Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1208

(01/2014)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación

Recomendación UIT-T X.1208

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1208

Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación

Resumen

La Recomendation UIT-T X.1208 describe una metodología para que las organizaciones utilicen indicadores de ciberseguridad en el cálculo de la medida de riesgo y enumera una lista de posibles indicadores de ciberseguridad.

La finalidad de la Recomendación UIT-T X.1208 es ayudar a las organizaciones que ponen en práctica o explotan una parte de la infraestructura mundial de las tecnologías de la información y la comunicación a evaluar su propia capacidad en materia de ciberseguridad así como el riesgo al que están expuestas. Estas directrices están destinadas a ayudar a las organizaciones a determinar de qué manera reducir los riesgos y a decidir si podrían/deberían invertir recursos para mejorar sus capacidades en materia de ciberseguridad.

La presente Recomendación no propone utilizar un índice o un solo indicador para expresar las capacidades de una organización en materia de ciberseguridad.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1208	2014-01-24	17	11.1002/1000/11950

Palabras clave

Indicador de ciberseguridad, indicador de riesgo de ciberseguridad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1208

Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación

1 Alcance

La presente Recomendación proporciona directrices para ayudar a las organizaciones a elaborar, seleccionar e identificar los datos que deben recopilarse (sobre la base de los indicadores seleccionados) y muestra la manera en que dicha información puede ser utilizada para calcular un indicador de riesgo de ciberseguridad (*CSIR, cybersecurity indicator of risk*). Conviene indicar que una organización puede generar un indicador de riesgo de ciberseguridad con respecto a un conjunto específico de indicadores de ciberseguridad (*CSI, cybersecurity indicators*) en tanto que las unidades de una organización también pueden generar un indicador de riesgo de ciberseguridad con respecto a su conjunto específico de indicadores de ciberseguridad. La finalidad de los indicadores de ciberseguridad es evaluar el nivel de competencia de una organización en materia de ciberseguridad en un momento determinado y, cuando ese proceso se repite en otro momento, determinar la evolución en el tiempo de su programa de ciberseguridad.

La presente Recomendación enumera además una lista de posibles indicadores y describe la metodología que debe aplicarse cuando esos indicadores de ciberseguridad se utilizan para calcular un indicador de riesgo de ciberseguridad.

La finalidad de la presente Recomendación es ayudar a las organizaciones que ponen en práctica o explotan una parte de la infraestructura mundial de las tecnologías de la información y la comunicación a evaluar su propia capacidad en materia de ciberseguridad y a calcular su indicador de riesgo de ciberseguridad. Estas directrices están destinadas a ayudar a las organizaciones a mejorar la ciberseguridad y a determinar de qué manera reducir el riesgo al que están expuestas. Asimismo, dan una indicación sobre si podrían/deberían invertir recursos para mejorar su ciberseguridad.

La presente Recomendación no debe aplicarse para generar un indicador de riesgo de ciberseguridad a nivel nacional. Por otra parte, no propone utilizar un índice o un solo indicador para expresar las capacidades de una organización en materia de ciberseguridad (véase la cláusula 6.1).

NOTA 1 – Los indicadores de riesgo de ciberseguridad calculados de las diferentes organizaciones no son comparables, dado que se supone que cada organización o comunidad seleccionará el conjunto de indicadores de ciberseguridad que considere apropiados para su organización. Por otra parte, se espera que elaboren su propia metodología de medición y sus propios criterios para afrontar los riesgos y los problemas que les plantea. En ciertos casos, la información subjetiva puede reemplazar los datos objetivos. Por consiguiente, se recomienda no comparar nunca los indicadores de riesgo de seguridad entre una organización y otra, ya que dependen en gran medida del contexto.

NOTA 2 – Los indicadores descritos en la presente Recomendación pueden no ser compatibles con los elaborados por otros sectores de actividad, dado que cada uno de ellos tiene finalidades diferentes.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 auditoría [b-UIT-T X.800]: Análisis y examen independiente de las actividades y registros del sistema para verificar el buen funcionamiento de sus controles, garantizar la observancia de los procedimientos de explotación y política establecidos, detectar fallos en la seguridad y recomendar cualesquiera cambios pertinentes en materia de control, política y procedimientos.

3.1.2 bot [b-UIT-T X-Sup.8]: Programa informático automatizado que se emplea para realizar determinadas tareas con fines malignos. Es sinónimo de robot.

3.1.3 ciberseguridad [b-UIT-T X.1205]: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

– disponibilidad;

– integridad, que puede incluir la autenticidad y el no repudio;

– confidencialidad.

3.1.4 medición [b-ENISA]: Acción y efecto de medir, que consiste en determinar el valor de una variable cuantitativa respecto de una unidad de medición (normalizada).

3.1.5 métrica [b-ENISA]: Sistema de medición relativa que permite la cuantificación de ciertas características del sistema, componente o proceso. La métrica está formada por dos o más mediciones..

3.1.6 parche [b-UIT-T X.1206]: Modificación que se distribuye para solucionar una vulnerabilidad de seguridad específica de un producto. Método de actualización de un fichero que consiste en reemplazar únicamente las partes que se modifican, en lugar de todo el fichero.

3.1.7 información de identificación personal (PII) [b-UIT-T X.1252]: Toda información a) que identifica a una persona y que puede utilizarse para identificar, contactar o localizar a la misma; b) que puede utilizarse para obtener información de identificación o de contacto sobre una determinada persona; c) que puede relacionarse directa o directamente con una persona.

3.1.8 riesgo [b-ISO/IEC 27000]: Efecto de la incertidumbre sobre los objetivos.

3.1.9 gestión de riesgos [b-ISO/IEC 27000]: Actividades coordinadas para dirigir y controlar una organización en lo que respecta a los riesgos.

3.1.10 certificado de seguridad [b-UIT-T X.810]: Conjunto de datos pertinentes a la seguridad expedida por una autoridad de seguridad o tercera parte confiable, junto con información de seguridad que se utiliza para proporcionar servicios de integridad y autenticación de origen de los datos.

3.1.11 control de seguridad [b-NIST FIPS 199]: Controles administrativos, operativos y técnicos (es decir, salvaguardias y contramedidas) prescritos para un sistema de información a los efectos de proteger la confidencialidad, la integridad y la disponibilidad de dicho sistema y de su información.

3.1.12 incidente de seguridad [b-ITU-T E.409]: Cualquier evento adverso que podría amenazar algún aspecto relacionado con la seguridad.

3.1.13 spam [b-ITU-T X.1242]: Información electrónica que circula desde el remitente hasta el destinatario mediante terminales tales como computadores, teléfonos móviles, teléfonos, etc. que, por regla general, no se ha solicitado, ni deseada y que perjudica a los destinatarios.

3.1.14 amenaza [b-ISO/IEC 27000]: Causa posible de incidente indeseado, que podría perjudicar a un sistema u organización.

3.1.15 vulnerabilidad [b-ITU-T X.1500]: Cualquier debilidad que pudiera utilizarse para vulnerar un sistema o la información que contiene. (En consonancia con el Anexo A de [b-ITU-T X.800].)

3.1.16 debilidad [b-ITU-T X.1500]: Defecto o imperfección que, aunque no se reconozca en sí misma, pudiera en algún momento convertirse en vulnerabilidad o contribuir a la introducción de otras vulnerabilidades.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 indicador de ciberseguridad: Todo indicador de la serie de indicadores utilizados para calcular o medir el grado de riesgo o de competencia de una organización o una comunidad en materia de ciberseguridad.

NOTA − Los indicadores de ciberseguridad seleccionados son indicadores que han sido seleccionados debido a su importancia, es decir, guardan en cierta forma relación con posibles riesgos.

3.2.2 indicador de riesgo de ciberseguridad: Resultado de aplicar una metodología que calcula un indicador de riesgo de ciberseguridad.

3.2.3 conjunto de indicadores de ciberseguridad: Conjunto seleccionado de indicadores de ciberseguridad que será utilizado para calcular un indicador de riesgo de ciberseguridad.

NOTA – No hay un solo conjunto de indicadores de ciberseguridad.

