Glosario de Ciberseguridad[1]

El presente glosario tiene la finalidad de aunar criterios y definiciones entre los expertos de ciberseguridad de distintas jurisdicciones y para maximizar el trabajo interdisciplinario que requiere la protección del sistema financiero en su conjunto.

Notas

- Las citas de las fuentes que figuran a continuación han sido abreviadas. Puede encontrarse la cita completa al final del glosario.
- Los términos definidos en el glosario figuran en itálica cuando están usados en definiciones del glosario.
- En el glosario, el término "entidad" incluye a las personas humanas cuando el contexto lo requiere.

Término	**Definición**
Activo (*asset*)	Recurso de valor tangible o intangible que debería ser protegido, lo que comprende personas, información, infraestructura, finanzas y reputación. Fuente: ISACA Fundamentals.
Agente de amenaza (*threat actor*)	Persona, grupo u organización que supuestamente está operando con intención maliciosa. Fuente: Adaptado de STIX.

[1] Los términos y las definiciones utilizados en el glosario se desarrollaron para ser utilizados únicamente con respecto al sector de servicios financieros y las entidades financieras. El glosario no tiene por objeto ser utilizado para una interpretación jurídica de ningún acuerdo internacional ni de contratos entre privados.
Texto original: https://www.fsb.org/2018/11/cyber-lexicon/

Amenaza persistente avanzada (*Advanced Persistent Threat, APT*)	*Agente de amenaza* que cuenta con niveles sofisticados de conocimiento y recursos significativos que le permiten generar oportunidades para lograr sus objetivos usando numerosos *vectores de amenaza*. La *amenaza persistente avanzada*: (i) persigue sus objetivos de manera reiterada durante un período prolongado; (ii) se adapta a los esfuerzos que realizan quienes se defienden de ella en un intento por resistirla; y (iii) está decidida a llevar a cabo sus objetivos. Fuente: Adaptado de NIST.
Análisis de vulnerabilidades (*vulnerability assessment*)	Examen sistemático de un *sistema de información*, junto con sus controles y procesos, para determinar la adecuación de las medidas de seguridad, identificar deficiencias en la seguridad, proporcionar datos a partir de los cuales predecir la eficacia de las medidas de seguridad propuestas y confirmar la adecuación de dichas medidas luego de la implementación. Fuente: Adaptado de NIST.
Autenticación multifactor (*multi-factor authentication*)	Uso de dos o más de los siguientes factores para verificar la identidad de un usuario: • factor de conocimiento, "algo que una persona sabe"; • factor de posesión, "algo que una persona tiene"; • factor biométrico, "una característica biológica o conductual de una persona". Fuente: Adaptado de ISO/IEC 27040:2015 e ISO/IEC 2832-37:2017 (definición de "característica biométrica" ["*biometric characteristic*"]).
Autenticidad (*authenticity*)	Propiedad que consiste en que una entidad es lo que afirma ser. Fuente: ISO/IEC 27000:2018.

Aviso cibernético (*cyber advisory*)	Notificación de nuevas tendencias o de novedades acerca de una *ciberamenaza* contra *sistemas de información* o acerca de una *vulnerabilidad* de los *sistemas de información*. Dicha notificación puede abarcar un estudio analítico de tendencias, intenciones, tecnologías o tácticas empleadas para atacar *sistemas de información*. Fuente: Adaptado de NIST.
Campaña (*campaign*)	Conjunto de comportamientos adversos coordinados que describe una serie de actividades maliciosas contra uno o más objetivos específicos a lo largo de un período. Fuente: Adaptado de STIX.
Ciber- o cibernético (*cyber*)	Relativo a una infraestructura tecnológica interconectada en la que interactúan personas, procesos, datos y *sistemas de información*. Fuente: Adaptado de CPMI-IOSCO (cita de NICCS).
Ciberalerta (*cyber alert*)	Notificación de un *ciberincidente* específico o de que se ha dirigido una *ciberamenaza* contra los *sistemas de información* de una organización. Fuente: Adaptado de NIST.
Ciberamenaza (*cyber threat*)	Circunstancia que podría explotar una o más *vulnerabilidades* y afectar la *ciberseguridad*. Fuente: Adaptado de CPMI-IOSCO.

