Activo

Compoñente ou funcionalidade dun sistema de información susceptible de ser atacado deliberada ou accidentalmente con consecuencias para a organización. Inclúe: información, datos, servizos, aplicacións (software), equipos (hardware), comunicacións, recursos administrativos, recursos físicos e recursos humanos. *(Esquema Nacional de Seguridade, en diante ENS)*

É calquera información ou sistema relacionado co tratamento da mesma que teña valor para a organización, poden ser procesos de negocio, datos, aplicacións, equipos informáticos, persoal, soportes de información, redes, equipamento auxiliar ou instalacións. É susceptible de ser atacado deliberada ou accidentalmente con consecuencias para a organización. *(Instituto Nacional de Ciberseguridade, en diante INCIBE)*

Ameaza

Eventos que poden desencadear un incidente na Organización, producindo danos materiais ou perdas inmateriais nos seus activos. *(CCN)*

Ameaza persistente avanzada (APT polas súas siglas en inglés)

Un ataque selectivo de ciberespionaxe ou cibersabotaxe, levado a cabo baixo o auspicio ou a dirección dun país, por razóns que van máis aló das meramente financeiras/delituosas ou de protesta política. Non todos os ataques deste tipo son moi avanzados e sofisticados, do mesmo xeito que non todos os ataques selectivos complexos e ben estruturados son unha ameaza persistente avanzada. A motivación do adversario, e non tanto o nivel de sofisticación ou o impacto, é o principal diferenciador dun ataque APT doutro levado a cabo por ciberdelincuentes ou hacktivistas. *(CCN)*

Análise de riscos

Utilización sistemática da información dispoñible para identificar perigos e estimar os riscos. *(ENS)*

Aprendizaxe automática

É unha aplicación da intelixencia artificial (I.A.) na que as máquinas poden “aprender dos resultados”.

Auditoría da seguridade

Revisión e exame independentes dos rexistros e actividades do sistema para verificar a idoneidade dos controis do sistema, asegurar que se cumpren a política de seguridade e os procedementos operativos establecidos, detectar as infraccións da seguridade e recomendar modificacións apropiadas dos controis, da política e dos procedementos. *(ENS)*

Autenticación

Procedemento para comprobar que alguén é quen di ser cando accede a un ordenador ou a un servizo online. Este proceso constitúe unha funcionalidade característica para unha comunicación segura. *(INCIBE)*

Autenticidade

Propiedade ou característica consistente en que unha entidade é quen di ser ou ben que garante a fonte da que proceden os datos. *(ENS)*

Bastionado

É o proceso de asegurar un sistema mediante a redución de vulnerabilidades no mesmo.

Big Data

Big Data é un gran volume, unha alta velocidade e unha gran variedade de activos de información que demandan rendibilidade e innovación no procesamento da información para aumentar a comprensión e a toma de decisións.

Categoría dun sistema

É un nivel, dentro da escala Básica-Media-Alta, co que se adxectiva un sistema a fin de seleccionar as medidas de seguridade necesarias para o mesmo. A categoría do sistema recolle a visión holística do conxunto de activos como un todo harmónico, orientado á prestación duns servizos. *(ENS)*

Ciber-resiliencia

Ciber-resiliencia refírese xeralmente ás capacidades organizativas e técnicas para absorber impactos externos e internos, e recuperar a normalidade nas operacións dunha forma controlada.

Ciberseguridade

Ver seguridade das redes e da información.

Confidencialidade

Propiedade ou característica consistente en que a información nin se pon a disposición, nin se revela a individuos, entidades ou procesos non autorizados. *(ENS)*

É a propiedade da información, pola que se garante que está accesible unicamente a persoal autorizado a acceder a dita información. *(INCIBE)*

A confidencialidade da información constitúe a pedra angular da seguridade da información. Xunto coa integridade e a dispoñibilidade supoñen as tres dimensións da seguridade da información. *(INCIBE)*

Cortafogos

Sistema de seguridade composto ou ben de programas (software) ou de dispositivos hardware situados nos puntos limítrofes dunha rede que teñen o obxectivo de permitir e limitar, o fluxo de tráfico entre os diferentes ámbitos que protexe sobre a base dun conxunto de normas e outros criterios. *(INCIBE)*

A funcionalidade básica dun cortafogo é asegurar que todas as comunicacións entre a rede e Internet realícense conforme ás políticas de seguridade da organización ou corporación. *(INCIBE)*

Datos

Representación da información usando algún formato que permita a súa comunicación, interpretación, almacenamento e procesado automático.