3.2.4 indicador: Sinónimo de métrica (cláusula 3.1.5).

3.2.5 sistema de gestión de la seguridad de la información: Parte del sistema general de gestión que, a partir de un análisis de riesgo de su actividad, establece, aplica, explota, supervisa, examina, mantiene y mejora la seguridad de la información, véase la cláusula 3.2.1 de [b-ISO/IEC 27000].

NOTA − El sistema de gestión comprende la estructura orgánica, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

3.2.6 programa (de actividades): Conjunto de actividades coordinadas destinadas a lograr un objetivo determinado.

3.2.7 programa (informático): Conjunto de instrucciones codificadas que permite a una máquina, en particular a una computadora, realizar una secuencia de operaciones deseada.

3.2.8 origen de la amenaza: Acto o método para explotar deliberadamente una vulnerabilidad o situación y método que pudieran dar lugar accidentalmente a una vulnerabilidad.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

AS Sistema autónomo (*autonomous system*)

BSA Business Software Alliance

C&A Certificado y acreditado (*certified and accredited*)

CIS Center for Internet Security

CSI Indicador de ciberseguridad (*cybersecurity indicator*)

CSIR Indicador de riesgo de ciberseguridad (*cybersecurity indicator of risk*)

CVE Vulnerabilidades y contingencias comunes (*common vulnerabilities and exposures*)

CYBEX Intercambio de información de ciberseguridad (*cybersecurity information exchange)*

DB Base de datos (*data base*)

DDoS Denegación del servicio distribuida (*distributed denial-of-service*)

DHCP Protocolo de configuración dinámica de anfitrión (*dynamic host configuration protocol)*

DoS Denegación del servicio (*denial-of-service*)

DNS Sistema de nombres dinámico (*dynamic name system*)

ID Identificador

IDS Sistema de detección de intrusiones (*intrusion detection system*)

IP Protocolo Internet (*Internet protocol*)

IPS Sistema de prevención de intrusiones (*intrusion prevention system*)

ISMS Sistema de gestión de la seguridad de la información (*information security management system*

PCA Análisis de los componentes principales (*principal components analysis*)

PII Información de identificación personal (*personally identifiable information*)

PIB Producto interior bruto

SSL Capa de conexión segura (*secure socket layer*)

TI Tecnología de la información

TIC Tecnologías de la información y la comunicación

TLS Seguridad en la capa de transporte (*transport layer security*)

TTP Tercero fiable (*trusted third party*)

5 Convenios

En la presente Recomendación, el término organización debe interpretarse en un sentido amplio. Queda entendido que una comunidad debe considerarse incluida en el término organización. Sin embargo, nunca debe considerarse que organización es equivalente a país.

6 Indicador de ciberseguridad

6.1 Introducción

Se han invertido numerosos esfuerzos para medir el rendimiento de las Tecnologías de la Información y la Comunicación (TIC), seguir su evolución y evaluar la incidencia de su utilización por los gobiernos, los operadores, los investigadores y las empresas del sector privado. Entre los ejemplos de indicadores específicos de cada sector se encuentra el *Global Cloud Computing Scorecard* [b-BSA] y las métricas de seguridad publicadas por el Center for Internet Security [b-CIS]. Los indicadores descritos en la presente Recomendación corresponden a ciertos aspectos particulares de la ciberseguridad.

El indicador de riesgo de ciberseguridad descrito en la presente Recomendación asocia numerosos indicadores de ciberseguridad para medir el grado de riesgo que afecta, en un determinado momento, las capacidades de ciberseguridad de una organización o una comunidad y su eficacia, así como la eficiencia de la aplicación de controles de seguridad.

Un indicador de riesgo de ciberseguridad puede calcularse a partir de una autoevaluación de sus capacidades de ciberseguridad o a partir de un conjunto de indicadores calculados por una organización externa. La presente Recomendación está destinada a ser utilizada en el caso de la autoevaluación por parte de una organización.

Los indicadores de esta Recomendación pueden seleccionarse teniendo en cuenta Normas Internacionales sobre sistemas de gestión de la seguridad de la información [b-ISO/CEI 27001], [b-ISO/CEI 27002], [b-ISO/CEI 27003], seguridad de la red [b-ISO/CEI 27033-1], [b-ISO/CEI 27033-2], [b-ISO/CEI 27033-4] y otras especificaciones [b-NIST SP 800-27], [b-NIST SP 800-30], [b-NIST SP 800-53]. Las normas internacionales relativas a la gestión permiten a las organizaciones diseñar, aplicar y mantener un conjunto coherente de políticas, procesos y sistemas para gestionar el riesgo relacionado con sus activos de información, garantizando así que el riesgo de seguridad de la información se mantenga en niveles aceptables. Las normas internacionales relativas a la seguridad de la red definen y describen los conceptos asociados con la seguridad de la red y dan orientaciones para su gestión. Las demás especificaciones ofrecen el concepto básico de control para reducir los riesgos que corren los activos de información e indican cómo gestionar tales riesgos en el entorno TIC de la organización.

Los indicadores pueden agruparse según su función administrativa: gestión de incidentes, gestión de vulnerabilidades, gestión de parches, seguridad en las aplicaciones, gestión de la configuración y aspectos financieros.

La presente Recomendación no propone utilizar un índice o un solo indicador para expresar las capacidades de una organización en materia de ciberseguridad. Esto se debe a que la seguridad de una organización sólo es tan buena como su eslabón más débil y la utilización de un índice para expresar las capacidades de la organización en materia de ciberseguridad no identifica debidamente los posibles efectos derivados del eslabón más débil. Si un indicador de riesgo de ciberseguridad se presenta como un número único, puede inducir a error a quienes deban utilizar ese número. También podría crear falsas expectativas en quienes lo utilicen para tomar una decisión. Concretamente, cuando un cierto número de indicadores se combinan y normalizan en un solo número (es decir, en un índice), la existencia y la importancia de los puntos débiles de una organización en materia de ciberseguridad ya no son tan claras. Por consiguiente, no convendría utilizar ese índice para indicar que las capacidades de una organización en materia de ciberseguridad son satisfactorias ni para comparar las capacidades de diferentes organizaciones al respecto.

6.2 Principios generales de los indicadores de ciberseguridad

En esta cláusula se describen los principios generales que convendría tener en cuenta en la elaboración de indicadores de ciberseguridad.

- Al calcular un indicador de riesgo de seguridad, habría que utilizar un conjunto de indicadores acordado a escala mundial.
- Habría que seleccionar indicadores de ciberseguridad de tal forma que puedan utilizarse para evaluar, en un determinado momento, el grado de competencia de una organización o una comunidad contra las amenazas en materia de ciberseguridad o para determinar la evolución de su programa de ciberseguridad.
- Los indicadores de ciberseguridad deberían seleccionarse de tal forma que tengan en cuenta la precisión y confidencialidad de los datos primarios recopilados y utilizados para calcular el indicador de riesgo de ciberseguridad.
- Los métodos de recopilación deben mantener la integridad de los datos primarios, que constituirán la base para el cálculo del indicador de riesgo de ciberseguridad.
- Habría que utilizar indicadores que puedan ayudar a los encargados de adoptar decisiones a medir el rendimiento de la aplicación de las políticas en materia de seguridad de la información y a seguir la evolución del programa de ciberseguridad.

- Convendría elaborar nuevos indicadores o modificar los existentes a su debido tiempo habida cuenta de la rápida evolución de los servicios y tecnologías TIC.

6.3 Directrices para la selección de indicadores de ciberseguridad

A la hora de seleccionar los indicadores que serán utilizados para calcular un indicador de riesgo de ciberseguridad, quizá convenga que una organización seleccione aquellos que faciliten el cumplimiento de sus metas y objetivos. Por ejemplo, las organizaciones pueden seleccionar los indicadores en función de sus actividades prioritarias.

