NORMA
CHILENA

NCh ISO 27032

Primera edición
2015.10.20
Corregida y reimpresa en 2019

Tecnología de la información — Técnicas de seguridad — Directrices para la ciberseguridad

Information technology — Security techniques — Guidelines for cybersecurity

ICS 35.040

INSTITUTO NACIONAL DE NORMALIZACION

Número de referencia
NCh-ISO 27032:2015
66 páginas

DOCUMENTO PROTEGIDO POR COPYRIGHT

Instituto Nacional de Normalización - INN

Av. Libertador Bernardo O'Higgins 1449, Santiago Downton Torre 7, piso 18 • Santiago de Chile

Tel. + 56 2 2445 88 00

Correo Electrónico info@inn.cl

Sitio Web www.inn.cl

Publicado en Chile

© ISO 2012 - Todos los derechos reservados
© INN 2015 - Para la adopción nacional

Contenido

Página

Preámbulo

El Instituto Nacional de Normalización, INN, es el organismo que tiene a su cargo el estudio y preparación de las normas técnicas a nivel nacional. Es miembro de la INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) y de la COMISION PANAMERICANA DE NORMAS TECNICAS (COPANT), representando a Chile ante esos organismos.

Esta norma se estudió a través del Comité Técnico CL013 *Tecnologías de la información*, con el propósito de proporcionar una visión general en relación a la ciberseguridad, amenazas, mecanismos de ataques, tratamiento de riesgos y medidas para evitar posibles ataques.

Esta norma es idéntica a la versión en inglés de la Norma Internacional ISO/IEC 27032:2012 *Information technology - Security techniques - Guidelines for cybersecurity.*

Para los propósitos de esta norma, se han realizado los cambios editoriales que se indican y justifican en Anexo E.

La Nota Explicativa incluida en un recuadro en cláusula 2 Referencias normativas y en Anexo D, Bibliografía, es un cambio editorial que se incluye con el propósito de informar la correspondencia con Norma Chilena de las Normas Internacionales citadas en esta norma.

Los Anexos A, B, C, D y E no forman parte de la norma, se insertan sólo a título informativo.

Esta norma ha sido aprobada por el Consejo del Instituto Nacional de Normalización, en sesión efectuada el 20 de octubre de 2015.

Esta norma ha sido corregida y reimpresa en 2019, modificándose las cláusulas que se indican a continuación:

Título;

Preámbulo;

0;

1;

2.2;

4.19;

4.19, Nota 2;

4.20;

4.20, Nota 2;

4.31;

4.32;

6.1;

6.2;

6.3;

Figura 1;

6.4.1;

6.4.2;

Figura 2, Título;

6.4.2;

6.5;

7.3;

8.3;

9;

9.1.2;

9.1.3;

10;

10.1;

10.2.1;

10.2.2;

10.2.3;

10.3;

11.1;

11.1, c);

11.2;

11.3;

11.4.1;

11.4.2.1, Nota 1;

11.4.2.4;

11.4.2.5;

12;

12.1;

12.4, g;

12.5.1;

12.5.2;

12.5.3.2;

15.5.5, c);

12.6;

13.1;

13.1, Nota;

13.2.1;

13.3.1;

13.3.3;

13.4.1;

13.4.4;

13.5.1;

13.5.2;

13.5.5;

13.6;

Anexo A, Título;

A.1;

B.1;

C.1;

Tabla C.13, Título;

Tabla C.17, Título.

Si bien se ha tomado todo el cuidado razonable en la preparación y revisión de los documentos normativos producto de la presente comercialización, INN no garantiza que el contenido del documento es actualizado o exacto o que el documento será adecuado para los fines esperados por el Cliente.

En la medida permitida por la legislación aplicable, el INN no es responsable de ningún daño directo, indirecto, punitivo, incidental, especial, consecuencial o cualquier daño que surja o esté conectado con el uso o el uso indebido de este documento.

Introducción

El Ciberespacio es un entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet, con el apoyo de dispositivos físicos y comunicaciones de tecnología de información (ICT, según sigla en inglés) y redes distribuidas mundialmente.

