lotes o series para saber dónde ha estado y dónde está en la cadena la suministro. *(Fuente: ISO 22.300:)*

1012. Seguridad:

Cualidad de encontrarse exento de peligro o amenazas. *(Fuente: ISO 22.300:)*

1013. Seguridad (de personas):

La seguridad es la necesidad de asegurar que las personas involucradas con la empresa, incluyendo empleados, clientes y visitantes, estén protegidas de daños. *(Fuente: SANS:)*

1014. Seguridad De La Información:

Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Puede, además, abarcar otras propiedades, como la autenticidad, responsabilidad, fiabilidad y el no repudio. *(Fuente: UNE 71.505:)*

Preservación de la confidencialidad, la integridad y la disponibilidad de la información. *(Fuente: ISO 27.000:)*

1015. Seguridad de Protocolo de Internet (IPsec):

Un estándar en desarrollo para la seguridad en la capa de red o de procesamiento de paquetes en la comunicación en red. *(Fuente: SANS:)*

1016. Seguridad de la información:

La seguridad de la información (InfoSec) se refiere a la práctica de proteger la información contra acceso no autorizado, divulgación, alteración, destrucción o interrupción. *(Fuente: SANS:)*

Los procesos y herramientas diseñados y desplegados para proteger información empresarial sensible contra modificación, interrupción, destrucción e inspección. *(Fuente: NICSS:)*

1017. Seguridad en la Capa de Transporte (TLS):

Protocolo que asegura privacidad entre aplicaciones que se comunican y sus usuarios en Internet. Cuando un servidor y cliente se comunican, TLS asegura que ningún tercero pueda interceptar o manipular mensajes. TLS es el sucesor del Secure Sockets Layer. *(Fuente: SANS:)*

1018. Sello De Tiempo:

Fecha y hora asignada por medios electrónicos a un fichero electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del fichero. *(Fuente: UNE 71.505:)*

1019. Separación de Funciones:

La separación de funciones es el principio de dividir privilegios entre múltiples individuos o sistemas. *(Fuente: SANS:)*

1020. Separación física:

La separación o aislamiento físico de un sistema respecto de otros sistemas o redes. *(Fuente: NICSS:)*

1021. Servicio:

Salida de una organización con al menos una actividad, necesariamente llevada a cabo entre la organización y el cliente. *(Fuente: ISO 9.000:)*

1022. Servicio Al Cliente:

Interacción de la organización con el cliente a lo largo del ciclo de vida de un producto o un servicio. *(Fuente: ISO 9.000:)*

1023. Servicio al cliente y soporte técnico:

En el marco NICE, trabajo de ciberseguridad donde la persona resuelve problemas, instala, configura, soluciona errores, da mantenimiento y brinda capacitación en respuesta a necesidades o consultas de los clientes. *(Fuente: NICSS:)*

1024. Servicio de control de acceso:

Servicio de seguridad que protege los recursos del sistema contra accesos no autorizados. Los dos mecanismos básicos para implementar este servicio son las ACL y los tickets. *(Fuente: SANS:)*

1025. Servicios de red:

En el marco NICE, trabajo de ciberseguridad donde una persona: instala, configura, prueba, opera, mantiene y administra redes y sus firewalls, incluyendo hardware (ej.: hubs, bridges, switches, multiplexores, routers, cables, servidores proxy y sistemas distribuidos protectores) y software que permiten compartir y transmitir todo el espectro de transmisiones de información para apoyar la seguridad de la información y sistemas de información. *(Fuente: NICSS:)*

1026. Servidor:

Una entidad de sistema que provee un servicio en respuesta a solicitudes de otras entidades de sistema llamadas clientes. *(Fuente: SANS:)*

1027. Servidor proxy:

Un servidor que actúa como intermediario entre un usuario de estación de trabajo y la Internet para que la empresa pueda asegurar la seguridad, control administrativo y servicio de caché. Un servidor proxy está asociado o es parte de un servidor gateway que separa la red empresarial de la red externa y un servidor firewall que protege la red empresarial de intrusiones externas. *(Fuente: SANS:)*

1028. Servidor web:

Un proceso de software que se ejecuta en un equipo anfitrión conectado a Internet para responder a solicitudes HTTP de documentos desde navegadores web cliente. *(Fuente: SANS:)*

1029. Sesión:

Una sesión es una conexión virtual entre dos hosts a través de la cual se transmite tráfico de red. *(Fuente: SANS:)*

1030. Sesión nula:

Conocida como inicio de sesión anónimo, es un método que permite a un usuario anónimo obtener información como nombres de usuario y recursos compartidos en la red o conectarse sin autenticación. Es utilizada por aplicaciones como explorer.exe para enumerar recursos compartidos en servidores remotos. *(Fuente: SANS:)*