En particular, un indicador de ciberseguridad debería tener en cuenta:

- la evaluación del principal efecto en los resultados de las actividades;
- su utilización para resolver problemas a nivel de sistema, a nivel de programa y a ambos niveles, llegado el caso;
- la medición de la evolución de la aplicación del programa de ciberseguridad, de los controles de seguridad específicos y de las correspondientes políticas y procedimientos afines en materia de ciberseguridad;
- la medición de los aspectos que permitirán definir la eficacia y eficiencia de un programa de ciberseguridad;
- la medición del efecto positivo o negativo de un programa de ciberseguridad en la misión de una organización;
- la medición de los resultados de la aplicación de políticas de ciberseguridad, que tengan la capacidad de obtener resultados a nivel de sistema, a nivel de programa o a ambos niveles;
- la medición de los efectos positivos y negativos en la vida cotidiana de los usuarios.

Por otra parte, habría que seleccionar un indicador de ciberseguridad que tenga en cuenta la recopilación de datos primarios de forma exacta y fiable. Durante todo el proceso de medición, es necesario asegurar la disponibilidad de los datos primarios, la integridad de los datos que se utilizan y la disponibilidad de la protección de la privacidad de los datos.

6.4 Clasificación de indicadores

Los indicadores se pueden clasificar en tres tipos en función de su naturaleza, a saber, los relativos a la aplicación, la eficacia/eficiencia y la incidencia. Los indicadores relativos a la aplicación sirven para mostrar cómo evoluciona un programa de seguridad de la información, las medidas de seguridad específicas y las correspondientes políticas y procedimientos en materia de seguridad. Pueden dividirse en dos subtipos: indicadores a nivel de programa y a nivel de sistema. Un ejemplo de indicador de aplicación a nivel de sistema es el porcentaje de personal de seguridad de sistemas de información que han recibido formación en materia de seguridad.

Los indicadores de eficacia/eficiencia pueden utilizarse para verificar si se aplican correctamente controles de seguridad a nivel de sistema y procesos a nivel de programa, si funcionan según lo previsto, y si satisfacen las metas y los objetivos deseados. Miden dos aspectos de los resultados de la aplicación del control de seguridad: la eficacia y eficiencia del resultado, es decir, la eficacia se refiere a la robustez y la eficiencia a la puntualidad. Como ejemplo de indicador de eficacia puede citarse el porcentaje de incidentes de seguridad de la información debidos a una mala configuración del control de acceso; un ejemplo de indicador de eficiencia es el porcentaje de componentes del sistema que reciben mantenimiento según el calendario previsto.

Los indicadores de incidencia tratan de especificar la incidencia de la seguridad de la información en la misión de una organización. Pueden ser utilizados para cuantificar el ahorro producido por el programa de seguridad de la información o el coste incurrido al resolver los incidentes de seguridad de la información, el grado de confianza pública obtenido por el programa de seguridad de la información, u otros efectos de la seguridad de la información relacionados con la misión. Como

ejemplo de este indicador puede citarse el porcentaje de gastos consagrados por una organización a la seguridad de la información respecto a los gastos totales consagrados a los sistemas de información.

Por otra parte, los indicadores pueden agruparse de acuerdo con su función administrativa: gestión de incidentes, gestión de vulnerabilidades, gestión de parches, seguridad en las aplicaciones, seguridad de la configuración, aspectos financieros, seguridad de los datos y la red, etc.

7 Proceso de elaboración del indicador de ciberseguridad

7.1 Introducción

El conjunto de indicadores de ciberseguridad debería considerarse una herramienta fundamental para evaluar la validez de la aplicación de las políticas de seguridad de la información y determinar la situación de una organización en un determinado momento en cuanto a la seguridad de la información.

7.2 Metodología para la elaboración de un conjunto de indicadores de ciberseguridad

La elaboración de un conjunto de indicadores de ciberseguridad es una tarea compleja que se debe encargar a profesionales muy cualificados expertos en economía, ciberseguridad y estadística. Para elaborar la lista de indicadores de ciberseguridad, hay que tener en cuenta el contexto de la organización y los diferentes aspectos del riesgo que se ha de medir.

Un diseñador de indicadores de ciberseguridad debería tener en cuenta que un determinado indicador podría experimentar una importante variabilidad, a diferencia de los indicadores con muestras grandes, debido a la escasez de las muestras que se miden, por ejemplo, incidentes, que podrían observarse a escala limitada. Por consiguiente, el análisis macroscópico tendría que ser aplicado con sumo cuidado.

A continuación se indican las etapas que podrían seguirse para elaborar un conjunto de indicadores de ciberseguridad y lograr que la información esté lista para su utilización:

- determinar los principales indicadores que deben seleccionarse y utilizarse para calcular el indicador de riesgo de ciberseguridad;
- identificar las fuentes de datos;
- gestionar las observaciones que faltan;
- hacer que los indicadores sean comparables entre sí;
- convertir los indicadores en valores de medición del riesgo;
- aprovechar la recopilación de valores de medición del riesgo.

7.2.1 Selección de indicadores para crear una medida de riesgo

La selección de indicadores para crear la medida de riesgo dependerá de lo que se desea medir y de la viabilidad de recabar datos primarios.

NOTA – Aunque tal vez no sea práctico realizar una medición en la actualidad, un indicador podría ser objeto de un serio examen de selección. Es posible que este proceso pueda utilizarse para identificar una nueva actividad que tenga en cuenta la obtención de datos para que ese riesgo pueda ser correctamente evaluado.

El número de indicadores dependerá de la misión y objetivos de la organización o del tipo de tecnologías que ésta utilice. Se recomienda utilizar una amplia gama de indicadores (por ejemplo, de 10 a 30) para crear la medida de riesgo de un indicador de riesgo de ciberseguridad. La combinación de indicadores subjetivos con mediciones objetivas puede afectar la validez del cálculo resultante. Por consiguiente, se recomienda evitar recurrir a indicadores subjetivos al crear un indicador de riesgo de ciberseguridad. Sin embargo, para ciertos aspectos de la gestión de riesgos puede ser necesario un indicador subjetivo, por lo que es fundamental definir muy detalladamente cómo definirlo. Una vez seleccionados los indicadores, podría ser conveniente agruparlos en distintas categorías con arreglo a su función administrativa, por ejemplo gestión de incidentes, gestión de

vulnerabilidades, gestión de parches, etc. De este modo, los indicadores resultan más fáciles de gestionar y las comparaciones más pertinentes.

En la cláusula 7.3 se describe en detalle el procedimiento de elaboración.

7.2.2 Fuentes de datos

La disponibilidad de datos para los indicadores de ciberseguridad puede determinar el número y calidad de los indicadores para el cálculo de un indicador de riesgo de ciberseguridad. Una dependencia excesiva de una sola fuente de datos puede dar lugar a errores y omisiones. Por tanto, es fundamental verificar los datos con diversas fuentes antes de utilizarlos para calcular un indicador de riesgo de ciberseguridad

7.2.3 Gestión de los datos que faltan

Cuando se recopilan medidas de riesgo para un indicador de ciberseguridad, es posible que falten datos o que no estén disponibles. En esos casos, se pueden dejar en blanco esos datos – es decir, no se asigna valor alguno a ese indicador – o se puede recurrir a una extrapolación para estimar los datos que faltan. Dejar los datos en blanco puede dar lugar a la exclusión de ciertos aspectos del indicador de ciberseguridad. La extrapolación puede amplificar el valor de los datos y, por ello, inflar los resultados calculados. Es preciso entonces llegar a un equilibrio entre la extrapolación y la omisión, equilibrio que tendrá en cuenta el valor de los datos o la importancia de los indicadores. Se podría efectuar una prueba de sensibilidad para determinar el grado de sensibilidad de los resultados calculados a las fluctuaciones del valor extrapolado o si los datos en blanco son sustituidos por un valor estimado.

7.2.4 Transformación de los datos

La transformación se realiza en dos etapas: primero se convierten los valores absolutos en valores relativos y luego se convierten los valores relativos de los indicadores en un indicador de riesgo de ciberseguridad. Por lo general, los valores absolutos se hacen comparables al dividirlos por el número total de elementos. Es posible que muchos indicadores ya estén disponibles en su forma transformada, por lo que no es necesario realizar esta etapa.