Ciberincidente (*cyber incident*)	*Evento cibernético* que: i. pone en peligro la *ciberseguridad* de un *sistema de información* o la información que el sistema procesa, almacena o transmite; o ii. infringe las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable, sea o no producto de una actividad maliciosa. Fuente: Adaptado de NIST (definición de "incidente" ["*incident*"]).
Ciberresiliencia (*cyber resilience*)	Capacidad de una organización de continuar llevando a cabo su misión anticipando y adaptándose a *ciberamenazas* y otros cambios relevantes en el entorno, y resistiendo, conteniendo y recuperándose rápidamente de *ciberincidentes*. Fuente: Adaptado de CERT Glossary (definición de "resiliencia operativa" ["*operational resilience*"]), CPMI-IOSCO y NIST (definición de "resiliencia" ["*resilience*"]).
Ciberseguridad (*cyber security*)	Preservación de la *confidencialidad*, la *integridad* y la *disponibilidad* de la información y/o de los *sistemas de información* a través del medio *cibernético*. Asimismo, pueden estar involucradas otras propiedades, tales como la *autenticidad*, la *trazabilidad*, el *no repudio* y la *confiabilidad*. Fuente: Adaptado de ISO/IEC 27032:2012.
Compromiso (*compromise*)	Transgresión de la seguridad de un *sistema de información*. Fuente: Adaptado de ISO 21188:2018.
Confiabilidad (*reliability*)	Uniformidad en cuanto al comportamiento y los resultados deseados. Fuente: ISO/IEC 27000:2018.

Confidencialidad (*confidentiality*)	Propiedad según la cual la información no está disponible para personas, entidades, procesos o sistemas no autorizados, ni se da a conocer a personas, entidades, procesos o sistemas no autorizados. Fuente: Adaptado de ISO/IEC 27000:2018.
Control de acceso (*access control*)	Medio para asegurar que el acceso a los *activos* esté autorizado y restringido en función de requisitos relacionados con la actividad y la seguridad. Fuente: ISO/IEC 27000:2018.
Curso de acción (*Course of Action, CoA*)	Una o más acciones que se llevan a cabo para prevenir o responder a un *ciberincidente*. Este concepto puede referirse a respuestas técnicas automatizables, pero también puede describir otras acciones, tales como la capacitación para los empleados o los cambios en las políticas. Fuente: Adaptado de STIX.
Defensa en profundidad (*defence-in-depth*)	Estrategia de seguridad que abarca personas, procesos y tecnología para establecer una serie de barreras en múltiples niveles y dimensiones de la organización. Fuente: Adaptado de NIST y FFIEC.
Denegación de servicio (*Denial of Service, DoS*)	Acción de impedir el acceso autorizado a información o *sistemas de información*, o de demorar la ejecución de operaciones y funciones de los *sistemas de información*, lo cual conlleva la pérdida de *disponibilidad* para los usuarios autorizados. Fuente: Adaptado de ISO/IEC 27033-1:2015.
Denegación de servicio distribuida (*Distributed Denial of Service, DDoS*)	*Denegación de servicio* que se lleva a cabo usando numerosas fuentes en forma simultánea. Fuente: Adaptado de NICCS.

Detectar (función) (*detect*)	Desarrollar e implementar las actividades apropiadas para identificar un *evento cibernético*. Fuente: Adaptado de NIST Framework.
Disponibilidad (*availability*)	Cualidad de accesible y utilizable a demanda por parte de una entidad autorizada. Fuente: ISO/IEC 27000:2018.
Equipo de respuesta ante incidentes (*Incident Response Team, IRT*) [también conocido como *CERT* o *CSIRT*]	Equipo conformado por miembros capacitados y confiables de la organización que maneja los incidentes durante su ciclo de vida. Fuente: ISO/IEC 27035-1:2016.
Evaluación de amenazas (*threat assessment*)	Proceso de evaluación formal del grado de amenaza para una organización y descripción de la naturaleza de la amenaza. Fuente: Adaptado de NIST.
Evento cibernético (*cyber event*)	Ocurrencia observable en un *sistema de información*. Los *eventos cibernéticos* a veces indican que se está produciendo un *ciberincidente*. Fuente: Adaptado de NIST (definición de "evento" ["*event*"]).
Exploit	Forma definida de transgredir la seguridad de los *sistemas de información* a través de una *vulnerabilidad*. Fuente: ISO/IEC 27039:2015.

Gestión de identidades y accesos (*Identity and Access Management, IAM*)	Comprende personas, procesos y tecnología para identificar y gestionar los datos utilizados en un *sistema de información* a fin de autenticar a los usuarios y otorgar o denegar derechos de acceso a datos y recursos del sistema. Fuente: Adaptado de ISACA Full Glossary.
Gestión de parches (*patch management*)	Notificación, identificación, implementación, instalación y *verificación* sistemáticas de revisiones de los sistemas operativos y los códigos de software de aplicación. Estas revisiones se conocen con el nombre de "parche" ("*patch*"), "corrección rápida" ("*hot fix*") y "conjunto de parches" ("*service pack*"). Fuente: NIST.
Identificar (función) (*identify*)	Desarrollar el entendimiento organizacional necesario para gestionar el *riesgo cibernético* al que se encuentran expuestos los *activos* y las capacidades. Fuente: Adaptado de NIST Framework.
Incidente de seguridad de los datos (*data breach*)	*Compromiso* que, de manera accidental o ilegal, da lugar a la destrucción, la pérdida, la alteración o la divulgación o el acceso no autorizados a datos transmitidos, almacenados o procesados de otra manera. Fuente: Adaptado de ISO/IEC 27040:2015.
Indicadores de compromiso (*Indicators of Compromise, IoC*)	Señales que indican que podría haber ocurrido o que podría estar produciéndose un *ciberincidente*. Fuente: Adaptado de NIST (definición de "indicador" ["*indicator*"]).