1031. Señuelo o honeypot:

un mecanismo de seguridad informática configurado para detectar, desviar o contrarrestar de alguna manera intentos de uso no autorizado de información *(Fuente: NICSS:)*

1032. Shell:

Término Unix para la interfaz de usuario interactiva con un sistema operativo. El shell es la capa de programación que entiende y ejecuta los comandos que un usuario ingresa. En algunos sistemas, el shell se llama intérprete de comandos. Usualmente implica una interfaz con sintaxis de comandos (como el sistema operativo DOS con sus prompts "C:>" y comandos como "dir" y "edit"). *(Fuente: SANS:)*

1033. Sin contraseña:

Un método de autenticación en el que un usuario puede iniciar sesión en un sistema informático sin ingresar una contraseña u otro secreto basado en conocimiento. *(Fuente: NICSS:)*

1034. Sincronización:

La sincronización es la señal compuesta por un patrón distintivo de bits que el hardware de red busca para indicar el inicio de un marco. *(Fuente: SANS:)*

1035. Sistema:

Conjunto de elementos interrelacionados o que interactúan. *(Fuente: ISO 9.000:)*

1036. Sistema De Alerta A La Comunidad:

Método que permite comunicar información al público general a través de redes establecidas. *(Fuente: ISO 22.300:)*

1037. Sistema De Aviso Al Público:

Conjunto de protocolos, procesos y tecnologías basados en la política de avisos al público para enviar mensajes de notificación y alerta en una situación de emergencia en evolución a personas en riesgo y a primeros intervinientes. *(Fuente: ISO 22.300:)*

1038. Sistema De Gestión:

Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos. *(Fuente: ISO 27.000:)*

Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos. *(Fuente: ISO 22.300:)*

1039. Sistema De Gestión De Atributos De Datos; Adms:

Sistema que almacena, gestiona y controla el acceso a datos correspondientes a objetos. *(Fuente: ISO 22.300:)*

1040. Sistema De Gestión De Evidencias Electrónicas, Sgee:

Parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar de manera segura la administración de las evidencias electrónicas. *(Fuente: UNE 71.505:)*

1041. Sistema De Gestión De Incidentes:

Sistema que define los roles y las responsabilidades del personal y los procedimientos operativos que se tienen que utilizar durante la gestión de incidentes. *(Fuente: ISO 22.300:)*

1042. Sistema De Gestión De La Calidad:

Parte de un sistema de gestión relacionada con la calidad. *(Fuente: ISO 9.000:)*

1043. Sistema De Gestión De La Continuidad Del Negocio; Sgcn:

Parte del sistema de gestión general que establece, implementa, opera, realiza el seguimiento, revisa, mantiene y mejora la continuidad del negocio. *(Fuente: ISO 22.300:)*

1044. Sistema De Gestión De Las Mediciones:

Conjunto de elementos interrelacionados, o que interactúan, necesarios para lograr la confirmación metrológica y el control de los procesos de medición. *(Fuente: ISO 9.000:)*

1045. Sistema De Gestión De Seguridad De La Información, Sgsi:

Parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. *(Fuente: UNE 71.505:)*

1046. Sistema De Grabación En Circuito Cerrado; Sistema Cctv:

Sistema de vigilancia compuesto de cámaras, grabadoras, interconexiones y pantallas que se usa para vigilar las actividades en un comercio, una empresa o, más en general, una infraestructura específica y/o un lugar público. *(Fuente: ISO 22.300:)*

1047. Sistema De Información:

Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información. *(Fuente: ISO 27.000:)*

<sistema de gestión de la calidad> Red de canales de comunicación utilizados dentro de una organización. *(Fuente: ISO 9.000:)*

1048. Sistema De Mando Y Control:

Sistema que da apoyo a una gestión de emergencias eficaz de todos los activos en un proceso de preparación, respuesta a incidentes, continuidad y/o recuperación. *(Fuente: ISO 22.300:)*

1049. Sistema autónomo:

Una red o serie de redes que están bajo un mismo control administrativo. A veces también se le llama dominio de enrutamiento. A un sistema autónomo se le asigna un número único global, a veces llamado Número de Sistema Autónomo (ASN). *(Fuente: SANS:)*

1050. Sistema de Archivos Rápido:

La primera revisión mayor al sistema de archivos Unix, proporcionando acceso de lectura más rápido y acceso de escritura más rápido (demorado, asincrónico) a través de un caché de disco y mejor diseño del sistema de archivos en disco. Usa inodos (punteros) y bloques de datos. *(Fuente: SANS:)*

1051. Sistema de Nombres de Dominio (DNS):

El sistema de nombres de dominio (DNS) es la forma en que los nombres de dominio de Internet son localizados y traducidos en direcciones de Protocolo de Internet. Un nombre de dominio es un "identificador" significativo y fácil de recordar para una dirección de Internet. *(Fuente: SANS:)*