7.3 Proceso de elaboración de indicadores de ciberseguridad

El proceso de elaboración de indicadores de ciberseguridad comprende la selección de los indicadores que resultan adecuados para la misión y los objetivos de la organización o comunidad. Este proceso consta de cinco etapas, a saber: identificación de los intereses de las partes, definición de metas y objetivos, examen de las políticas, directrices y procedimientos en materia de seguridad de la información, análisis de la seguridad de la información aplicada y selección de indicadores.

Etapa 1 – Identificación de los intereses de las partes: consiste en identificar a las partes pertinentes y sus intereses. Los principales interesados son el jefe de la organización, el director de información, el director de seguridad, el director de seguridad de los sistemas de información, el administrador de programas, el administrador de red, los ingenieros de seguridad y el personal auxiliar del sistema informático. El resultado de esta etapa comprende todos los intereses en medir la seguridad de la información. Cada parte interesada puede solicitar un conjunto diferente de indicadores que representan su punto de vista en su ámbito de responsabilidad.

Etapa 2 – Definición de metas y objetivos: consiste en identificar las metas y objetivos de la seguridad de la información. Puede expresarse mediante políticas, requisitos, directrices y orientaciones. Las metas y objetivos del programa de seguridad pueden ser determinados a partir de las metas y objetivos de alto nivel de la organización para asegurar su misión.

Etapa 3 – Examen de las políticas, directrices y procedimientos en materia de seguridad de la información: consiste en describir en detalle cómo deben aplicarse controles de seguridad en las políticas y procedimientos específicos de la organización.

Etapa 4 – Análisis de la seguridad de la información aplicada: consiste en examinar los indicadores existentes y los bancos de datos pertinentes que pueden utilizarse para obtener nuevos indicadores.

Etapa 5 – Selección de indicadores: implica la selección y elaboración, según proceda, de tres tipos de indicadores descritos en la cláusula 6.4. Esta etapa implica la selección de un conjunto de indicadores que siguen la pista de la aplicación del proceso, la eficiencia/eficacia y el efecto en la misión, y si es necesario, la elaboración de nuevos indicadores.

8 Posibles indicadores de ciberseguridad

En esta cláusula se describen diversos indicadores de ciberseguridad considerados esenciales y que pueden aplicarse para crear un conjunto de indicadores de ciberseguridad destinados a una organización. Los indicadores pueden clasificarse en tres categorías: indicadores básicos, recomendados o facultativos. Asimismo, los indicadores pueden clasificarse en tres categorías dependiendo de su naturaleza: indicadores relativos a la aplicación, a la eficacia/eficiencia y a la incidencia. En la presente Recomendación no se define el nivel de exigencia asociado a cada indicador. Se espera que las organizaciones determinen el nivel de exigencia de cada indicador, en función de su política de seguridad. Además, las organizaciones deben elaborar, y se invita a que lo hagan, otros indicadores para resolver su propia situación.

Los indicadores que se describen en esta cláusula (véanse los Cuadros 8-1 a 8-30) se han concebido para una organización; no obstante, pueden aplicarse a una comunidad si se suman los indicadores de las organizaciones que pertenecen a dicha comunidad.

Hay indicadores para los que, en ciertos casos, sería más conveniente un valor más grande, es decir, mejor más grande, y en otros casos, un valor más pequeño, es decir, mejor más pequeño. Hay otro tipo de casos en los que no puede saberse si es mejor un valor más grande o más pequeño.

Cuadro 8-1 – Indicador 1: Gestión de vulnerabilidades (a nivel de programa, mejor más grande)

Campo	Datos
ID del indicador	Porcentaje de vulnerabilidades de alto impacto mitigadas.
Objetivo	La organización debe tratar a tiempo las vulnerabilidades conocidas.
Indicador	Porcentaje de vulnerabilidades de alto impacto mitigadas dentro del plazo definido por la organización desde su descubrimiento.
Fórmula	(Número total de vulnerabilidades de alto impacto mitigadas a tiempo/Número total de vulnerabilidades de alto impacto identificadas) × 100.
Data primarios	• Número de vulnerabilidades identificadas dentro del plazo especificado por la organización. (No olvidar que el número de vulnerabilidades de alto impacto identificadas dentro del plazo especificado por la organización debe ser calculado a partir de los datos primarios.) • Número de vulnerabilidades de alto impacto mitigadas dentro del plazo.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	Recomendación UIT-T X.1521, Sistema de puntuación para las vulnerabilidades corrientes, [b-UIT-T X.1521] y Recomendación UIT-T X.1520, Vulnerabilidades y riesgos corrientes (CVE) [b-UIT-T X.1520].

Cuadro 8-2 – Indicador 2: Mantenimiento de registros de inspección (a nivel de sistema, mejor más grande)

Campo	Datos
ID del indicador	Porcentaje de dispositivos de punto extremo para los que se mantiene un registro de inspección.
Objetivo	La organización debería mantener un registro de inspección del sistema con el fin de investigar las actividades impropias de los puntos extremos.
Indicador	Porcentaje de dispositivos de punto extremo para los que se mantiene un registro de inspección.
Fórmula	(Número total de dispositivos de punto extremo con registro de inspección/Número total de dispositivos de punto extremo) × 100.
Data primarios	• Número de dispositivos de punto extremo para los que se mantiene un registro de inspección en un servidor centralizado o en el dispositivo de punto extremo. • Número total de dispositivos de punto extremo.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-3 – Indicador 3: Respuesta a incidentes (a nivel de sistema y de programa, mejor más grande)

Campo	Datos
ID del indicador	Respuesta a incidentes.
Objetivo	La organización debe notificar los incidentes a tiempo para cada categoría de incidentes.
Indicador	Porcentaje de incidentes notificados dentro del plazo estipulado para la categoría del caso.
Fórmula	(Número de incidentes notificados a tiempo/Número total de incidentes notificados) × 100, para cada categoría.
Data primarios	• Número de incidentes notificados dentro del plazo estipulado por la organización. • Número total de incidentes notificados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	Recomendación UIT-T X.1544, Enumeración y clasificación de pautas de ataques comunes [b-UIT-T X.1544].

Cuadro 8-4 – Indicador 4: Tiempo medio para mitigar vulnerabilidades (a nivel de sistema y de programa, mejor más pequeño)

Campo	Datos
ID del indicador	Tiempo medio para mitigar vulnerabilidades.
Objetivo	Indicar el rendimiento de la organización en la resolución de las vulnerabilidades detectadas. Cuanto menos tiempo requiera, mayor será la probabilidad de que la organización pueda reducir con eficacia el riesgo de explotación de vulnerabilidades.
Indicador	Tiempo medio para mitigar vulnerabilidades cuantifica el tiempo medio para mitigar las vulnerabilidades identificadas en una organización.
Fórmula	Suma (Día_vulnerabilidad_resuelta – Día de detección)/Número (vulnerabilidades_resueltas).
Data primarios	• Fecha de detección de las vulnerabilidades. • Fecha de mitigación de las vulnerabilidades. • Número total de vulnerabilidades detectadas. • Número total de vulnerabilidades mitigadas notificadas.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	Recomendación UIT-T X.1521, Sistema común de puntuación de vulnerabilidades, [b-UIT-T X.1521] y Recomendación UIT-T X.1520, Vulnerabilidades y exposiciones comunes (CVE) [b-UIT-T X.1520].

