INTERNACIONAL ESTÁNDAR

ISO/CEI 27032

Segunda edicion
2023-06

Ciberseguridad: directrices para la seguridad en Internet

Ciberseguridad — Líneas directrices relativas a la seguridad en Internet

Número de referencia
ISO/IEC 27032:2023(E)

Oficina de derechos de autor ISO
CP 401 • Cap. de Blandonnet 8
CH-1214 Vernier, Ginebra
Teléfono: +41 22 749 01 11 Correo
electrónico: copyright@iso.org
Sitio web:www.iso.org

Publicado en Suiza

Contenido

Página

Prefacio

ISO (la Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por la organización respectiva para abordar campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. También participan en el trabajo otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC.

Los procedimientos utilizados para desarrollar este documento y aquellos destinados a su mantenimiento posterior se describen en las Directivas ISO/IEC, Parte 1. En particular, se deben tener en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documento. Este documento fue redactado de acuerdo con las reglas editoriales de las Directivas ISO/IEC, Parte 2 (verwww.iso.org/directivas o www.iec.ch/members_experts/refdocs).

ISO e IEC llaman la atención sobre la posibilidad de que la implementación de este documento pueda implicar el uso de (una) patente(s). ISO e IEC no adoptan ninguna posición con respecto a la evidencia, validez o aplicabilidad de cualquier derecho de patente reivindicado con respecto a los mismos. A la fecha de publicación de este documento, ISO e IEC no habían recibido notificación de (una) patente(s) que puedan ser necesarias para implementar este documento. Sin embargo, se advierte a los implementadores que esto puede no representar la información más reciente, que puede obtenerse de la base de datos de patentes disponible enwww.iso.org/patents yhttps://patents.iec.ch . ISO e IEC no serán responsables de identificar cualquiera o todos estos derechos de patente.

Cualquier nombre comercial utilizado en este documento es información proporcionada para la comodidad de los usuarios y no constituir un aval.

Para una explicación de la voluntad de ISO sobre términos específicos y expresiones relacionadas con la evaluación de la conformidad, así como información sobre la adhesión de ISO a la Organización Mundial del Comercio (OMC) priInorteSCohIP/IlemisCi2norte70th3mi2:2t0mi2ch3Obstáculos técnicos al comercio (OTC) ver www.iso.org/iso/hparaTTrpagmisw

Este documento fue preparado por Joi0norte5tdtFmi3Cbh0norte2i1C2a6bC/ohesmetro0hmetro2i2ES DECIR0C23JTC 1,*Tecnologías de la información*, Subcomité SC 27,*Seguridad de la información, ciberseguridad y protección de la privacidad*.

Esta segunda edición anula y reemplaza la primera edición (ISO/IEC 27032:2012) que ha sido revisada técnicamente.

Los principales cambios son los siguientes:

— se ha modificado el título;

— se ha modificado la estructura del documento;

— se ha cambiado el enfoque de evaluación y tratamiento de riesgos, con la adición de contenido sobre amenazas, vulnerabilidades y vectores de ataque para identificar y gestionar los riesgos de seguridad en Internet;

— un mapeo entre los controles para la seguridad de Internet citados en9.2 y los controles contenidos en ISO/IEC 27002 se han agregado aAnexo A .

Cualquier comentario o pregunta sobre este documento debe dirigirse al organismo de normalización nacional del usuario. Una lista completa de estos organismos se puede encontrar enwww.iso.org/members.html y www.iec.ch/national-committees .

Introducción

El objetivo de este documento es abordar los problemas de seguridad de Internet y proporcionar orientación para abordar las amenazas comunes a la seguridad de Internet, como:

— ataques de ingeniería social;

— ataques de día cero;

— ataques a la privacidad;

- hackear; y

— la proliferación de software malicioso (malware), spyware y otro software potencialmente no deseado.