1052. Sistema de Prevención de Intrusiones de Voz (IPS):

El Voice IPS es un sistema de gestión de seguridad para redes de voz que monitorea el tráfico de voz para múltiples patrones de llamada o firmas de ataques/abusos para detectar y

prevenir proactivamente fraudes en llamadas, Denegación de Servicio, ataques telecom, abuso de servicios y otras actividades anómalas. *(Fuente: SANS:)*

1053. Sistema de control industrial:

Un sistema de información usado para controlar procesos industriales como manufactura, manejo de productos, producción y distribución o para controlar activos de infraestructura. *(Fuente: NICSS:)*

1054. Sistema de prevención y detección de intrusiones (IDPS):

Software que automatiza el proceso de monitoreo de eventos que ocurren en un sistema informático o red y los analiza para detectar indicios de posibles incidentes, intentando detener los incidentes posibles detectados. *(Fuente: NICSS:)*

1055. Sistema de ventanas:

Un sistema de ventanas es un sistema para compartir los recursos de presentación gráfica de una computadora entre múltiples aplicaciones al mismo tiempo. En una computadora con interfaz gráfica (GUI), puedes usar varias aplicaciones a la vez (esto se llama multitarea). Usando una ventana separada para cada aplicación, puedes interactuar con cada una y cambiar entre ellas sin reiniciarlas. Tener diferentes informaciones o actividades en varias ventanas también puede facilitar el trabajo. Un sistema de ventanas utiliza un gestor de ventanas para rastrear la ubicación, tamaño y estado de cada ventana en la pantalla. No solo gestiona ventanas sino también otras formas de entidades gráficas de la interfaz. *(Fuente: SANS:)*

1056. Sitio de Recuperación ante Desastres Frío/Templado/Caliente:

* Sitio caliente. Contiene hardware y software completamente redundantes, con conectividad de telecomunicaciones, teléfono y servicios públicos para continuar todas las operaciones del sitio principal. El cambio por fallo ocurre en minutos u horas, tras un desastre. Usualmente ocurre una sincronización diaria de datos entre el sitio principal y el sitio caliente, resultando en una pérdida mínima o nula de datos. Se pueden obtener y entregar cintas de respaldo de datos fuera del sitio para ayudar a restaurar las operaciones. Las cintas de respaldo deben ser probadas regularmente para detectar corrupción de datos, código malicioso y daños ambientales. Un sitio caliente es la opción más costosa. * Sitio templado. Contiene hardware

y software parcialmente redundantes, con conectividad de telecomunicaciones, teléfono y servicios públicos para continuar algunas, pero no todas, las operaciones del sitio principal. El cambio por fallo ocurre en horas o días, tras un desastre. Usualmente ocurre una sincronización diaria o semanal de datos entre el sitio principal y el sitio templado, resultando en una pérdida mínima de datos. Se deben obtener y entregar cintas de respaldo de datos fuera del sitio para restaurar operaciones. Un sitio templado es la segunda opción más costosa. * Sitio frío. El hardware es ordenado, enviado e instalado, y el software es cargado. La conectividad básica de telecomunicaciones, teléfono y servicios públicos puede necesitar ser activada para continuar algunas, pero no todas, las operaciones del sitio principal. La reubicación ocurre en semanas o más, dependiendo del tiempo de llegada del hardware, tras un desastre. No ocurre sincronización de datos entre el sitio principal y el sitio frío, y podría resultar en una pérdida significativa de datos. Se deben obtener y entregar cintas de respaldo de datos fuera del sitio para restaurar operaciones. Un sitio frío es la opción menos costosa. *(Fuente: SANS:)*

1057. SlowLoris:

Una herramienta de ataque diseñada para derribar un servidor inundándolo con solicitudes HTTP incompletas, sin usar mucho ancho de banda. *(Fuente: NICSS:)*

1058. Smishing:

Smishing es una combinación de los términos "SMS" y "phishing". Es similar al phishing, pero se refiere a mensajes fraudulentos enviados por SMS (mensajes de texto) en lugar de correo electrónico. *(Fuente: SANS:)*

Similar a phishing y vishing. *(Fuente: NICSS:)*

1059. SoC (Centro de Operaciones de Seguridad):

Un centro de inteligencia para la empresa, que recopila datos de las redes, servidores, puntos finales y otros activos digitales de la organización, utilizando automatización inteligente para identificar, priorizar y responder a posibles amenazas cibernéticas. *(Fuente: NICSS:)*

1060. SoD (Segregación de funciones):

Un control interno diseñado para prevenir errores y fraudes asegurando que al menos dos personas sean responsables de las partes separadas de cualquier tarea. *(Fuente: NICSS:)*