Cuadro 8-5 – Indicador 5: Distribución de programa de parches de seguridad (a nivel de sistema, mejor más grande)

Campo	Datos
ID del indicador	Programa de parches de seguridad.
Objetivo	Que los dispositivos de punto extremo instalen un programa de parches de seguridad para mitigar las vulnerabilidades.
Indicador	Porcentaje de dispositivos de punto extremo que tienen instalado el sistema de gestión de parches.
Fórmula	(Número total de dispositivos de punto extremo que utilizan un programa de parches de seguridad/Número total de dispositivos de punto extremo) × 100.
Data primarios	• Número total de dispositivos de punto extremo que disponen de un programa de parches de seguridad. • Número de dispositivos de punto extremo.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-6 – Indicador 6: Tiempo medio de instalación de un parche (a nivel de sistema y de programa, mejor más pequeño)

Campo	Datos
ID del indicador	Tiempo medio de instalación de un parche.
Objetivo	Cuantificar el tiempo medio que se tarda en distribuir un parche para los sistemas de la organización. Cuanto más rápido se distribuya, menor es el tiempo medio de instalación de un parche, y menos tiempo tarda la organización en instalarlo en sus sistemas en estado vulnerable.
Indicador	Tiempo medio que se tarda en instalar un parche para los sistemas de la organización.
Fórmula	Suma (Fecha_instalación – Fecha_disponibilidad)/Número (parches_aplicados).
Data primarios	• Fecha de instalación. • Fecha de disponibilidad. • Número total de parches aplicados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	-

Cuadro 8-7 – Indicador 7: Tiempo medio para modificar la configuración (a nivel de sistema y de programa, mejor más pequeño)

Campo	Datos
ID del indicador	Tiempo medio para realizar una modificación de la configuración.
Objetivo	Cuantificar el tiempo medio para realizar una modificación de la configuración en los sistemas de la organización. Cuanto más rápido se realice el cambio, menor será el tiempo para instalar el parche y, menos tardará la organización en modificar los sistemas en estado inestable.
Indicador	Tiempo medio para realizar una modificación de la configuración en los sistemas de la organización.
Fórmula	Suma (Fecha_terminación – Fecha_presentación)/Número (Cambios_realizados)
Data primarios	• Fecha de terminación. • Fecha de presentación. • Número total de cambios realizados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-8 – Indicador 8: Cobertura del análisis de riesgos (a nivel de sistema y de programa, mejor más grande)

Campo	Datos
ID del indicador	Cobertura de análisis de riesgos.
Objetivo	La organización debería realizar el mayor número posible de análisis de riesgos de las aplicaciones en sus sistemas.
Indicador	Porcentaje de aplicaciones administrativas que han sido objeto de un análisis de riesgos en algún momento.
Fórmula	Número (aplicaciones_objeto_análisis de riesgos)/Número (aplicaciones) × 100.
Data primarios	• Número de aplicaciones que han sido objeto de un análisis de riesgos. • Número de aplicaciones.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-9 – Indicador 9: Cobertura del programa de detección y tratamiento de malware (a nivel de sistema, mejor más grande)

Campo	Datos
ID del indicador	Cobertura del programa de detección y tratamiento de malware.
Objetivo	Dispositivos de usuario final con programas antivirus para mitigar el malware, incluidos los virus que residen en esos dispositivos.
Indicador	Porcentaje de dispositivos de punto extremo con programas de detección y tratamiento de malware.
Fórmula	(Número total de dispositivos de punto extremo con programas de detección y tratamiento de malware/número total de dispositivos de punto extremo) × 100.
Data primarios	• Número total de dispositivos de punto extremo con programas antivirus. • Número de dispositivos de punto extremo.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-10 – Indicador 10: Cobertura del plan de contingencias (a nivel de programa, mejor más grande)

Campo	Datos
ID del indicador	Pruebas del plan de contingencias.
Objetivo	La organización debería realizar pruebas del plan de contingencias para sistemas de información.
Indicador	Porcentaje de sistemas de información para los que se han realizado pruebas del plan de contingencias.
Fórmula	(Número de sistemas de punto extremo para los que se han realizado pruebas del plan de contingencias/Número total de sistemas de punto extremo) × 100.
Data primarios	• Número de sistemas de información para los que se han realizado pruebas del plan de contingencias. • Número de sistemas de punto extremo.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-11 – Indicador 11: Evaluación de la seguridad (a nivel de programa, mejor más grande)

Campo	Datos
ID del indicador	Porcentaje de sistemas de información con evaluación positiva de la seguridad.
Objetivo	El sistema de punto extremo de una organización debería certificarse y acreditarse antes de su instalación para garantizar un contexto de seguridad y responsabilidad exhaustivo para el personal, las instalaciones y los productos.
Indicador	Porcentaje de nuevos sistemas de punto extremo que se han certificado y acreditado antes de su instalación.
Fórmula	(Número de nuevos sistemas de información certificados y acreditados/Número total de sistemas de información) × 100.
Data primarios	• Número de nuevos sistemas de punto extremo certificados y acreditados. • Número de sistemas de punto extremo.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-12 – Indicador 12: Compromiso en materia de seguridad (a nivel de programa, mejor más grande)

Campo	Datos
ID del indicador	Compromiso o código de conducta en materia de seguridad.
Objetivo	Los empleados autorizados a acceder a los sistemas de información deberían firmar un compromisos en materia de seguridad antes de poder acceder a los sistemas de punto extremo de la organización.
Indicador	Porcentaje del personal encargado de la seguridad de los sistemas de información que han firmado el compromiso.
Fórmula	(Número de empleados con acceso a los sistemas que han firmado el reglamento de conducta/Nº total de empleados autorizados a acceder al sistema de punto extremo) × 100.
Data primarios	• Número de empleados con acceso a los sistemas que han firmado el compromiso en materia de seguridad. • Número de empleados con acceso a los sistemas.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-13 – Indicador 13: Control del acceso a distancia mediante pasarela de seguridad (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Puntos de acceso a distancia protegidos.
Objetivo	La organización debería instalar pasarelas de seguridad que permitan proteger los activos internos cuando se emplea el acceso a distancia.
Indicador	Porcentaje de puntos de acceso a distancia protegidos.
Fórmula	(Número de puntos de acceso a distancia que utilizan una pasarela de seguridad/Número total de puntos de acceso a distancia de la organización) × 100.
Data primarios	• Número de puntos de acceso a distancia que utilizan pasarelas de seguridad. • Número de puntos de acceso a distancia protegidos.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-14 – Indicador 14: Control de acceso a distancia con función de seguridad para la prevención de intrusiones o la detección de intrusiones (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Puntos de acceso a distancia protegidos.
Objetivo	La organización debería instalar una función de seguridad para detectar o prevenir las intrusiones a fin de proteger los activos internos de la organización.
Indicador	Porcentaje de puntos de acceso a distancia protegidos.
Fórmula	(Número de puntos de acceso a distancia que aplican la función de seguridad para la detección y prevención de intrusiones/Número total de puntos de acceso a distancia) × 100.
Data primarios	• Número de puntos de acceso a distancia que aplican la función de seguridad para la detección o prevención de intrusiones. • Número de puntos de acceso a distancia.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-15 – Indicador 15: Control del acceso inalámbrico (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Puntos de acceso inalámbrico protegidos.
Objetivo	La organización debería disponer de protección en los puntos de acceso inalámbrico para proteger la red interna contra el acceso no autorizado.
Indicador	Porcentaje de puntos de acceso inalámbrico protegidos.
Fórmula	(Número de puntos de acceso inalámbrico protegidos/Número total de puntos de acceso inalámbrico) × 100.
Data primarios	• Número de puntos de acceso inalámbrico protegidos. • Número de puntos de acceso inalámbrico.
Frecuencia	Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-16 – Indicador 16: Seguridad personal (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Control de seguridad personal.
Objetivo	La organización debería permitir que el personal autorizado acceda a sistemas de punto extremo.
Indicador	Porcentaje de individuos controlados antes de concederles el acceso a los sistemas de punto extremo de la organización.
Fórmula	(Número de individuos controlados/Número total de individuos con acceso) × 100.
Data primarios	• Número de individuos controlados. • Número de individuos.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-17 – Indicador 17: Protección de la información de identificación personal (PII) (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Porcentaje de información de identificación personal protegida.
Objetivo	La organización debería proteger la información de identificación personal confidencial mediante encriptación.
Indicador	Porcentaje de información de identificación personal protegida.
Fórmula	(Número de información de identificación personal confidencial encriptada/Número total de información de identificación personal) × 100.
Data primarios	• Número de elementos de información de identificación personal protegida. • Número total de elementos de información de identificación personal.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia y aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-18 – Indicador 18: Protección de las copias de seguridad de los datos (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Tasa de copias de seguridad de los datos cuya integridad se ha inspeccionado.
Objetivo	La organización debería proteger la integridad de las copias de seguridad de los datos.
Indicador	Porcentaje de las copias de seguridad de los datos cuya integridad se ha protegido.
Fórmula	(Volumen de copias de seguridad de los datos cuya integridad se ha protegido/ Volumen total de copias de seguridad de los datos) × 100.
Data primarios	• Volumen de copias de seguridad de los datos cuya integridad se ha protegido. • Volumen total de copias de seguridad.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia y aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-19 – Indicador 19: Cobertura del sistema certificado de gestión de la seguridad (por ejemplo, ISMS) (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Cobertura del sistema de gestión.
Objetivo	El punto extremo de la organización debería estar cubierto por un sistema certificado de gestión de la seguridad (por ejemplo, ISMS).
Indicador	Porcentaje de sistemas de punto extremo cubiertos por el sistema certificado de gestión de la seguridad.
Fórmula	(Número de sistemas de punto extremo cubiertos por el sistema certificado de gestión de la seguridad (por ejemplo, ISMS)/Número total de sistemas de punto extremo) × 100.
Data primarios	• Número de sistemas de punto extremo cubiertos por el sistema certificado de gestión de la seguridad (por ejemplo, ISMS). • Número total de sistemas de punto extremo.
Frecuencia	Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia y aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-20 – Indicador 20: Instalación de un servidor seguro (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Instalación de un servidor seguro.
Objetivo	Los servicios de red de la organización deberían intercambiar información a través de un túnel seguro para el acceso a distancia.
Indicador	Porcentaje de servicios de red que utilizan un túnel seguro, por ejemplo, TLS, SSL o *secure shell*.
Fórmula	(Número de servicios de red que utilizan un túnel seguro/Número total de servicios de red) × 100.
Data primarios	• Número de servicios de red que utilizan un canal seguro. • Número total de servicios de red.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia y aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	
NOTA – Hay muchas maneras de utilizar el servidor seguro (mencionado en el título del indicador) para que ofrezca un túnel seguro entre puntos extremos. Se incluyen los servidores protegidos con SSL/TLS y *secure shell*	