Datos estruturados

Son datos arquivados en táboas ou en base de datos relacionais.

Datos non estruturados

Son datos de moi diversos formatos.

Por exemplo: fotos, vídeos, datos de WhatsApp , Facebook, Twiter, datos de diversos sensores, do IoT; datos biométricos, pegadas dixitais, escáner de retina; emails, rexistros de voz, historias clínicas, etc.

Os datos non estruturados, xeralmente son datos binarios que non teñen estrutura interna identificable. É un conglomerado masivo e desorganizado de varios obxectos que non teñen valor ata que se identifican e almacenan de maneira organizada. *(http://smarterworkspaces.kyocera.es/blog/diferencia-datos-estruturados-non-estruturados/)*

Dispoñibilidade

Propiedade ou característica dos activos consistente en que as entidades ou procesos autorizados teñen acceso aos mesmos cando o requiren. *(ENS)*

Efecto perturbador significativo (Art 6 DCbs)

Á hora de determinar a importancia dun efecto perturbador teranse en conta polo menos os seguintes factores intersectoriais:

a) o número de usuarios que confían nos servizos prestados pola entidade de que se trate;

b) a dependencia doutros sectores que figuran no anexo II sobre o servizo prestado por esa entidade;

c) a repercusión que poderían ter os incidentes, en termos de grao e duración, nas actividades económicas e sociais ou na seguridade pública;

d) a cota de mercado da entidade; e) a extensión xeográfica con respecto á zona que podería verse afectada por un incidente;

e) a importancia da entidade para manter un nivel suficiente do servizo, tendo en conta a dispoñibilidade de alternativas para a prestación dese servizo.

f) tamén se terán en conta factores específicos do sector, cando proceda.

Xestión de riscos

Actividades coordinadas para dirixir e controlar unha organización con respecto aos riscos. *(ENS)*

Achado de auditoría

Resultados da avaliación da evidencia de auditoría fronte aos criterios de auditoría. Os achados de auditoría poden indicar conformidade ou non conformidade. Poden conducir á identificación de oportunidades de mellora ou ao rexistro de boas prácticas. Se os requisitos de auditoría selecciónanse de entre os requisitos legais ou outros requisitos, o achado de auditoría denomínase "cumprimento" ou "non cumprimento". *(UNE-EN-ISO 19011:2012) (CCN-STIC-802)*

Incidente de seguridade

Todo feito que teña efectos adversos reais na seguridade das redes e sistemas de información. *(Art 4 DCbs)*

A fin de determinar a importancia dos efectos dun incidente, teranse en conta, en particular, os seguintes parámetros: *(Art 14.4 DCbs)*

a) o número de usuarios afectados pola perturbación do servizo esencial;

b) a duración do incidente;

c) a extensión xeográfica con respecto á zona afectada polo incidente.

Calquera suceso que afecte á confidencialidade, integridade ou dispoñibilidade dos activos de información da empresa, por exemplo: acceso ou intento de acceso aos sistemas, uso, divulgación, modificación ou destrución non autorizada de información. *(INCIBE)*

Integridade (en relación cos controis de procesos/aplicación)

Completitude. *(Nas NIAs e outros documentos técnicos en inglés o termo utilizado é "completeness", que se traduciu como integridade, o que pode inducir a confusión co seu significado cando se fala de seguridade da información).*

Rexistráronse todos os feitos e transaccións que tiñan que rexistrarse. (GPF-OCEX 1317).