Sin embargo, hay asuntos de seguridad que no son cubiertos por las buenas prácticas actuales de protección de la información, protección de Internet, protección de red y protección de TIC, puesto que existen brechas entre estos dominios así como una falta de comunicación entre las organizaciones y los proveedores en el Ciberespacio. Esto se debe a que los dispositivos y redes conectadas que han soportado el Ciberespacio tienen múltiples dueños, cada uno con sus propias preocupaciones de negocio, operacionales y normativas. Los diferentes focos establecidos por cada organización y proveedor en el Ciberespacio en los dominios de protección relevantes, donde se toma muy poco en cuenta, o no en lo absoluto, las contribuciones que pueden hacer otras organizaciones o proveedores, ha resultado en un estado fragmentado de la protección para el Ciberespacio.

Así, la primera área de foco de esta norma es abordar los temas de la protección del Ciberespacio o Ciberseguridad, los que se concentran en superar las brechas entre los diferentes dominios de protección en el Ciberespacio. En particular, esta norma provee una guía técnica para abordar los riesgos comunes de Ciberseguridad, incluyendo:

— ataques de ingeniería social;

— hackeos;

— la proliferación de software malignos (“malwares”);

— spyware; y

— otro software potencialmente no deseado.

La guía técnica provee controles para abordar estos riesgos, incluyendo controles para:

— prepararse para ataques de, por ejemplo, malwares, malhechores individuales u organizaciones criminales en Internet;

— detectar y monitorear ataques; y

— responder a los ataques.

La segunda área de foco de esta norma es la colaboración, ya que hay una necesidad de compartir y coordinar información de manera eficiente y efectiva y de manejar los incidentes que ocurren entre los actores en el Ciberespacio. Esta colaboración se debe llevar a cabo de manera segura y confiable para que además proteja la privacidad de los individuos involucrados. Muchos de estos actores pueden habitar en diferentes ubicaciones geográficas y zonas horarias y es probable que sigan requisitos normativos diferentes. Los actores incluyen:

— consumidores, los que pueden incluir varios tipos de organizaciones o individuos; y

— proveedores, incluyendo a los proveedores de servicios.

Por consiguiente, esta norma también provee un marco para:

— compartir información;

— coordinación; y

— manejar incidentes.

Este marco incluye:

— elementos clave de consideración para establecer confianza;

— procesos necesarios para la colaboración y para compartir e intercambiar información; así como

— requisitos técnicos para la integración e interoperabilidad de los sistemas entre los diferentes actores.

Dado el alcance de esta norma, los controles proporcionados son necesarios en un nivel alto. En esta norma, se referencian normas de especificación técnica y directrices aplicables detalladas para cada área, para futuras orientaciones.

Tecnología de la información — Técnicas de seguridad — Directrices para la ciberseguridad

1 Alcance y campo de aplicación

Esta norma proporciona una guía para mejorar el estado de la Ciberseguridad, resalta los aspectos importantes de esa actividad y sus dependencias en otros dominios de protección, en particular:

— protección de la información;

— protección de red;

— protección de Internet; y

— protección de la infraestructura de información crítica[1].

Esta norma abarca las prácticas de protección de línea base para las partes interesadas en el Ciberespacio. Esta norma proporciona:

— una visión general de la Ciberseguridad,

— una explicación de la relación entre la Ciberseguridad y otros tipos de protección,

— una definición de las partes interesadas y una descripción de sus roles en la Ciberseguridad,

— una orientación para abordar temas comunes de Ciberseguridad, y

— un marco de trabajo para permitir que las partes interesadas colaboren para resolver temas de Ciberseguridad.

2 Aplicabilidad

2.1 Audiencia

Esta norma se aplica a los proveedores de servicios en el Ciberespacio. La audiencia, sin embargo, incluye a los consumidores que usan estos servicios. Donde las organizaciones proporcionen servicios en el Ciberespacio para que las personas los usen en sus hogares o en otras organizaciones, estas pueden necesitar preparar una orientación basada en esta norma que contenga explicaciones o ejemplos adicionales que sean suficientes para permitir que los lectores entiendan y actúen de acuerdo a ella.