1061. Sobre digital:

Un sobre digital es un mensaje cifrado con la clave de sesión cifrada. *(Fuente: SANS:)*

1062. Sobreajuste:

Un comportamiento indeseable en aprendizaje automático que ocurre cuando el modelo da predicciones precisas para los datos de entrenamiento pero no para datos nuevos. *(Fuente: NICSS:)*

1063. Sobrecarga:

Obstáculo para la operación del sistema al imponer una carga excesiva en las capacidades de rendimiento de un componente del sistema. *(Fuente: SANS:)*

1064. Socio Comercial:

Contratista o proveedor de bienes o servicios con el que la organización celebra un contrato para recibir soporte en su función como organización de la cadena de suministro. *(Fuente: ISO 22.300:)*

1065. Socket:

El socket indica a la pila IP de un host dónde conectar un flujo de datos para que se conecte a la aplicación correcta. *(Fuente: SANS:)*

1066. Software:

Programas informáticos (que se almacenan y ejecutan en hardware de computadora) y datos asociados (que también se almacenan en el hardware) que pueden ser escritos o modificados dinámicamente durante la ejecución. *(Fuente: SANS:)*

1067. Software antispyware:

Un programa especializado en detectar, bloquear o eliminar formas de software espía. *(Fuente: NICSS:)*

1068. Software antivirus:

Un programa que monitorea una computadora o red para detectar o identificar tipos principales de código malicioso y prevenir o contener incidentes de malware. *(Fuente: NICSS:)*

1069. Software delictivo (crimeware):

Clase de malware diseñado específicamente para automatizar delitos cibernéticos. *(Fuente: NICSS:)*

1070. Software malicioso:

Un término general que abarca todos los tipos de software malicioso en computadoras y dispositivos electrónicos. *(Fuente: NICSS:)*

1071. Solicitud Echo:

Una solicitud echo es un mensaje ICMP enviado a una máquina para determinar si está en línea y cuánto tiempo tarda el tráfico en llegar a ella. *(Fuente: SANS:)*

1072. Solicitud de Comentario (RFC):

Una serie de notas sobre Internet, iniciadas en 1969 (cuando Internet era ARPANET). Un documento de Internet puede ser enviado a la IETF por cualquiera, pero la IETF decide si el documento se convierte en un RFC. Eventualmente, si gana suficiente interés, puede evolucionar a un estándar de Internet. *(Fuente: SANS:)*

1073. Solución De Autenticación:

Conjunto íntegro de medios y procedimientos que permite llevar a cabo la autenticación de un bien material. *(Fuente: ISO 22.300:)*

1074. Soporte de infraestructura para defensa de redes informáticas:

En el Marco NICE, trabajo de ciberseguridad donde una persona prueba, implementa, despliega, mantiene, revisa y administra el hardware y software necesarios para gestionar eficazmente la red y recursos del proveedor de servicios de defensa de red. *(Fuente: NICSS:)*

1075. Spam:

Correo electrónico no deseado o publicaciones no deseadas en grupos de noticias. *(Fuente: SANS:)*

El abuso de sistemas de mensajería electrónica para enviar masivamente mensajes no solicitados de forma indiscriminada. *(Fuente: NICSS:)*

1076. Spyware (software espía):

Software que se instala secreta o furtivamente en un sistema de información sin el conocimiento del usuario o propietario del sistema. *(Fuente: NICSS:)*

1077. Subred:

Una parte identificable por separado de una red mayor que típicamente representa un número limitado de computadoras host, los hosts en un edificio o área geográfica, o los hosts en una red local individual. *(Fuente: SANS:)*

1078. Sujeto:

Una entidad activa. *(Fuente: NICSS:)*

1079. Suma de comprobación:

Un valor que es calculado por una función dependiente del contenido de un objeto de datos y se almacena o transmite junto con el objeto, con el propósito de detectar cambios en los datos. *(Fuente: SANS:)*

1080. Superficie de ataque:

Características de un sistema de información que permiten a un adversario explorar, atacar o mantener presencia en el sistema. *(Fuente: NICSS:)*

1081. Superficie de ataque dinámica:

Cambios automáticos y en tiempo real de las características de un sistema de información para frustrar las acciones de un adversario. *(Fuente: NICSS:)*

1082. Supervisión y desarrollo:

Una categoría del Marco NICE que consiste en áreas especializadas que proveen liderazgo, gestión, dirección y/o desarrollo y defensa para que todos los individuos y la organización puedan realizar eficazmente el trabajo en ciberseguridad. *(Fuente: NICSS:)*

1083. Supervisión, Seguimiento O Monitorización:

Determinación del estado de un sistema, un proceso o una actividad. *(Fuente: ISO 27.000:)*