Integridade (en relación coa seguridade da información)

Propiedade ou característica consistente en que o activo de información non foi alterado de maneira non autorizada. *(ENS)*

É a propiedade da información, pola que se garante a exactitude dos datos transportados ou almacenados, asegurando que non se produciu a súa alteración, perda ou destrución, xa sexa de forma accidental ou intencionada, por erros de software ou hardware ou por condicións ambientais. *(INCIBE)*

Intelixencia artificial

É o concepto de máquinas que poden realizar tarefas de maneira tal que podiamos considerar "intelixentes".

Internet das cousas (Internet of Things)

Este termo atópase en plena evolución. En esencia, actualmente refírese a redes de obxectos físicos (edificios, marcapasos, biosensores, software, etc.), en definitiva sensores que dispoñen de conectividade en rede que lles permiten colleitar información de todo tipo (CCN).

Medidas de seguridade

Conxunto de disposicións encamiñadas a protexerse dos riscos posibles sobre o sistema de información, co fin de asegurar os seus obxectivos de seguridade. Pode tratarse de medidas de prevención, de disuasión, de protección, de detección e reacción, ou de recuperación. *(ENS)*

Metadatos

Os metadatos son o conxunto de datos relacionados cun documento e que recollen información fundamentalmente descritiva do mesmo, así como información de administración e xestión. Os metadatos é unha información que enriquece o documento ao que está asociado. *(INCIBE)*

Non repudio

O non repudio no envío de información a través das redes é capacidade de demostrar a identidade do emisor desa información. O obxectivo que se pretende é certificar que os datos, ou a información, proveñen realmente da fonte que di ser. *(INCIBE)*

O problema do control de autenticidade dentro dos sistemas de información a través da Rede, en relación tanto da identidade do suxeito como do contido dos datos, pode ser resolto mediante a utilización da firma electrónica (ou dixital). *(INCIBE)*

É sinónimo de autenticidade. *(INCIBE)*

Plan de continxencia

Un Plan de Continxencia das Tecnoloxías da Información e as Comunicacións (TIC) consiste nunha estratexia planificada en fases, constituída por un conxunto de recursos de respaldo, unha organización de emerxencia e uns procedementos de actuación, encamiñados a conseguir unha restauración ordenada, progresiva e áxil dos sistemas de información que soportan a información e os procesos de negocio considerados críticos no Plan de Continuidade de Negocio da compañía. *(INCIBE)*

Plan de continuidade

Un Plan de Continuidade de Negocio é un conxunto formado por plans de actuación, plans de emerxencia, plans financeiros, plans de comunicación e plans de continxencias destinados a mitigar o impacto provocado pola concreción de determinados riscos sobre a información e os procesos de negocio dunha compañía. *(INCIBE)*

Política de seguridade

Son as decisións ou medidas de seguridade que unha empresa decidiu tomar respecto da seguridade dos seus sistemas de información despois de avaliar o valor dos seus activos e as regas aos que están expostos. *(INCIBE)*

Este termo tamén se refire ao documento de nivel executivo mediante o cal unha empresa establece as súas directrices de seguridade da información. *(INCIBE)*

Conxunto de directrices plasmadas en documento escrito, que rexen a forma en que unha organización xestiona e protexe a información e os servizos que considera críticos. *(ENS)*

Principios básicos de seguridade

Fundamentos que deben rexer toda acción orientada a asegurar a información e os servizos. *(ENS)*

Proceso

Conxunto organizado de actividades que levan a cabo para producir a un produto ou servizo; ten un principio e fin delimitado, implica recursos e dá lugar a un resultado. *(ENS)*

Redes e sistemas de información (Art 4 DCbs)

a) unha rede de comunicacións electrónicas;

b) todo dispositivo ou grupo de dispositivos interconectados ou relacionados entre si no que un ou varios deles realizan, mediante un programa, o tratamento automático de datos dixitais, ou

c) os datos dixitais almacenados, tratados, recuperados ou transmitidos mediante elementos contemplados nas letras a) e b) para o seu funcionamento, utilización, protección e mantemento;

Requisitos mínimos de seguridade

Esixencias necesarias para asegurar a información e os servizos. *(ENS)*

Risco

Toda circunstancia ou feito razoablemente identificable que teña un posible efecto adverso na seguridade das redes e sistemas de información. *(Art 4 DCbs)*