2.2 Limitaciones

Esta norma no aborda:

— la Ciberprotección;

— el Cibercrimen;

1 *En inglés: CIIP, Critical Information Infrastructure Protection.*

— CIIP;

— la protección de Internet; y

— crímenes relacionados a Internet.

Se reconoce que existen relaciones entre los dominios mencionados y la Ciberseguridad. Sin embargo, abordar estas relaciones y el intercambio de controles entre estos dominios va más allá del alcance de esta norma.

Es importante destacar que no se aborda el concepto de Cibercrimen, a pesar de estar mencionado. Esta norma no provee una orientación sobre los aspectos legales del Ciberespacio o sobre la regulación de la Ciberseguridad.

La guía en esta norma se limita al entendimiento del Ciberespacio en Internet, incluyendo los endpoints. Sin embargo, no se aborda la extensión del Ciberespacio a otras representaciones espaciales a través de plataformas y medios de comunicación, ni tampoco sus aspectos de protección física.

EJEMPLO 1 No se aborda la protección de los elementos de infraestructura, tales como los portadores de comunicación que soportan el Ciberespacio.

EJEMPLO 2 No se aborda la protección física de los teléfonos celulares que se conectan al Ciberespacio para descargar y/o manipular contenido.

EJEMPLO 3 No se abordan las funciones de mensajería de texto y chat de voz provistas por teléfonos celulares.

3 Referencias normativas

El documento siguiente es indispensable para la aplicación de esta norma. Para referencias con fecha, sólo se aplica la edición citada. Para referencias sin fecha se aplica la última edición del documento referenciado (incluyendo cualquier enmienda).

ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*.

NOTA EXPLICATIVA NACIONAL

La equivalencia de la Norma Internacional señalada anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma Internacional	Norma nacional	Grado de correspondencia
ISO/IEC 27000	NCh-ISO 27000:2014	La Norma Chilena NCh-ISO 27000:2014 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27000:2014.

4 Términos y definiciones

Para los propósitos de esta norma se aplican los términos y definiciones indicados en ISO/IEC 27000 y adicionalmente los siguientes:

4.1
adware
aplicación que fuerza al usuario a ver publicidad y/o registra el comportamiento online del usuario

NOTA La aplicación puede o no ser instalada con el conocimiento o consentimiento del usuario o forzada al usuario por medio de los términos de licencia para otro software.

4.2
aplicación
solución TI, incluyendo los software de aplicación, procedimientos y datos de aplicación, diseñada para ayudar a los usuarios de una organización a llevar a cabo tareas particulares o resolver tipos particulares de problemas TI al automatizar un proceso o función de negocio

[ISO/IEC 27034-1:2011]

4.3
proveedor de servicios de aplicación
operador que provee una solución de software hospedado y ofrece servicios de aplicación, incluye modelos de entrega basados en Web o cliente-servidor

EJEMPLO Los operadores de juegos online, proveedores de aplicaciones de oficina y proveedores de almacenamiento online.

4.4
servicios de aplicación
software con una funcionalidad entregada bajo demanda a los suscriptores a través de un modelo online que incluye aplicaciones basadas en Web o cliente-servidor

4.5
software de aplicación
software diseñado para ayudar a los usuarios a realizar tarea particulares o manejar tipos particulares de problemas, diferente de los softwares que controlan al computador

[ISO/IEC 18019]

4.6
activo
cualquier elemento que tenga valor para un individuo, una organización o un gobierno

NOTA Adaptado de ISO/IEC 27000 para establecer disposiciones para individuos y la separación de organizaciones y de gobiernos (ver 4.37).

4.7
avatar
representación de una persona que participa en el Ciberespacio

NOTA 1 Un avatar también se puede llamar el alter ego de una persona.

NOTA 2 Un avatar también se puede ver como un “objeto” que representa la personificación del usuario.