1084. Suplantación:

Un tipo de ataque de phishing dirigido donde un actor malicioso finge ser otra persona u otra entidad para robar datos sensibles. *(Fuente: NICSS:)*

1085. Suplantación (Spoof):

Intento de una entidad no autorizada de obtener acceso a un sistema haciéndose pasar por un usuario autorizado. *(Fuente: SANS:)*

1086. Suplantación (spoofing):

La inducción deliberada de un usuario o recurso para que tome una acción incorrecta. Nota: hacerse pasar por otro, disfrazarse, aprovecharse y mimetizar son formas de suplantación. *(Fuente: NICSS:)*

1087. Suplantación de IP:

La técnica de suministrar una dirección IP falsa. *(Fuente: SANS:)*

1088. Switch:

Un switch es un dispositivo de red que mantiene un registro de las direcciones MAC asociadas a cada uno de sus puertos para que los datos solo se transmitan en los puertos que son el destinatario previsto de los datos. *(Fuente: SANS:)*

1089. SysOp (Administrador de sistemas):

Responsable del mantenimiento y conservación de servidores, redes y otra infraestructura TI. *(Fuente: NICSS:)*

1090. Syslog:

Syslog es la instalación de registro de sistemas para sistemas Unix. *(Fuente: SANS:)*

— T —

1091. T1, T3:

Circuito digital que usa TDM (Multiplexación por División de Tiempo). *(Fuente: SANS:)*

1092. TCP Wrapper:

Paquete de software que puede usarse para restringir el acceso a ciertos servicios de red basado en la fuente de la conexión; una herramienta sencilla para monitorear y controlar el tráfico de red entrante. *(Fuente: SANS:)*

1093. TCP/IP:

Sinónimo de "Conjunto de Protocolos de Internet", donde el Protocolo de Control de Transmisión y el Protocolo de Internet son partes importantes. TCP/IP es el lenguaje o protocolo básico de comunicación de Internet. También puede usarse como protocolo de comunicaciones en una red privada (Intranet o Extranet). *(Fuente: SANS:)*

1094. TCPDump:

TCPDump es un analizador de protocolos gratuito para Unix que puede monitorear el tráfico de red en un cable. *(Fuente: SANS:)*

1095. TELNET:

Protocolo estándar de Internet basado en TCP y en la capa de aplicación para inicio de sesión remoto de un host a otro. *(Fuente: SANS:)*

1096. Tablas de Hosts Estáticas:

Las tablas de hosts estáticas son archivos de texto que contienen el mapeo entre nombres de host y direcciones. *(Fuente: SANS:)*

1097. Tapas de red:

Los taps de red son dispositivos de hardware que se conectan directamente al cable de red y envían una copia del tráfico que pasa por él a uno o más dispositivos conectados en red. *(Fuente: SANS:)*

1098. Tarjeta Inteligente:

Una tarjeta inteligente es una credencial electrónica que incluye una banda magnética o chip que puede grabar y reproducir una clave establecida. *(Fuente: SANS:)*

1099. Tasa De Falsos Aceptados:

Proporción de autenticaciones que se han declarado erróneamente como correctas. *(Fuente: ISO 22.300:)*

1100. Tasa De Falsos Rechazos:

Proporción de autenticaciones que se han declarado erróneamente como incorrectas. *(Fuente: ISO 22.300:)*

1101. Tecnología de la información:

Cualquier equipo o sistema interconectado o subsistema de equipo que procesa, transmite, recibe o intercambia datos o información. *(Fuente: NICSS:)*

1102. Tecnología de la información y comunicaciones (TIC):

Cualquier tecnología de la información, equipo o sistema o subsistema interconectado de equipos que procesa, transmite, recibe o intercambia datos o información. *(Fuente: NICSS:)*

1103. Tecnología operativa:

Los sistemas de hardware y software usados para operar dispositivos de control industrial. *(Fuente: NICSS:)*

1104. Tenedor De Derechos:

Entidad jurídica que tiene uno o varios derechos de propiedad intelectual o está autorizada para hacer uso de ellos. *(Fuente: ISO 22.300:)*

1105. Texto cifrado:

Texto cifrado es la forma encriptada del mensaje que se está enviando. *(Fuente: SANS:)*

Datos o información en su forma cifrada. *(Fuente: NICSS:)*

1106. Texto plano:

Texto ordinario legible antes de ser cifrado en texto cifrado o después de ser descifrado. *(Fuente: SANS:)*

Información sin encriptar. *(Fuente: NICSS:)*

1107. Ticket:

En control de acceso, datos que autentican la identidad de un cliente o un servicio y que, junto con una clave de cifrado temporal (clave de sesión), forman una credencial. *(Fuente: NICSS:)*

1108. Tiempo Objetivo De Recuperación, Rto:

Tiempo en el que se reanuda un producto o servicio o una actividad, o se recuperan los recursos, tras un incidente. *(Fuente: ISO 22.300:)*