Cuadro 8-21 – Indicador 21: Tasa de spam recibido (a nivel de programa, mejor más pequeño)

Campo	Datos
ID del indicador	Tasa de spam recibido
Objetivo	La organización debería utilizar filtros para bloquear los mensajes spam para que no los reciban los empleados.
Indicador	Porcentaje de empleados que reciben un número de mensajes spam mayor que el definido por la organización en un determinado intervalo de tiempo.
Fórmula	(Número de empleados que recibe un determinado número de mensajes spam/Número total de empleados) × 100.
Data primarios	• Número de empleados que reciben un número de mensajes spam mayor que el definido por la organización en un determinado intervalo de tiempo. • Número de empleados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia y aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-22 – Indicador 22: Programa de sensibilización de la organización (mejor más grande)

Campo	Datos
ID del indicador	Programa de sensibilización de la organización.
Objetivo	Los empleados deben seguir un programa de sensibilización.
Indicador	Porcentaje de empleados que participan en el programa de sensibilización.
Fórmula	(Número de empleados que participan en programas de sensibilización/Número total de empleados) × 100.
Data primarios	• Número de empleados que participan en programas de sensibilización. • Número de empleados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia y aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-23 – Indicador 23: Formación y educación en materia de seguridad (a nivel de programa, mejor más grande)

Campo	Datos
ID del indicador	Formación y educación en materia de seguridad.
Objetivo	Los empleados de la organización deberían recibir formación y educación en materia de seguridad para responder adecuadamente a los incidentes de seguridad.
Indicador	Porcentaje de empleados que han recibido formación y educación en materia de seguridad en un intervalo de tiempo definido por la organización.
Fórmula	(Número de empleados que han recibido formación y educación en materia de seguridad/Número total de empleados) × 100.
Data primarios	• Número de empleados que han recibido formación y educación en materia de seguridad. • Número de empleados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto/aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-24 – Indicador 24: Función y responsabilidad de la ciberseguridad (a nivel de programa, mejor más grande)

Campo	Datos
ID del indicador	Función y responsabilidad.
Objetivo	La organización debería contratar y organizar un equipo de respuesta a incidentes de ciberseguridad.
Indicador	Porcentaje del personal encargado de la seguridad de la información.
Fórmula	(Número de empleados encargados de la ciberseguridad/Número total de empleados de TI) × 100.
Data primarios	• Número de empleados encargados de la ciberseguridad. • Número total de empleados de TI.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto/aplicación.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-25 – Indicador 25: Infección por malware (a nivel de sistema/programa, mejor más pequeño)

Campo	Datos
ID del indicador	Dispositivos de punto extremo infectados por malware.
Objetivo	Los dispositivos de punto extremo de los empleados deberían protegerse contra diversos tipos de malware.
Indicador	Porcentaje de computadores infectados por virus o malware o atacados mediante tecnologías de pirateo.
Fórmula	(Número total de dispositivos de punto extremo infectados por malware/Número total de dispositivos de punto extremo) × 100.
Data primarios	• Número de dispositivos de punto extremo infectados por virus o malware o atacados mediante tecnologías de pirateo. • Número total de dispositivos de punto extremo en la organización.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto y eficacia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-26 – Indicador 26: Filtración de información de identificación personal (a nivel de programa)

Campo	Datos
ID del indicador	Filtración de información de identificación personal.
Objetivo	La organización debería proteger la información de identificación personal para que no haya filtraciones a otras organizaciones.
Indicador	Porcentaje de unidades de información de identificación personal que se ha filtrado durante un periodo de tiempo determinado en el incidente de PII en cuestión.
Fórmula	(Número de unidades de información de identificación personal que se ha filtrado durante un periodo de tiempo especificado por la organización en el incidente de PII en cuestión/Número total de unidades de información de identificación personal) × 100.
Data primarios	• Número de unidades de información de identificación personal que se ha filtrado durante un periodo de tiempo especificado por la organización en el incidente de PII en cuestión. • Número total de unidades de información de identificación personal.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-27 – Indicador 27: Porcentaje del presupuesto de TIC destinado a seguridad (a nivel de programa)

Campo	Datos
ID del indicador	Porcentaje del presupuesto de TIC destinado a seguridad de la información.
Objetivo	La organización debería disponer de un presupuesto para ciberseguridad.
Indicador	Porcentaje del presupuesto de TIC destinado a seguridad de la información; se supone que el presupuesto de seguridad forma parte del presupuesto de TI.
Fórmula	(Presupuesto de ciberseguridad/Presupuesto total de TIC) × 100.
Data primarios	• Presupuesto destinado a ciberseguridad. • Presupuesto total destinado a TIC.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-28 – Indicador 28: Tasa de dispositivos autorizados (mejor más grande)

Campo	Datos
ID del indicador	Tasa de dispositivos autorizados de la organización con respecto a todos los dispositivos.
Objetivo	La organización debe rastrear/controlar/prevenir/corregir el acceso a la red por parte de los dispositivos (computadores, componentes de red, impresoras, todo dispositivo con dirección IP) de acuerdo con el inventario de los dispositivos autorizados a conectarse a la red.
Indicador	Tasa de dispositivos autorizados de la organización con respecto a todos los dispositivos.
Fórmula	(Número de dispositivos autorizados/número de dispositivos) × 100.
Data primarios	• Número de dispositivos autorizados. • Número de dispositivos.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro 8-29 – Indicador 29: Tasa de software autorizado (mejor más grande)

Campo	Datos
ID del indicador	Tasa de activos de software autorizados de la organización con respecto a todos los activos de software.
Objetivo	La organización debe rastrear/controlar/prevenir/ corregir la instalación y ejecución de software en los computadores de acuerdo con un inventario del software aprobado.
Indicador	Tasa de activos de software autorizados de la organización con respecto a todos los activos de software.
Fórmula	(número de activos de software autorizados/número total de activos de software) × 100.
Data primarios	• Número de activos de software autorizados. • Número total de activos de software.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	Recomendación UIT-T X.1528, Enumeración de plataforma común [b-UIT-T X.1528] e [ISO/CEI 19770-2], *Information technology – Software asset management* – Part 2 : *Software identification tag* [b-ISO/CEI 19770-2].