4.8
ataque
intento de destruir, exponer, alterar, inhabilitar, robar u obtener un acceso no autorizado para usar un activo de manera no autorizada

[ISO/IEC 27000:2009]

4.9
potencial de ataque
potencial percibido para el éxito de un ataque (si se debería lanzar un ataque) expresado en términos de la experiencia, recursos y motivación de un atacante

[ISO/IEC 15408-1:2005]

4.10
vector de ataque
camino o medios por los cuales un atacante puede obtener acceso a un servidor de computador o de red para entregar un resultado malicioso

4.11
ataque combinado
ataque que busca maximizar la severidad del daño y la velocidad de contagio al combinar múltiples métodos de ataque

4.12
bot, robot
programa de software automatizado usado para llevar a cabo tareas específicas

NOTA 1 Esta palabra se suele usar para describir programas, que trabajan usualmente en un servidor, que automatizan tareas tales como el reenvío y clasificación de correos electrónicos.

NOTA 2 Un bot se describe también como un programa que opera como un agente para un usuario u otro programa o que simula una actividad humana. En Internet, los bots más extendidos son los programas, también llamados arañas o rastreadores, que acceden a los sitios Web y recolectan su contenido para índices de motor de búsqueda.

4.13
botnet
software de control remoto, específicamente una colección de bots maliciosos, que corre de manera autónoma y automática en computadores comprometidos

4.14
cookie
<control de acceso> capacidad o autenticación en un sistema de control de acceso

4.15
cookie
<IPSec> intercambio de datos por el ISAKMP para prevenir ciertos ataques de Denegación de Servicio durante el establecimiento de una asociación de seguridad

4.16
cookie
<HTTP> intercambio de datos entre un servidor HTTP y un navegador para almacenar información del lado del cliente y recuperarlo posteriormente para uso del servidor

NOTA Un navegador Web puede ser un cliente o un servidor.

4.17
control, contramedida
medios para manejar riesgos, incluyendo políticas, directrices, directrices, prácticas o estructuras organizacionales, las que pueden ser de naturaleza administrativa, técnica, de gestión o legales

[ISO/IEC 27000:2009]

NOTA La Guía ISO 73:2009 define control simplemente como una medida para modificar riesgos.

4.18
Cibercrimen
actividad criminal que implica que los servicios o aplicaciones en el Ciberespacio se utilicen o sean blanco de un crimen, lo que significa que el Ciberespacio es la fuente, herramienta, blanco o lugar de un crimen

4.19
Ciberprotección
condición de estar protegido en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el Ciberespacio que se pueda considerar no deseable

NOTA 1 Esta puede tomar la forma de estar protegido del evento o de la exposición a algo que cause pérdidas económicas o de salud. Puede incluir la protección de personas o de activos.

NOTA 2 La protección en general también se define como el estado de estar convencido de que los efectos adversos no van a ser causados por algún agente bajo condiciones definidas.

4.20
Ciberprotección
seguridad del Ciberespacio
conservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio

NOTA 1 Además, otras propiedades pueden estar involucradas, como la autenticidad, la contabilidad, el no repudio y la confiabilidad.

NOTA 2 Adaptada de la definición de seguridad de la información descrita en ISO/IEC 27000:2009.

4.21
el Ciberespacio
entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física

4.22
servicios de aplicación de Ciberespacio
servicios de aplicación (ver 4.4) provistos en el Ciberespacio

4.23
Ciberocupa
individuos u organizaciones que registran y se aferran a URLs que se parecen a referencias o nombres de otras organizaciones en el mundo real o en el Ciberespacio

4.24
software engañoso
software que realiza actividades en el computador de un usuario sin antes notificar al usuario de lo que va a hacer exactamente en el computador o sin pedir el consentimiento del usuario para llevar a cabo estas acciones

EJEMPLO 1 Un programa que roba las configuraciones de un usuario.

EJEMPLO 2 Un programa que causa la aparición de publicidad en ventanas emergentes que un usuario no puede detener fácilmente.

EJEMPLO 3 Adware y spyware.