La guía contenida en este documento proporciona controles técnicos y no técnicos para abordar los riesgos de seguridad de Internet, incluidos controles para:

— prepararse para los ataques;

— prevenir ataques;

— detección y seguimiento de ataques; y

- respondiendo

La guía se centra en pro(v est) educación de consumidores y empleados para ayudar a las partes interesadas en desempeñando un papel activo para abordar los desafíos de seguridad en Internet. El documento también se centra en la preservación de la confidencialidad, integridad y disponibilidad de la información a través de Internet y otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad que también pueden estar involucradas.

— funciones;

— políticas;

- métodos;

— procesos; y

— controles técnicos aplicables.

Dado el alcance de este documento, los controles previstos son necesariamente de alto nivel. En el documento se hace referencia a las normas y directrices de especificaciones técnicas detalladas aplicables a cada área para obtener más orientación. VerAnexo A para la correspondencia entre los controles citados en este documento y los de la norma ISO/IEC 27002.

Este documento no aborda específicamente los controles que las organizaciones pueden requerir para los sistemas que respaldan la infraestructura crítica o la seguridad nacional. Sin embargo, la mayoría de los controles mencionados en este documento se pueden aplicar a dichos sistemas.

Este documento utiliza conceptos existentes de ISO/IEC 27002, la serie ISO/IEC 27033, ISO/IEC TS 27100 e ISO/IEC 27701, para ilustrar:

— la relación entre seguridad de Internet, seguridad web, seguridad de redes y ciberseguridad;

— orientación detallada sobre los controles de seguridad de Internet citados en9.2 , que aborda la preparación en materia de ciberseguridad para los sistemas conectados a Internet.

Como se menciona en ISO/IEC TS 27100, Internet es una red global, utilizada por las organizaciones para todas las comunicaciones, tanto digitales como de voz. Dado que algunos usuarios dirigen ataques hacia estas redes, es fundamental abordar los riesgos de seguridad relevantes.

Ciberseguridad: directrices para la seguridad en Internet

1 Alcance

Este documento proporciona:

— una explicación de la relación entre la seguridad de Internet, la seguridad web, la seguridad de la red y la ciberseguridad;

— una visión general de la seguridad en Internet;

— identificación de las partes interesadas y descripción de sus funciones en la seguridad de Internet;

— orientación de alto nivel para abordar problemas comunes de seguridad en Internet.

Este documento está destinado a organizaciones que utilizan Internet.

2 Referencias normativas

Los siguientes documentos se mencionan en el texto de tal manera que parte o todo su contenido constituye un requisito. Elementos de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para referencia sin fecha s, the latest edition (including any amendments) applies.

ISO/CEI 27000, *Information technology — Security techniques — Information security management systems: descripción general y vocabulario*

3 plazos y definiciones

Para los fines de este documento en ISO/IEC 27000, y lo siguiente ejem Me postulo.

ISO e IEC mantienen bases de datos terminológicas para su uso en la estandarización en las siguientes direcciones:

— Plataforma de navegación ISO Online: disponible en https://www.iso.org/obp

— Electropedia IEC: disponible en https://www.electropedia.org/

3.1
vector de ataque
Ruta o medio por el cual un atacante puede obtener acceso a una computadora o servidor de red para generar un resultado malicioso.

EJEMPLO 1 Dispositivos de IoT.

EJEMPLO 2 Teléfonos inteligentes.

3.2
agresor
Persona que explota deliberadamente vulnerabilidades en los controles de seguridad técnicos y no técnicos para robar o comprometer sistemas y redes de información, o para comprometer la disponibilidad para los usuarios legítimos del sistema de información y los recursos de la red.

[FUENTE: ISO/IEC 27033-1:2015, 3.3]

3.3
ataque combinado
ataque que busca maximizar la gravedad del daño y la velocidad de contagio combinando múltiples *vectores de ataque*(3.1)

3.4
bot
Programa de software automatizado utilizado para realizar tareas específicas.

Nota 1 a la entrada: Esta palabra se usa a menudo para describir programas, generalmente ejecutados en un servidor, que automatizan tareas como reenviar u ordenar el correo electrónico.