1109. Tiempo de vida:

Un valor en un paquete del Protocolo de Internet que indica a un router de red si el paquete ha estado demasiado tiempo en la red y debe ser descartado. *(Fuente: SANS:)*

1110. Todos Los Peligros:

Eventos que ocurren de manera natural, eventos inducidos por los seres humanos (tanto intencionados como no intencionados) y eventos provocados por la tecnología con un impacto potencial sobre una organización, una comunidad o la sociedad y el entono ambiental del cual esta depende. *(Fuente: ISO 22.300:)*

1111. Token Ring:

Una red Token Ring es una red de área local en la que todas las computadoras están conectadas en una topología de anillo o estrella y se usa un dígito binario o esquema de paso de token para prevenir la colisión de datos entre dos computadoras que quieran enviar mensajes al mismo tiempo. *(Fuente: SANS:)*

1112. Token trampa (honeytoken):

un recurso informático falso creado y posicionado en un sistema o red para parecer valioso a los ciberdelincuentes, pero que en realidad se utiliza para rastrear y detectar intentos de hackeo *(Fuente: NICSS:)*

1113. Tolerancia Al Riesgo:

Disponibilidad de una organización o de las partes interesadas para soportar el riesgo después del tratamiento del riesgo con objeto de conseguir sus objetivos. *(Fuente: ISO 22.300:)*

1114. Tonalidad:

Atributo de la sensación visual por el que una superficie parece similar a uno de los colores percibidos, rojo, amarillo, verde y azul, o a una combinación de dos de ellos. *(Fuente: ISO 22.300:)*

1115. Topología:

La disposición geométrica de un sistema informático. Las topologías comunes incluyen bus, estrella y anillo. La disposición específica física (real) o lógica (virtual) de los elementos de una red. Nota 1: Dos redes tienen la misma topología si la configuración de conexiones es

igual, aunque puedan diferir en interconexiones físicas, distancias, tasas de transmisión y/o tipos de señal. Nota 2: Se ilustran los tipos comunes de topología de red. *(Fuente: SANS:)*

1116. Traceroute (tracert.exe):

Traceroute es una herramienta que mapea la ruta que un paquete toma desde la máquina local a un destino remoto. *(Fuente: SANS:)*

1117. Traducción de direcciones de red:

La traducción de una dirección de protocolo de Internet utilizada dentro de una red a una dirección IP diferente conocida dentro de otra red. Una red se designa como la red interna y la otra como la externa. *(Fuente: SANS:)*

1118. Tramas:

Datos transmitidos entre puntos de red como una unidad completa con direccionamiento e información necesaria de control de protocolo. Una trama generalmente se transmite en serie bit a bit y contiene un campo de encabezado y un campo de remolque que "enmarca" los datos. (Algunas tramas de control no contienen datos.) *(Fuente: SANS:)*

1119. Transacciones Electrónicas Seguras (SET):

Transacciones Electrónicas Seguras es un protocolo desarrollado para transacciones con tarjeta de crédito en el cual todas las partes (clientes, comerciantes y banco) son autenticadas usando firmas digitales, la encriptación protege el mensaje y provee integridad, y ofrece seguridad de extremo a extremo para transacciones con tarjeta de crédito en línea. *(Fuente: SANS:)*

1120. Tratamiento Del Riesgo:

Proceso destinado a modificar el riesgo. *(Fuente: ISO 27.000:)*

Proceso destinado a modificar el riesgo. *(Fuente: ISO 22.300:)*

1121. Trazabilidad:

Capacidad para seguir el histórico, la aplicación o la localización de un objeto. *(Fuente: ISO 9.000:)*

1122. Triple DES:

Un cifrado por bloques basado en DES que transforma cada bloque de texto plano de 64 bits aplicando el Algoritmo de Cifrado de Datos tres veces sucesivas, usando dos o tres claves diferentes, para una longitud efectiva de clave de 112 o 168 bits. *(Fuente: SANS:)*

1123. Triple Envolvimiento:

Uso en S/MIME: datos que han sido firmados con una firma digital, luego cifrados, y luego firmados nuevamente. *(Fuente: SANS:)*

1124. Trojanizar:

Convertir en un troyano. *(Fuente: NICSS:)*

1125. Troyano:

Un tipo de malware que oculta su verdadero contenido para engañar a un usuario y hacerle pensar que es un archivo inofensivo. *(Fuente: NICSS:)*

1126. Trunking:

Trunking es conectar switches juntos para que puedan compartir información de VLAN entre ellos. *(Fuente: SANS:)*

1127. Typosquatting:

Una forma de cybersquatting (ocupar sitios bajo la marca o derechos de autor de otra persona) que apunta a usuarios de Internet que escriben incorrectamente la dirección de un sitio web en su navegador. *(Fuente: NICSS:)*