4.25
hackeo
acceder intencionalmente al sistema de un computador sin la autorización del usuario o dueño

4.26
hacktivismo
hackear por motivos políticos o sociales

4.27
activo de información
conocimiento o datos que tienen un valor para un individuo u organización

NOTA Adaptado de ISO/IEC 27000:2009.

4.28
Internet, interredes
grupo de redes interconectadas

NOTA 1 Adaptada de ISO/IEC 27033-1:2009

NOTA 2 En este contexto, se haría referencia a “una Internet”. Hay una diferencia entre la definición de “una Internet” y “el Internet”.

4.29
el Internet
sistema global de redes interconectadas en el dominio público

[ISO/IEC 27033-1:2009]

NOTA Hay una diferencia entre la definición de “una Internet” y “el Internet”.

4.30
crimen de Internet
actividad criminal que implica que los servicios o aplicaciones en Internet se utilizan o son blanco de un crimen, lo que significa que Internet es la fuente, herramienta, blanco o lugar de un crimen

4.31
protección de Internet
condición de estar protegido en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en Internet que se pueda considerar no deseable

4.32
seguridad de Internet
conservación de la confidencialidad, integridad y disponibilidad de la información en Internet

4.33
servicios de Internet
servicios entregados a un usuario para habilitar el acceso a Internet por medio de una dirección IP asignada, la que normalmente incluye una autenticación, autorización y servicios de nombre de dominio

4.34
proveedor de servicios de Internet
organización que provee servicios de Internet a un usuario y habilita el acceso a Internet a sus clientes

NOTA También se suele llamar proveedor de acceso a Internet.

4.35
malware, software malicioso
software diseñado con un propósito malicioso que contiene características o capacidades que pueden potencialmente causar un perjuicio de manera directa o indirecta al usuario y/o al sistema computacional del usuario

EJEMPLOS Virus, gusanos, troyanos.

4.36
contenidos maliciosos
aplicaciones, documentos, archivos, datos u otros recursos que tienen características o capacidades maliciosas incrustadas, disfrazadas o escondidas en ellos

4.37
organización
grupo de personas e instalaciones con un acuerdo de responsabilidades, autoridades y relaciones

[ISO 9000:2005]

NOTA 1 En el contexto de esta norma se hace la diferencia entre individuo y organización.

NOTA 2 En general, un gobierno también es una organización. En el contexto de esta norma, los gobiernos se pueden considerar de manera separada de otras organizaciones para que haya claridad.

4.38
suplantación de identidad
proceso fraudulento para intentar adquirir información privada o confidencial al disfrazarse como una entidad de confianza en una comunicación electrónica

NOTA Una suplantación de identidad se puede llevar a cabo al usar la ingeniería social o un engaño técnico.

4.39
activo físico
activo que tiene una existencia tangible o material

NOTA Los activos físico se refieren normalmente a dinero, equipos, inventarios y propiedades que le pertenecen a un individuo u organización. Un software se considera un activo intangible o activo no físico.

4.40
software potencialmente no deseado
softwares engañosos, incluyendo los softwares maliciosos y no maliciosos, que exhiben características de un software engañoso

4.41
estafa
fraude o engaño

4.42
spam
abuso a los sistemas de mensajería electrónica llevados a cabo para mandar mensajes no solicitados de manera indiscriminada y en masa

NOTA Aunque la forma más ampliamente reconocida de spam es el spam por correo electrónico, el término se aplica a abusos similares en otros tipos de soportes: spam de mensajería instantánea, spam de grupos de noticias, spam de motores de búsqueda Web, spam en blogs, wiki spam, spam de mensajería de telefonía celular, spam en foros de Internet y transmisiones de fax basura.

4.43
spyware
software engañoso que recolecta información privada o confidencial desde un usuario de computador

NOTA Esta información puede incluir material como los sitios Web visitados más frecuentemente por un usuario o información más sensible como contraseñas.