Ingeniería social (*social engineering*)	Término general que describe la acción de intentar engañar a las personas con el fin de que revelen información o realicen determinadas acciones. Fuente: Adaptado de FFIEC.
Integridad (*integrity*)	Cualidad de exacto y completo. Fuente: ISO/IEC 27000:2018.
Inteligencia sobre amenazas (*threat intelligence*)	Información sobre amenazas que ha sido agregada, transformada, analizada, interpretada o enriquecida para ofrecer el contexto necesario para los procesos de toma de decisiones. Fuente: NIST 800-150.
Intercambio de información (*information sharing*)	Acción de compartir datos, información y/o conocimiento que pueden utilizarse para gestionar riesgos o responder ante eventos. Fuente: Adaptado de NICCS.
Malware	Software diseñado con un objetivo malicioso y que contiene características o capacidades que podrían provocar un daño directo o indirecto a entidades o a sus *sistemas de información*. Fuente: Adaptado de ISO/IEC 27032:2012.
No repudio (*non-repudiation*)	Capacidad de demostrar la ocurrencia de un evento o acción y las entidades que los originaron. Fuente: ISO 27000:2018.

Plan de respuesta ante ciberincidentes (*cyber incident response plan*)	Documentación de un conjunto predeterminado de instrucciones o procedimientos para responder ante un *ciberincidente* y limitar sus consecuencias. Fuente: Adaptado de NIST (definición de "plan de respuesta ante incidentes" ["*incident response plan*"]) y NICCS.
Proteger (función) (*protect*)	Desarrollar e implementar los resguardos adecuados para garantizar la prestación de los servicios y limitar o contener el impacto de los *ciberincidentes*. Fuente: Adaptado de NIST Framework.
Protocolo de divulgación (*Traffic Light Protocol, TLP*)	Conjunto de designaciones utilizadas para asegurar que la información se comparta únicamente con los destinatarios definidos. Emplea un código de colores preestablecido (semáforo) para indicar los límites previstos de intercambio que deberá aplicar el receptor. Fuente: Adaptado de FIRST.
Recuperar (función) (*recover*)	Desarrollar e implementar las actividades adecuadas para mantener planes de *ciberresiliencia* y restaurar capacidades o servicios que se hayan visto afectados debido a un *ciberincidente*. Fuente: Adaptado de NIST Framework.
Responder (función) (*respond*)	Desarrollar e implementar las actividades apropiadas para tomar medidas acerca de un *evento cibernético* detectado. Fuente: Adaptado de NIST Framework.
Riesgo cibernético (*cyber risk*)	Combinación de la probabilidad de que se produzcan *ciberincidentes* y su impacto. Fuente: Adaptado de CPMI-IOSCO, ISACA Fundamentals (definición de "riesgo" ["*risk*"]) e ISACA Full Glossary (definición de "riesgo" ["*risk*"]).

Sistema de información (*information system*)	Conjunto de aplicaciones, servicios, *activos* de tecnología de la información u otros componentes de manejo de información, que incluye el entorno operativo. Fuente: Adaptado de ISO/IEC 27000:2018.
Tácticas, técnicas y procedimientos (*Tactics, Techniques and Procedures, TTP*)	Comportamiento de un *agente de amenaza*. Una táctica es la descripción de más alto nivel de este comportamiento, mientras que las técnicas brindan una descripción más detallada del comportamiento en el contexto de una táctica y los procedimientos implican una descripción de menor nivel, muy detallada en el contexto de una técnica. Fuente: Adaptado de NIST 800-150.
Test de intrusión (*penetration testing*)	Metodología de prueba en la cual los evaluadores, usando toda la documentación disponible (p. ej., diseño del sistema, código fuente, manuales) y trabajando con limitaciones específicas, intentan eludir las funciones de seguridad de un *sistema de información*. Fuente: NIST.
Test de intrusión basado en amenazas (*Threat-Led Penetration Testing, TLPT*) [también conocido como prueba del equipo rojo (*red team testing*)]	Intento controlado por comprometer la *ciberresiliencia* de una entidad simulando las *tácticas, técnicas y procedimientos* de *agentes de amenaza* reales. Se basa en *inteligencia sobre amenazas* dirigida y se centra en las personas, los procesos y la tecnología de una entidad, con un conocimiento previo e impacto mínimos en las operaciones. Fuente: G-7 Fundamental Elements.
Trazabilidad (*accountability*)	Propiedad que asegura que las acciones de una entidad puedan ser rastreadas y atribuidas de manera inequívoca a dicha entidad. Fuente: ISO/IEC 2382:2015.