Cuadro 8-30 – Indicador 30: Seguridad del software de aplicación (mejor más grande)

Campo	Datos
ID del indicador	Tasa de software de aplicación de la organización protegido contra los principales ataques de software de aplicación (por ejemplo CWE top25) con respecto a todos los activos de software de aplicación.
Objetivo	La organización debe detectar y bloquear los ataques al software de aplicación y generar una alerta o enviar un correo-e al personal administrativo de la empresa en menos de 24 horas después de la detección y el bloqueo.
Indicador	Tasa de software de aplicación de la organización protegido contra los principales ataques de software de aplicación con respecto a todos los activos de software de aplicación.
Fórmula	(Número de software de aplicación protegido contra los principales ataques de software de aplicación/número de todos los activos de software de aplicación) × 100.
Data primarios	• Número de software de aplicación protegido contra los principales ataques de software de aplicación. • Número de todos los activos de software de aplicación.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Impacto.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	Recomendación UIT-T X.1524, Lista de puntos débiles comunes [b-UIT-T X.1524] y Recomendación UIT-T X.1544, Enumeración y clasificación de pautas de ataques comunes [b-UIT-T X.1544].

Apéndice I

Ejemplos de indicadores de medidas de riesgo de seguridad de la información y de métricas

(Este apéndice no forma parte integrante de la presente Recomendación)

En este apéndice se dan dos ejemplos de indicadores de medidas de riesgo de seguridad de la información y de métricas que podrían utilizarse al calcular un indicador de ciberseguridad.

[b-NIST SP 800-55] facilita posibles medidas de riesgo a nivel de sistema y a nivel de programa que pueden agruparse de la siguiente forma:

- Medidas de riesgo a nivel de sistema:
  - control de acceso
  - auditoría y rendición de cuentas
  - identificación y autenticación
  - mantenimiento
  - evaluación de riesgos.
- Medidas de riesgo a nivel de programa:
  - gastos en concepto de seguridad, gestión de la vulnerabilidad
  - sensibilización y formación
  - certificación, acreditación y evaluaciones de seguridad
  - gestión de la configuración
  - planificación de contingencias
  - entorno físico.
- Medidas de riesgo a nivel de programa y a nivel de sistema:
  - respuesta a incidentes
  - protección de medios
  - planificación
  - seguridad personal
  - adquisición de sistemas y comunicaciones
  - integridad de los sistemas y de la información.

Asimismo, [b-NRI] del Foro Económico Mundial (WEF) facilita varios indicadores y [b-WEF] utiliza un certificado de capa de conexión segura (*SSL, secure socket layer*) o certificado de seguridad en la capa de transporte (*TLS, transport layer security*) propios del proveedor.

Apéndice II

Clasificación de los indicadores según su naturaleza

(Este apéndice no forma parte integrante de la presente Recomendación)

A fin de que la presente Recomendación reciba una mayor aceptación entre las organizaciones, sería útil determinar las mediciones mínimas que pueden obtenerse y utilizarse sin incurrir en grandes costes.

Por ejemplo, se puede comenzar fácilmente con el indicador 24 (función y responsabilidad de la ciberseguridad) de la cláusula 8, dado que consiste solamente en contar el número de efectivos. En cambio, para medir otros indicadores se necesitan herramientas y/o bases de datos. Por ejemplo, en el caso del indicador 1 (gestión de vulnerabilidades), es necesario contar con herramientas y bases de datos correspondientes para gestionar las vulnerabilidades. De esa forma, las organizaciones que deseen utilizar ese indicador deben considerar qué ventajas aporta realizar una inversión para disponer de esa información teniendo en cuenta el costo que representa hacerla. Análogamente, el indicador 2 requiere que ya se aplique una función de gestión de recursos de TIC en la organización. Para medir otros tipos de indicadores se requieren ciertas capacidades dentro de la organización. Por ejemplo, para medir el indicador 4 (tiempo medio para mitigar vulnerabilidades) es necesario conocer la fecha en que se producen, lo que resulta difícil sin capacidades de auditoría y análisis.

En el presente apéndice se describe una clasificación de indicadores en función de su naturaleza, a saber: los que son fáciles de medir, los que requieren herramientas y/o bases de datos que normalmente existen en una organización y los que se miden si la organización decide aplicar capacidades de medición mejoradas.

Cuadro II-1 – Clasificación de indicadores en función de su naturaleza

Naturaleza	Número de indicador	ID del indicador
Fáciles de medir	Indicador 12: Compromiso en materia de seguridad	Compromiso o código de conducta en materia de seguridad
	Indicador 16: Seguridad personal	Control de seguridad personal
	Indicador 24: Función y responsabilidad de la ciberseguridad	Función y responsabilidad de la ciberseguridad
	Indicador 27: Porcentaje del presupuesto de TIC dedicado a seguridad	Porcentaje del presupuesto de TIC de la organización destinado a seguridad de la información

Cuadro II-1 – Clasificación de indicadores en función de su naturaleza

Naturaleza	Número de indicador	ID del indicador
Se necesitan herramientas de medición y/o bases de datos que normalmente existen en una organización	Indicador 1: Gestión de vulnerabilidades	Porcentaje de grandes vulnerabilidades mitigadas
	Indicador 2: Mantenimiento de registro de inspección	Porcentaje de dispositivos de punto extremo para los que se mantiene un registro de inspección
	Indicador 3: Respuesta a incidentes	Respuesta a incidentes
	Indicador 8: Cobertura del análisis de riesgos	Cobertura del análisis de riesgos
	Indicador 9: Cobertura del programa de detección y tratamiento de malware	Cobertura del programa de detección y tratamiento de malware
	Indicador 21: Tasa de spam recibido	Tasa de spam recibido
	Indicador 22: Programa de sensibilización de la organización	Programa de sensibilización de la organización
	Indicador 23: Formación y educación en materia de seguridad	Formación y educación en materia de seguridad
	Indicador 28: Tasa de dispositivos autorizados	Tasa de dispositivos autorizados de una organización en relación con el total de dispositivos
	Indicador 29: Tasa de software autorizado	Tasa de recursos de software autorizados de una organización en relación con el total de recursos de software
	Indicador 30: Seguridad del software de aplicación	Tasa de software de aplicación de una organización que están protegidos de los principales ataques a nivel de la aplicación (por ejemplo, CWE top 25) en relación con todos los recursos de software de aplicación.

Cuadro II-1 – Clasificación de indicadores en función de su naturaleza

Naturaleza	Número de indicador	ID del indicador
Se requieren probablemente capacidades de medición más avanzadas dentro de la organización	Indicador 4: Tiempo medio para mitigar vulnerabilidades	Tiempo medio para mitigar vulnerabilidades
	Indicador 5: Instalación de programa de parches de seguridad	Programa de parches de seguridad
	Indicador 6: Tiempo medio de instalación de un parche	Tiempo medio de instalación de un parche
	Indicador 7: Tiempo medio para modificar la configuración	Tiempo medio para modificar la configuración
	Indicador 10: Cobertura del plan de contingencias	Cobertura del plan de contingencias
	Indicador 11: Evaluación de la seguridad	Porcentaje de sistemas de información con evaluación positiva de la seguridad
	Indicador 13: Control del acceso a distancia mediante pasarelas de seguridad	Puntos de acceso a distancia protegidos
	Indicador 14: Control de acceso a distancia con función de seguridad para la prevención de intrusiones o la detección de intrusiones	Puntos de acceso a distancia protegidos
	Indicador 15: Control del acceso inalámbrico	Puntos de acceso inalámbrico protegidos
	Indicador 17: Protección de la información de identificación personal (PII)	Porcentaje de información de identificación personal protegida
	Indicador 18: Protección de las copias de seguridad de los datos	Tasa de copias de seguridad de los datos cuya integridad se ha inspeccionado
	Indicador 19: Cobertura del sistema certificado de gestión de la seguridad	Cobertura del sistema de gestión
	Indicador 20: Instalación de un servidor seguro	Instalación de un servidor seguro
	Indicador 25: Infección por malware	Dispositivos de punto extremo infectados por malware
	Indicador 26: Filtración de información de identificación personal	Filtración de información de identificación personal

Apéndice III

Indicadores experimentales

(Este apéndice no forma parte integrante de la presente Recomendación)

En este apéndice se describen numerosos indicadores experimentales (véanse los Cuadros III.1 a III.6) que podrían utilizar las organizaciones.