4.44
parte interesada
<gestión de riesgos> persona u organización que puede afectar, verse afectado por o percibirse como afectados por una decisión o actividad

[Guía ISO 73:2009]

4.45
parte interesada
<sistema> individuo u organización que tenga un derecho, porción, reclamación o interés en un sistema o en su posesión de características que suplan sus necesidades y expectativas

[ISO/IEC 12207:2008]

4.46
amenaza
causa potencial de un incidente no deseado, que puede resultar en un perjuicio a un sistema, individuo u organización

NOTA Adaptado de ISO/IEC 27000:2009.

4.47
troyano, caballo troyano
malware que aparentemente realiza una función deseada

4.48
correo electrónico no solicitado
correo electrónico que no es bienvenido o no fue requerido o invitado

4.49
activo virtual
representación de un activo en el Ciberespacio

NOTA En este contexto, la moneda se puede definir tanto como un medio de intercambio o una propiedad que tiene un valor en un entorno específico, como un video juego o un ejercicio de simulación de intercambio financiero.

4.50
moneda virtual
activos virtuales monetarios

4.51
mundo virtual
entorno simulado al cual pueden acceder múltiples usuarios a través de una interfaz en línea

NOTA 1 Los entornos simulados suelen ser interactivos.

NOTA 2 El mundo físico en el que viven las personas, y sus características relacionadas, se llamará “mundo real” para diferenciarlo de un mundo virtual.

4.52
vulnerabilidad
debilidad de un activo o control que puede ser aprovechada por una amenaza

[ISO/IEC 27000:2009]

4.53
zombi, computador zombi, drone
computador que contiene un software escondido que permite controlar la máquina de manera remota, normalmente para atacar a otro computador

NOTA Generalmente, una máquina comprometida es sólo una de muchas en una botnet y se usará para llevar a cabo actividades maliciosas siguiendo órdenes remotas.

5 Términos abreviados

En esta norma se usarán los siguientes términos abreviados.

AS	Sistema Autónomo
AP	Punto de Acceso
CBT	Enseñanza Mediada por Computadora
CERT	Equipo de Respuesta ante Emergencias Informáticas
CIRT	Equipo de Respuesta ante Incidentes Informáticos
CSIRT	Equipo de Respuesta ante Incidencias de Seguridad Informática
CIIP	Protección de la Infraestructura de Información Crítica
DoS	Denegación de Servicio

DDoS	Denegación de Servicio Distribuido
HIDS	Sistema de detección de Intrusos en un Host
IAP	Proveedor de Aplicación Independiente
ICMP	Protocolo de Mensajes de Control de Internet
ICT	Tecnología de la Información y Comunicación
IDS	Sistema de Detección de Intrusos
IP	Protocolo de Internet
IPO	Organización Proveedora de Información
IPS	Sistema de Prevención de Intrusos
IRO	Organización Receptora de Información
ISP	Proveedor de Servicios de Internet
ISV	Vendedor Independiente de Software
IT	Tecnología de la Información
MMORPG	Videojuego de Rol Multijugador Masivo Online
NDA	Acuerdo de Confidencialidad
SDLC	Ciclo de Vida de Desarrollo de Sistemas
SSID	Identificador del Conjunto de Servicios
TCP	Protocolo de Control de Transmisión
UDP	Protocolo de Datagramas de Usuario
URI	Identificador de Recursos Uniforme
URL	Localizador de Recursos Uniforme

6 Visión general

6.1 Introducción

La seguridad en Internet y en el Ciberespacio ha sido un tema de creciente preocupación. Las partes interesadas han establecido su presencia en el Ciberespacio a través de sitios Web y ahora intentan aprovechar aún más el mundo virtual que provee el Ciberespacio.

EJEMPLO Un número en aumento de individuos pasa grandes cantidades de tiempo con sus avatares virtuales en los MMORPGs.

Mientras algunos individuos son cuidadosos al gestionar sus identidades online, la mayoría de las personas actualizan detalles de sus perfiles personales para compartirlos con otros. Los perfiles en muchos sitios, particularmente sitios de redes sociales y salas de chat, se pueden descargar y almacenados por terceros. Esto puede llevar a la creación de un expediente digital de datos personales que se puede abusar, divulgar por terceros o usado para la recolección de datos secundarios. Si bien la exactitud e integridad de estos datos es cuestionable, éstos crean links a los individuos y organizaciones que suelen no ser fáciles de borrar completamente. Estos desarrollos en los dominios de comunicación, entretenimiento, transporte, compras, financieros, de seguros y salud crean nuevos riesgos para los actores en el Ciberespacio. Así, estos riesgos se pueden asociar con la pérdida de la privacidad.