Estimación do grao de exposición a que unha ameaza se materialice sobre un ou máis activos causando danos ou prexuízos á organización. *(ENS)*

Router

É un dispositivo que distribúe tráfico de rede entre dúas ou máis diferentes redes. Un router está conectado polo menos a dúas redes, xeralmente LAN ou WAN e o tráfico que recibe procedente dunha rede rediríxeo cara a(s) outra(s) rede(es). *(INCIBE)*

En termos domésticos un router é o dispositivo que proporciona o provedor de servizos de telefonía (ou ISP) e que permite conectar a nosa LAN doméstica coa rede do IS. *(INCIBE)*

O router comproba as direccións de destino dos paquetes de información e decide por que ruta serán enviados, para determinar o mellor camiño empregan cabeceiras e táboas de comparación. *(INCIBE)*

Seguridade da información

Garante que dentro da entidade, a información está protexida fronte a divulgación non autorizada (confidencialidade), modificación indebida (integridade), e que está accesible cando se solicita (dispoñibilidade). (ISACA)

Seguridade das redes e da información

É a capacidade das redes ou dos sistemas de información de resistir, cun determinado nivel de confianza, os accidentes ou accións ilícitas ou malintencionadas que comprometan a dispoñibilidade, autenticidade, integridade e confidencialidade dos datos almacenados ou transmitidos e dos servizos que ditas redes e sistemas ofrecen ou fan accesibles. *(ENS)*

A capacidade das redes e sistemas de información de resistir, cun nivel determinado de fiabilidade, toda acción que comprometa a dispoñibilidade, autenticidade, integridade ou confidencialidade dos datos almacenados, transmitidos ou tratados, ou os servizos correspondentes ofrecidos por tales redes e sistemas de información ou accesibles a través deles. *(Art 4 DCbs)*

A ciberseguridade trata da protección dos activos de información fronte ás ameazas á información procesada, almacenada e transportada por sistemas de información interconectados. (ISACA)

Sistema de xestión da seguridade da información (SGSI)

Sistema de xestión que, baseado no estudo dos riscos, establécese para crear, implementar, facer funcionar, supervisar, revisar, manter e mellorar a seguridade da información. O sistema de xestión inclúe a estrutura organizativa, as políticas, as actividades de planificación, as responsabilidades, as prácticas, os procedementos, os procesos e os recursos. *(ENS)*

Sistema de información

Conxunto organizado de recursos para que a información póidase recoller, almacenar, procesar ou tratar, manter, usar, compartir, distribuír, pór a disposición, presentar ou transmitir. *(ENS)*

Os elementos dun sistema de información son: hardware, software, soportes de información, comunicacións, instalacións, persoal e servizos aprovisionados por terceiros.

Conxunto de aplicacións, servizos, activos relacionados con tecnoloxías da información e outros compoñentes para manexar información. *(UNE-ISO/IEC 27000:2014; CCN-STIC-830)*

Tecnoloxías cognitivas

As tecnoloxías cognitivas utilizan os principios de intelixencia artificial e da aprendizaxe automática pero necesitan algúns elementos de criterio humano de interpretación para actuar a partir da información e alcanzar un resultado.

As persoas participan nas actividades da I.A./A.A. para alcanzar a decisión final. Isto leva a algúns a denominar os sistemas de tecnoloxías cognitiva como "intelixencia aumentada" (máquina + persoa) en lugar de simplemente I.A.

Trazabilidade

Propiedade ou característica consistente en que as actuacións dunha entidade poden ser imputadas exclusivamente a dita entidade. *(ENS)*

Vulnerabilidade

Unha debilidade que pode ser aproveitada por unha ameaza. *(ENS)*

Fallos ou deficiencias dun programa que poden permitir que un usuario non lexítimo acceda á información ou leve a cabo operacións non permitidas de maneira remota. *(INCIBE)*

Os buracos de seguridade poden ser aproveitadas por atacantes mediante exploits, para acceder aos sistemas con fins maliciosos. As empresas deben ser conscientes destes riscos e manter unha actitude preventiva, así como levar un control dos seus sistemas mediante actualizacións periódicas. *(INCIBE)*