1128. Técnicas de rejilla:

Las técnicas de rejilla usan designaciones de seguridad para determinar el acceso a la información. *(Fuente: SANS:)*

1129. Túnel:

Un canal de comunicación creado en una red informática al encapsular los paquetes de datos de un protocolo de comunicación dentro (encima) de un segundo protocolo que normalmente se transportaría por encima, o en la misma capa que, el primero. Generalmente, un túnel es un enlace lógico punto a punto — es decir, una conexión de capa 2 del modelo OSI — creada al encapsular el protocolo de capa 2 en un protocolo de transporte (como TCP), en un protocolo de capa de red o interred (como IP), o en otro protocolo de capa de enlace. El tunelizado puede mover datos entre computadoras que usan un protocolo no soportado por la red que las conecta. *(Fuente: SANS:)*

— U —

1130. UIT-T:

Unión Internacional de Telecomunicaciones, Sector de Normalización de Telecomunicaciones (antes "CCITT"), una organización de tratado de Naciones Unidas compuesta principalmente por autoridades postales, telefónicas y telegráficas de países miembros y que publica estándares llamados "Recomendaciones". *(Fuente: SANS:)*

1131. Unicast:

Transmisión de host a host. *(Fuente: SANS:)*

1132. Unidad De Medida:

Cantidad concreta, definida y adoptada por convenio, con la cual se comparan otras cantidades de la misma naturaleza a fin de expresar su magnitud en relación a dicha cantidad. *(Fuente: ISO 27.000:)*

1133. Unidad De Transporte De Carga:

Vehículo para el transporte de mercancías por carretera, vagón para el transporte de mercancías por ferrocarril, contenedor de carga, vehículo cisterna de carretera, vagón cisterna o cisterna móvil. *(Fuente: ISO 22.300:)*

1134. Unix:

Un sistema operativo multitarea y multiusuario popular desarrollado en Bell Labs a principios de los años 70. Creado por un pequeño grupo de programadores, Unix fue diseñado para ser un sistema pequeño y flexible usado exclusivamente por programadores. *(Fuente: SANS:)*

1135. Usuario:

Una persona, entidad organizacional o proceso automatizado que accede a un sistema, ya sea autorizado para hacerlo o no. *(Fuente: SANS:)*

— V —

1136. Validación:

Confirmación, mediante la aportación de evidencia objetiva, de que se han cumplido los requisitos para una utilización o aplicación específica prevista. *(Fuente: ISO 9.000:)*

Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos para una utilización o aplicación específica prevista. *(Fuente: ISO 27.000:)*

1137. Valor hash:

Un valor numérico resultante de aplicar un algoritmo matemático a un conjunto de datos, como un archivo. *(Fuente: NICSS:)*

1138. Valoración:

Proceso sistemático que compara los resultados de una medición con criterios reconocidos para determinar las discrepancias entre el desempeño pretendido y el real. *(Fuente: ISO 22.300:)*

1139. Valoración Del Riesgo:

Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables. *(Fuente: ISO 22.300:)*

1140. Vector de amenaza:

El método que una amenaza usa para llegar al objetivo. *(Fuente: SANS:)*

1141. Vector de distancia:

Los vectores de distancia miden el costo de las rutas para determinar la mejor ruta a todas las redes conocidas. *(Fuente: SANS:)*

1142. Verificación:

Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados. *(Fuente: ISO 27.000:)*

Confirmación, mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados. *(Fuente: ISO 22.300:)*

1143. Verificación de Redundancia Cíclica (CRC):

A veces llamado "código de redundancia cíclica". Un tipo de algoritmo de suma de verificación que no es un hash criptográfico pero se usa para implementar servicio de integridad de datos donde se esperan cambios accidentales en los datos. *(Fuente: SANS:)*

1144. Violación de Datos:

Una violación de datos es un incidente de seguridad en el que información sensible, protegida o confidencial es accedida, robada o divulgada sin autorización. *(Fuente: SANS:)*

1145. Violación de datos:

El movimiento o divulgación no autorizada de información sensible a una parte, generalmente externa a la organización, que no está autorizada para tener o ver la información. *(Fuente: NICSS:)*

1146. Virtualización:

Crear representaciones virtuales de servidores, almacenamiento, redes y otras máquinas físicas. *(Fuente: NICSS:)*

1147. Virus:

Un programa informático que puede replicarse, infectar una computadora sin el permiso o conocimiento del usuario, y luego propagarse a otra computadora. *(Fuente: NICSS:)*