Vector de amenaza (*threat vector*)	Recorrido o ruta utilizados por el *agente de amenaza* para obtener acceso al objetivo. Fuente: Adaptado de ISACA Fundamentals.
Verificación (*verification*)	Confirmación, a través de la provisión de evidencia objetiva, de que se han cumplido los requisitos especificados. Fuente: ISO/IEC 27042:2015.
Vulnerabilidad (*vulnerability*)	Debilidad, susceptibilidad o defecto de un *activo* o control que pueden ser explotados por una o más amenazas. Fuente: Adaptado de CPMI-IOSCO e ISO/IEC 27000:2018.

Fuentes

Glosario de CERT	Carnegie Mellon Software Engineering Institute, CERT® Resilience Management Model, Version 1.2, Glossary of Terms (Instituto de Ingeniería de Software de la Universidad Carnegie Mellon, Modelo CERT® para la gestión de la resiliencia, versión 1.2, Glosario) https://resources.sei.cmu.edu/asset_files/BookChapter/2016_009_001_514934.pdf
CPMI-IOSCO	CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (June 2016) (CPMI-IOSCO, Guía sobre ciberresiliencia para infraestructuras de mercados financieros [junio de 2016]) https://www.bis.org/cpmi/publ/d146.pdf
FFIEC	FFIEC (Federal Financial Institutions Examination Council) IT Examination Handbook Infobase, Glossary (Consejo Federal de Inspección de Instituciones Financieras, Infobase - Manual de examen informático, Glosario) https://ithandbook.ffiec.gov/glossary.aspx
FIRST	FIRST Traffic Light Protocol (TLP), Version 1.0 (Protocolo de divulgación)FIRST [TLP], versión 1.0) https://www.first.org/tlp/docs/tlp-v1.pdf
G-7 Fundamental Elements	G-7 Fundamental Elements for Threat-Led Penetration Testing (G7: Elementos fundamentales para el test de intrusión basado en amenazas) https://www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf
ISACA Fundamentals	ISACA Cybersecurity Fundamentals Glossary (2016) (Glosario de conceptos fundamentales sobre ciberseguridad de ISACA [2016]) http://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

ISACA Full Glossary	ISACA Glossary (Glosario de ISACA) https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf
ISO/IEC 2832:2015	ISO/IEC 2832:2015 https://www.iso.org/standard/63598.html
ISO/IEC 2832-37:2017	ISO/IEC 2832-37:2017 https://www.iso.org/standard/66693.html
ISO 21188:2018	ISO 21188:2018 https://www.iso.org/standard/63134.html
ISO/IEC 27000:2018	ISO/IEC 27000:2018 https://www.iso.org/standard/73906.html
ISO/IEC 27032:2012	ISO/IEC 27032:2012 https://www.iso.org/standard/44375.html
ISO/IEC 27033-1:2015	ISO/IEC 27033-1:2015 https://www.iso.org/standard/63461.html
ISO/IEC 27035-1:2016	ISO/IEC 27035-1:2016 https://www.iso.org/standard/60803.html
ISO/IEC 27039:2015	ISO/IEC 27039:2015 https://www.iso.org/standard/56889.html
ISO/IEC 27040:2015	ISO/IEC 27040:2015 https://www.iso.org/standard/44404.html
ISO/IEC 27042:2015	ISO/IEC 27042:2015 https://www.iso.org/standard/44406.html
NICCS	NICCS (National Initiative for Cybersecurity Careers and Studies), Explore Terms: A Glossary of Common Cybersecurity Terminology (Iniciativa Nacional para Carreras y Estudios en Ciberseguridad [NICCS], Exploración de términos: glosario de terminología común de ciberseguridad) http://niccs.us-cert.gov/glossary

NIST	NIST, Glossary of Key Information Security Terms, Revision 2 (May 2013) (NIST, Glosario de términos clave de seguridad de la información, revisión 2 [mayo de 2013]) https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
NIST 800-150	NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing (October 2016) (NIST, Publicación especial 800-150, Guía de intercambio de información sobre ciberamenazas [octubre de 2016]) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
NIST Framework	NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (16 April 2018) (NIST, Marco para la mejora de la ciberseguridad en infraestructura crítica, versión 1.1. [16 de abril de 2018]) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
STIX	Structured Threat Information Expression (STIX™) 2 https://oasis-open.github.io/cti-documentation/stix/intro.html