Nota 2 a la entrada: Un bot también se describe como un programa que opera como agente para un usuario u otro programa o simula una actividad humana. En Internet, los bots más omnipresentes son los programas, también llamados arañas o rastreadores, que acceden a sitios web y recopilan su contenido para los índices de los motores de búsqueda.

3.5
red de robots
colección de bots maliciosos controlados remotamente que se ejecutan de forma autónoma o automática en computadoras comprometidas

EJEMPLO Nodos de denegación de servicio distribuido (DDoS), donde el controlador de la botnet puede dirigir la respuesta del usuario. computadora para generar tráfico a un sitio de terceros como parte de un ataque DDoS coordinado.

3.6
la seguridad cibernética
salvaguardia de las personas, sociedad, organizaciones y naciones de ciberriesgos

Nota 1 a la entrada: Salvaguardar significa (

[FUENTE: ISO/IEC TS 27100:2020, 3.2]

3.7
red oscura
red de sitios web secretos dentro del con software específico

Nota 1 a la entrada: La red oscura también se conoce como la web oscura.

3.8
software engañoso
Software que realiza actividades en la computadora de un usuario sin notificar primero al usuario exactamente qué hará el software en la computadora, o sin pedirle consentimiento para estas acciones.

EJEMPLO 1 Un programa que secuestra las configuraciones del usuario.

EJEMPLO 2 Un programa que genera interminables anuncios emergentes que el usuario no puede detener fácilmente.

EJEMPLO 3 Programas publicitarios y espías.

3.9
hackear
acceder intencionalmente a un sistema informático sin la autorización del usuario o del propietario

3.10
hacktivismo
hackear(3.9) con un propósito motivado política o socialmente

3.11
Internet
sistema global de redes interconectadas en el dominio público

[FUENTE: ISO/IEC 27033-1:2015, 3.14, modificada: “el” se ha eliminado del término.]

3.12

Seguridad de Internet

preservación de la confidencialidad, integridad y disponibilidad de la información a lo largo del *Internet* (3.11)

Nota 1 a la entrada: Además, también pueden estar involucradas otras propiedades, como autenticidad, responsabilidad, no repudio y confiabilidad.

Nota 2 a la entrada: Consulte las definiciones de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, no repudio y confiabilidad en ISO/IEC 27000:2018, Cláusula 3.

3.13

Proveedor de servicios de Internet

ISP

organización que proporciona servicios de Internet a un usuario y permite a sus clientes acceder a la *Internet* (3.11)

Nota 1 a la entrada: También, a veces denominado proveedor de acceso a Internet (IAP).

3.14

contenido malicioso

Aplicaciones, documentos, archivos, datos u otros recursos que tienen características o capacidades maliciosas incrustadas, disfrazadas u ocultas.

3.15

malware

software malicioso

diseño de software con el objetivo de interrumpir, dañar o obtener acceso no autorizado a un sistema que potencialmente pueden causar dañar directa o indirectamente

EJEMPLO Virus, gusanos y troyanos.

3.16

organización

Persona o grupo de personas que tiene funciones propias con responsabilidades, autoridades y relaciones para lograr sus objetivos.

Nota 1 a la entrada: En el contexto de este documento, un individuo es distinto de una organización.

Nota 2 a la entrada: En general, un gobierno también es una organización. En el contexto de este documento, los gobiernos pueden considerarse por separado de otras organizaciones para mayor claridad.

[FUENTE: ISO 9000:2015, 3.2.1, modificada — La Nota 1 a la entrada y la Nota 2 a la entrada han sido reemplazadas.]

3.17

suplantación de identidad

proceso fraudulento de intentar adquirir información privada o confidencial haciéndose pasar por una entidad confiable en una comunicación electrónica

Nota 1 a la entrada: El phishing se puede lograr mediante ingeniería social o engaño técnico.

3.18

software potencialmente no deseado

software engañoso (3.8), incluido *malicioso* (3.15) y software no malicioso, que presentan las características de software engañoso

3.19

correo basura

Correos electrónicos no solicitados que pueden contener contenido malicioso y/o mensajes fraudulentos.