La convergencia de las tecnologías de la información y comunicación, la facilidad para entrar al Ciberespacio y el estrechamiento del espacio personal entre los individuos se están ganando la atención de malhechores individuales y de organizaciones criminales. Estas entidades están usando mecanismos existentes, como la suplantación de identidad, spams y spywares, así como nuevas técnicas de ataque en desarrollo para aprovecharse de cualquier debilidad que puedan descubrir en el Ciberespacio. En los últimos años los ataques a la seguridad en el Ciberespacio han evolucionado desde el hackeo, para obtener un reconocimiento personal, hasta el crimen organizado o Cibercrimen. Una diversidad de herramientas y procesos previamente observados en incidentes de Ciberseguridad aislados, se utilizan ahora en conjunto en ataques multicombinados, normalmente con objetivos maliciosos de amplio alcance. Estos objetivos varían desde ataques personales, robo de identidad, fraudes o robos financieros hasta el hacktivismo político. Algunos foros de especialistas que destacan algunos problemas de seguridad potenciales, han servido para exponer técnicas de ataque y oportunidades de crimen.

Las múltiples formas de transacciones de negocio que se llevan a cabo en el Ciberespacio se están volviendo el blanco de los sindicatos de Cibercrimen. Variando desde los servicios de negocio a negocio, negocio a consumidor y de consumidor a consumidor, los riesgos presentados son inherentemente complejos. Conceptos como qué constituye una transacción o un acuerdo dependen de la interpretación de la ley y de cómo cada parte en la relación gestiona su propia responsabilidad. A menudo no se aborda correctamente el tema del uso de los datos recolectados durante la transacción o relación. Esto puede eventualmente afectar la seguridad, como la fuga de información.

Los desafíos legales y técnicos planteados por estos problemas de Ciberseguridad son de naturaleza global y tienen un amplio alcance. Sólo se pueden abordar estos desafíos mediante el trabajo conjunto de las comunidades técnicas de seguridad de la información, las comunidades legales, las naciones y las comunidades de naciones de acuerdo a una estrategia coherente. Esta estrategia debería tomar en cuenta el rol de cada actor y las iniciativas existentes, dentro de un marco de cooperación internacional.

EJEMPLO Un ejemplo de desafío surge del hecho de que el Ciberespacio permite tener un anonimato virtual y disimulo de ataque, lo que provoca que se dificulte la detección. Esto hace que sea muy difícil para los individuos y organizaciones establecer confianzas y transacciones, así como para los órganos encargados se hace muy difícil hacer que se cumplan las políticas. Incluso si se determina la fuente del ataque, los asuntos legales transfronterizos evitan que haya un mayor progreso en cualquier investigación o repatriación legal.

El actual progreso para abordar estos desafíos ha sido obstaculizado por muchos problemas y los problemas de Ciberseguridad están aumentando y continúan evolucionando.

Si bien las amenazas de Ciberseguridad no son escasas y existen muchas formas para contrarrestarlas (si bien no están estandarizadas), esta norma se enfoca en los siguientes aspectos clave:

— ataques por software malicioso o potencialmente no deseados;

— ataques de ingeniería social; y

— coordinación e intercambio de información.

Además, algunas herramientas de Ciberseguridad se discutirán brevemente en esta norma. Estas herramientas y áreas se relacionan estrechamente con la prevención, detección, respuesta e investigación de Cibercrímenes. En Anexo A se describen más detalles.

6.2 La naturaleza del Ciberespacio

El Ciberespacio se puede describir como un entorno virtual que no existe en ninguna forma física, si no en un entorno o espacio complejo que resulta de la aparición del Internet más la presencia de personas, organizaciones y actividades en todo tipo de dispositivos y redes de tecnología que se encuentran conectados a él. La seguridad en el Ciberespacio o Ciberseguridad trata la seguridad de este mundo virtual.