Cuadro III.1 – Indicador III-1: Tiempo medio para detectar incidentes (a nivel de sistema y de programa, mejor más pequeño)

Campo	Datos
ID del indicador	Tiempo medio para detectar incidentes.
Objetivo	La organización debe detectar incidentes en cuanto se produzcan y medir el tiempo medio que tarda en detectarlos con el fin de verificar su eficacia a la hora de detectar incidentes de seguridad. En general, cuanto más rápido se detecta un incidente, menores serán los daños que probablemente produzca.
Indicador	Tiempo medio, en horas, que transcurre entre que se produce y se detecta el incidente para un determinado conjunto de incidentes.
Fórmula	Suma (Hora de detección – Hora de poducción)/Número (de incidentes).
Data primarios	• Hora en que se detecta cada uno de los incidentes. • Número total de incidentes notificados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro III.2 – Indicador III-2: Redundancia de enlaces (a nivel de sistema, mejor más grande)

Campo	Datos
ID del indicador	Porcentaje de enlaces de red con redundancia.
Objetivo	La organización debería construir un enlace redundante con la red principal para garantizar la disponibilidad y continuidad de los servicios de la organización.
Indicador	Porcentaje de enlaces de red con redundancia.
Fórmula	(Número de enlaces con redundancia/Número total de enlaces de red) × 100.
Data primarios	• Número de enlaces con redundancia para encaminadores, sistema de nombres de dominio (DNS), protocolo de configuración dinámica del anfitrión (DHCP), cortafuegos o bases de datos (DB). • Número de enlaces sin redundancia.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro III.3 – Indicador III-3: Infección por bot (a nivel de sistema, mejor más pequeño)

Campo	Datos
ID del indicador	Porcentaje de dispositivos de usuario infectados por bot.
Objetivo	La organización debería reducir la presencia de bots en su red.
Indicador	Porcentaje de dispositivos de usuario en la organización infectados por bots conocidos. Se parte del supuesto de que la organización utiliza sistema de detección de infecciones por bot.
Fórmula	(Número total de dispositivos de usuario infectados con bots conocidos/Número total de dispositivos de usuario) × 100.
Data primarios	• Número de dispositivos de usuario infectados con bots.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro III.4 – Indicador III-4: Medidas contra ataques por denegación del servicio distribuido (a nivel de sistema, mejor más pequeño)

Campo	Datos
ID del indicador	Medidas contra de DDoS.
Objetivo	La organización debe proteger sus sistemas de información contra ataques DDoS (o de denegación del servicio (DoS)).
Indicador	Porcentaje de sistemas de la organización que han quedado indisponibles durante un periodo de tiempo determinado debido a ataques DDoS (DoS).
Fórmula	(Número de sistemas de la organización que han quedado indisponibles durante un periodo de tiempo determinado debido a ataques DDoS (DoS) en un intervalo de tiempo especificado por la organización/Número total de sitios web de la organización) × 100.
Data primarios	• Número de sitios web que han quedado indisponibles durante un periodo de tiempo determinado debido a ataques DDoS (DoS) en un intervalo de tiempo especificado por la organización. • Número total de sitios web
Frecuencia	Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro III.5 – Indicador III-5: Rendimiento del registro de inspección (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Porcentaje de incidentes de seguridad informática de los que queda constancia visible en un registro de inspección.
Objetivo	La organización debe evaluar la eficacia de los registros de inspección.
Indicador	Porcentaje de incidentes de seguridad informática de los que queda constancia visible en un registro de inspección.
Fórmula	(Incidentes constatados que han dejado rastros visibles en los registros/Número total de incidentes constatados) × 100.
Data primarios	• Número de incidentes constatados cuyos rastros visibles se han encontrado en los registros de inspección. (registros centralizados o registros agrupados de los puntos extremos). • Número total de incidentes constatados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Cuadro III.6 – Indicador III-6: Rendimiento de la mitigación de incidentes (a nivel de sistema/programa, mejor más grande)

Campo	Datos
ID del indicador	Porcentaje de incidentes de seguridad informática ocurridos en los sistemas C&A (puntos extremos o grupos de puntos extremos).
Objetivo	La organización debe evaluar la eficacia de los procedimientos C&A.
Indicador	Porcentaje de incidentes de seguridad informática ocurridos en los sistemas C&A.
Fórmula	(Incidentes constatados ocurridos en los sistemas C&A/Número total de incidentes constatados) × 100.
Data primarios	• Número de incidentes constatados ocurridos en los sistemas C&A. • Número total de incidentes constatados.
Frecuencia	• Semanal, mensual, trimestral, anual.
Tipo	• Eficacia/eficiencia.
Nivel de exigencia	
Aplicable a	Organizaciones (a una comunidad por agregación).
Referencia de técnicas CYBEX	

Bibliografía

[b-ITU-T E.409] Recomendación UIT-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.800] Recomendación UIT-T X.800 (1991) | ISO/IEC 7498-2 (1989), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recomendación UIT-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1205] Recomendación UIT-T X.1205 (2008), *Overview of cybersecurity*.

[b-ITU-T X.1206] Recomendación UIT-T X.1206 (2008), *A vendor-neutral framework for automatic notification of security related information and dissemination of updates*.

[b-ITU-T X.1242] Recomendación UIT-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules*.

[b-ITU-T X.1252] Recomendación UIT-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1500] Recomendación UIT-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[b-ITU-T X.1520] Recomendación UIT-T X.1520 (2011), *Vulnerabilidades y riesgos corrientes (CVE).*

[b-ITU-T X.1521] Recomendación UIT-T X.1521 (2011), *Sistema común de puntuación de vulnerabilidades*.

[b-ITU-T X.1524] Recomendación UIT-T X.1524 (2012), *Lista de puntos débiles comunes*.

[b-ITU-T X.1528] Recomendación UIT-T X.1528 (2012), *Enumeración de plataforma común*.

[b-ITU-T X.1544] Recomendación UIT-T X.1544 (2013), *Enumeración y clasificación de pautas de ataques comunes*.

[b-ITU-T X-Sup.8] Suplemento 8 (2010) a las Recomendaciones UIT-T de la serie X, ITU-T X.1205 − *Supplement on best practices against botnet threats*.

[b-ISO/IEC 19770-2] ISO/IEC 19770-2:2009, *Information technology – Software asset management – Part 2: Software identification tag*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27003] ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management system implementation guidance*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27033-2] ISO/IEC 27033-2:2012, *Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security*.

[b-ISO/IEC 27033-4] ISO/IEC 27033-4: 2014, *Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways*.

[b-NIST SP 800-27] NIST SP 800-27 Revision A (2004), *Engineering Principles for IT Security (A Baseline for Achieving Security), Revision A.*

[b-NIST SP 800-30] NIST SP 800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST SP 800-53] NIST SP 800-53 Revision 4 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-NIST SP 800-55] NIST SP 800-55 Revision 1 (2008), *Performance Measurement Guide for Information Security*.

[b-NIST FIPS 199] NIST FIPS PUB 199 (2004), *Standards for Security Categorization of Federal Information and Information Systems*.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report*.

[b-NRI] World Economic Forum (2013), *Networked Readiness Index*.

[b-WEF] World Economic Forum (2013), *Secure Internet servers*. (Sources: The World Bank, World Development Indicators Online; national sources).

[b-CIS] Center for Internet Security (2010), *The CIS security metrics*.

[b-Nelson] Nelson, C. E. (2010), *Security metrics: An overview,* ISSA Journal, Vol.8, No. 8.

[b-BSA] BSA (2013), *BSA Global Cloud Computing Scorecard*. http://cloudscorecard.bsa.org/2013/.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2014