Una sección oculta y autorreplicante de software, usualmente lógica maliciosa, que se propaga infectando — es decir, insertando una copia de sí misma y convirtiéndose en parte

de — otro programa. Un virus no puede ejecutarse solo; requiere que el programa huésped se ejecute para activarse. *(Fuente: SANS:)*

1148. Virus macro:

Un tipo de código malicioso que se adhiere a documentos y usa las capacidades de programación macro de la aplicación del documento para ejecutarse, replicarse y propagarse. *(Fuente: NICSS:)*

1149. Vishing:

Técnica de hacking que consiste en defraudar a víctimas por teléfono, incitándolas a revelar información sensible. *(Fuente: NICSS:)*

1150. Vishing (phishing por voz o VoIP):

Vishing se refiere a ataques de phishing que involucran el uso de llamadas de voz, usando sistemas telefónicos convencionales o sistemas de Voz sobre Protocolo de Internet (VoIP). *(Fuente: SANS:)*

1151. Visión:

<organización> Aspiración de aquello que una organización querría llegar a ser, tal como lo expresa la alta dirección. *(Fuente: ISO 9.000:)*

1152. Vulnerabilidad:

Característica del lugar o postura de seguridad, o del diseño, procedimientos de seguridad, controles internos o la implementación de cualquiera de estos que permiten que ocurra una amenaza o peligro. Vulnerabilidad (expresando grado de vulnerabilidad): expresión cualitativa o cuantitativa del nivel de susceptibilidad al daño cuando una amenaza o peligro se materializa. *(Fuente: NICSS:)*

Debilidad de un activo o de un control que puede ser explotada por una o más amenazas. *(Fuente: ISO 27.000:)*

1153. Vulnerabilidad; Análisis De Vulnerabilidad; Evaluación De La Vulnerabilidad:

Proceso de identificación y cuantificación de un elemento que crea susceptibilidad a una fuente de riesgo que puede provocar una consecuencia. *(Fuente: ISO 22.300:)*

1154. Vía Libre:

Mensaje o señal que indica que el peligro ha cesado. *(Fuente: ISO 22.300:)*

— W —

1155. WHOIS:

Un protocolo para encontrar información sobre recursos en redes. *(Fuente: SANS:)*

1156. War Chalking:

War chalking es marcar áreas, usualmente en aceras con tiza, que reciben señales inalámbricas que pueden ser accedidas. *(Fuente: SANS:)*

1157. War Driving:

War driving es el proceso de viajar buscando señales de puntos de acceso inalámbricos que pueden usarse para obtener acceso a la red. *(Fuente: SANS:)*

1158. Wardriving:

Ataques donde los atacantes buscan redes inalámbricas vulnerables mientras se desplazan en un vehículo por un área. *(Fuente: NICSS:)*

1159. Windump:

Windump es una herramienta gratuita para Windows que es un analizador de protocolos que puede monitorear el tráfico de red en un cable. *(Fuente: SANS:)*

1160. Wired Equivalent Privacy (WEP):

Un protocolo de seguridad para redes locales inalámbricas definido en el estándar IEEE 802.11b. *(Fuente: SANS:)*

1161. World Wide Web ("la Web", WWW, W3):

La colección global, basada en hipermedios, de información y servicios que está disponible en servidores de Internet y se accede mediante navegadores usando el Protocolo de Transferencia de Hipertexto y otros mecanismos de recuperación de información. *(Fuente: SANS:)*

— X —

1162. XaaS:

Categoría general de servicios relacionados con computación en la nube y acceso remoto. *(Fuente: NICSS:)*

— Z —

1163. Zombies:

Un computador zombie (a menudo abreviado como zombie) es una computadora conectada a Internet que ha sido comprometida por un hacker, un virus o un troyano. Generalmente, una máquina comprometida es solo una entre muchas en una botnet y se usa para realizar tareas maliciosas bajo control remoto. La mayoría de los dueños de estas máquinas no saben que su sistema se usa así, por lo que se les compara metafóricamente con zombies. *(Fuente: SANS:)*

1164. Zona Afectada:

Lugar afectado por un desastre. *(Fuente: ISO 22.300:)*

1165. Zona De Riesgo:

Lugar afectado por un desastre. *(Fuente: ISO 22.300:)*

1166. Zona desmilitarizada (DMZ):

En seguridad informática, en general una zona desmilitarizada (DMZ) o red perimetral es un área de red (una subred) que se encuentra entre la red interna de una organización y una red externa, generalmente Internet. Las DMZ ayudan a implementar el modelo de seguridad por capas ya que proporcionan segmentación de subredes basada en requisitos o políticas de seguridad. Las DMZ proporcionan un mecanismo de tránsito desde una fuente segura hacia un destino inseguro o desde una fuente insegura hacia un destino más seguro. En algunos casos, una subred filtrada utilizada para servidores accesibles desde el exterior se denomina DMZ. *(Fuente: SANS:)*