Nota 1 a la entrada: Si bien la forma más reconocida de spam es el spam de correo electrónico, el término se aplica a abusos similares en otros medios: spam de mensajería instantánea, spam de grupos de noticias de Usenet, spam de motores de búsqueda web, spam en blogs, spam de wikis, Spam de mensajes de teléfonos móviles, spam de foros de Internet y transmisiones de fax no deseado.

[FUENTE: ISO/IEC 27033-1:2015, 3.37, modificada. Se agregó la nota 1 a la entrada.]

3.20

software espía

software engañoso(3.8), que recopila información privada o confidencial de un usuario de computadora

Nota 1 a la entrada: La información puede incluir asuntos como los sitios web visitados con mayor frecuencia o información más confidencial, como contraseñas.

3.21

amenaza

causa potencial de un incidente no deseado, que puede resultar en daño a un sistema, individuo o*organización* (3.16)

3.22

troyano

malware(3.15) que parece realizar una función deseable para el usuario pero que lo induce a error sobre su verdadera intención

3.23

vistiendo

phishing de voz realizado para adquirir información privada o confidencial haciéndose pasar por una entidad confiable

Nota 1 a la entrada: El vishing se puede realizar mediante correo electrónico de voz, VoIP (voz sobre IP) o teléfono fijo o celular.

3.24

técnica de pozo de agua

Técnica que incita a las personas a acceder a un Wi malware

Nota 1 a la entrada: El abrevadero también se conoce como abrevadero.

3.25

World Wide Web

Web

universo de información y servicios accesibles en red

[FUENTE: ISO 19101-1:2014, 4.1.40]

4 términos abreviados

En este documento se utilizan los siguientes términos abreviados.

AI	inteligencia artificial
API	Interfaz de programación de aplicaciones
APTO	Amenaza Persistente Avanzada
BYOD	trae tu propio dispositivo
CERTIFICADO	equipo de respuesta a emergencias informáticas
DDoS	denegación de servicio distribuida
DLP	prevención de pérdida de datos
DMZ	zona desmilitarizada
DNS	sistema de nombres de dominio

DoS	negación de servicio
EDR	detección y respuesta de endpoints
ftp	Protocolo de transferencia de archivos
HTTP	Protocolo de Transferencia de Hipertexto
HTTPS	Protocolo de transferencia de hipertexto a través de una capa de conexión segura.
ICANN	Corporación de Internet para nombres y números asignados.
TIC	Tecnología de información y comunicaciones
identificación	sistema de detección de intrusos
IETF	Grupo de Trabajo de Ingeniería de Internet
TMI	equipo de gestión de incidentes
IoT	Internet de las Cosas
IP	Protocolo de Internet
IPS	Sistema de Prevención de Intrusión
ISP	Enterrar norte y sí servicio pag rovider
ISV	suave independiente w Arkansas mi vender o
TRI	equipo de respuesta a incidentes
SGSI	
OWASP	abrir aplicaciones web
PII	información de identificación personal
SDLC	Ciclo de vida del desarrollo de programas
SIEM	información de seguridad y gestión de eventos
PYME	pequeñas y medianas empresas
URL	Localizador Uniforme de Recursos
USB	bus serie universal
vpn	red privada virtual
W3C	Consorcio Mundial de la red
WWW	World Wide Web

5 Relación entre seguridad en Internet, seguridad web, seguridad de redes y ciberseguridad

Figura 1 muestra una visión de alto nivel de la relación entre la seguridad de Internet, la seguridad web, la seguridad de la red y la ciberseguridad.

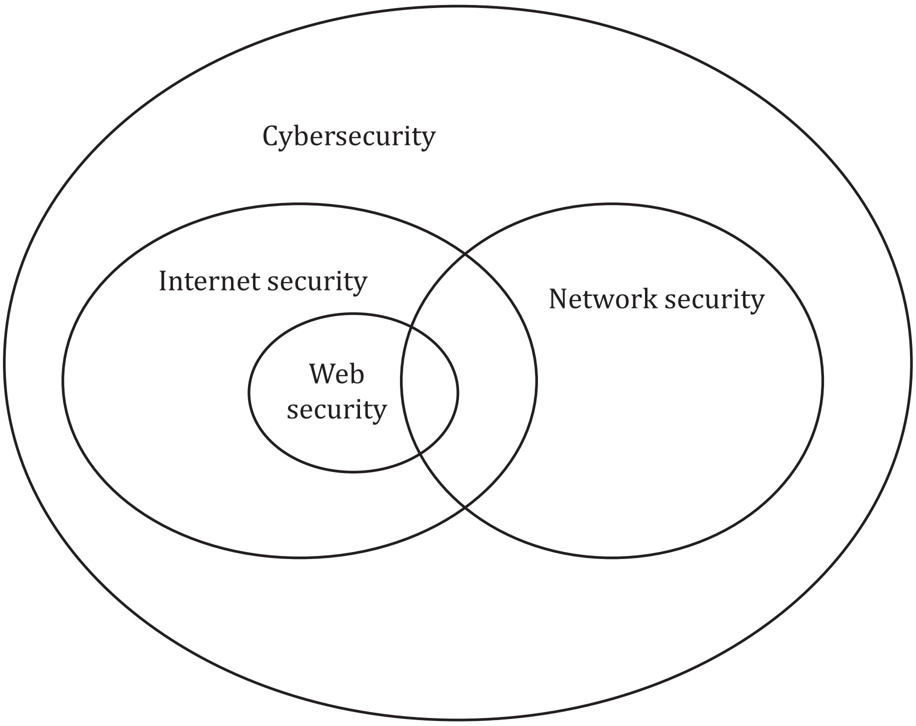

Figura 1 — Relación entre ciberseguridad, seguridad de Internet, seguridad web y seguridad de red

Internet es un sistema global de redes digitales interconectadas de dominio público. El intercambio de información en Internet también utiliza la red de telefonía móvil, que por tanto forma parte de Internet. Esta red global conecta mil millones de personas, computadoras y otros dispositivos de hardware. Cada dispositivo está conectado a Internet, lo que crea un entorno propicio para

La seguridad de Internet se ocupa de proteger los servicios relacionados con Internet y los sistemas y redes de TIC relacionados como una extensión de la seguridad de la red. Estos esfuerzos tienen como objetivo reducir los riesgos de seguridad relacionados con Internet para las organizaciones, los clientes y otras partes interesadas relevantes.

La seguridad de Internet también garantiza la disponibilidad y confiabilidad de los servicios de Internet. A través de Internet se ofrecen diversos servicios, como servicios de transferencia de archivos, servicios de correo o cualquier servicio que pueda compartirse públicamente con los usuarios finales. En este contexto, la seguridad en Internet se ocupa de la prestación segura de estos servicios a través de la red pública.

La web es una de las formas en que se comparte información en Internet [otras incluyen el correo electrónico, el protocolo de transferencia de archivos (FTP) y los servicios de mensajería instantánea]. La web está compuesta por miles de millones de documentos digitales conectados que se pueden ver mediante un navegador web. Un sitio web es un conjunto de páginas web relacionadas que se preparan y mantienen como una colección para respaldar un único propósito.

La seguridad web se ocupa de la seguridad de la información en el contexto de la World Wide Web (WWW) y de los servicios web a los que se accede a través de la red pública. El servicio web se habilita mediante el uso del protocolo HTTP en el que se puede acceder a cualquier URL registrada disponible públicamente. La seguridad web también se ocupa de la seguridad de esta conexión HTTP utilizada para el intercambio de información.

Una red puede incluir componentes como enrutadores, concentradores, cableado, controladores de telecomunicaciones, centros de distribución clave y dispositivos de control técnico. La seguridad de la red cubre ampliamente todo tipo de redes que existen dentro de una organización, desde redes de área local, redes de área amplia, redes de área personal y redes inalámbricas.