Muchos mundos virtuales tienen una moneda virtual como las usadas para comprar objetos dentro de los juegos. Hay un valor real asociado a la moneda virtual, incluso en los objetos dentro de los juegos. Estos objetos virtuales se intercambian normalmente por dinero real en sitios de remates online y algunos juegos incluso tienen un canal oficial con tasas publicadas de intercambios de dinero real o virtual para la monetización de objetos virtuales. Generalmente son estos canales de monetización los que hacen que los mundos virtuales sean blancos de ataques, usualmente por medio de la suplantación de identidad u otras técnicas para robar información de una cuenta.

6.3 La naturaleza de la Ciberseguridad

Para que la utilidad del ciberespacio prevalezca, las partes interesadas en el Ciberespacio deben tener un rol activo, lo que significa ir más allá de proteger sus propios activos . Las aplicaciones dentro del Ciberespacio están sobrepasando los modelos de “negocio a consumidor” y de “consumidor a consumidor”, hacia una forma de “muchas a muchas” interacciones y transacciones. Los requisitos se están ampliando para preparar a individuos y organizaciones para enfrentar los riesgos y desafíos de seguridad emergentes, y así prevenir y responder de manera efectiva a los malos usos y explotaciones criminales.

La Ciberseguridad tiene relación con las acciones que los actores deberían realizar para establecer y mantener la seguridad en el Ciberespacio.

La Ciberseguridad depende de la seguridad de la información, seguridad de aplicaciones, seguridad de red y seguridad de Internet como bloques estructurales fundamentales. La Ciberseguridad es una de las actividades necesarias para la CIIP y, al mismo tiempo, una protección adecuada de servicios de infraestructura crítica contribuye a la necesidades de seguridad básicas (es decir, seguridad, confiabilidad y disponibilidad de la infraestructura crítica) para cumplir con las metas de Ciberseguridad.

Sin embargo, la Ciberseguridad no es sinónimo de seguridad de Internet, seguridad de red, seguridad de aplicaciones, seguridad de la información o CIIP. Esto tiene un alcance único que requiere que las partes interesadas tengan un papel activo para mantener, o mejorar, la utilidad y confianza del Ciberespacio. Esta norma diferencia el término Ciberseguridad y los otros dominios de seguridad como se describen a continuación:

— La seguridad de información se preocupa de la protección de la confidencialidad, integridad y disponibilidad de la información en general, para responder con las necesidades del usuario en cuanto a la información aplicable.

— La seguridad de aplicaciones es un proceso que se realiza para aplicar controles y medidas a las aplicaciones de una organización para gestionar los riesgos que pueden surgir de su uso. Los controles y medidas se pueden aplicar a la misma aplicación (sus procesos, componentes, software y resultados), a sus datos (datos de configuración, datos del usuario, datos de la organización) y a toda la tecnología, procesos y actores involucrados en el ciclo de vida de la aplicación.

— La seguridad de red se preocupa del diseño, implementación y operación de las redes para lograr los propósitos de seguridad de la información en las redes dentro de las organizaciones, entre organizaciones y entre las organizaciones y los usuarios.

— La seguridad de Internet se preocupa de proteger los servicios relacionados a Internet y los sistemas y redes relacionados a las TIC como una extensión de la seguridad de red en las organizaciones y hogares para lograr el propósito de seguridad. La seguridad de Internet también asegura la disponibilidad y confiabilidad de los servicios de Internet.

— CIIP se preocupa de proteger los sistemas proporcionados u operados por los proveedores de infraestructura crítica, tales como la energía, la telecomunicación y los departamentos de aguas. CIIP se asegura de que esos sistemas y redes estén protegidos y sean resistentes a los riesgos de seguridad de la información, los riesgos de seguridad de red, los riesgos de seguridad de Internet así como los riesgos de Ciberseguridad.

La Figura 1 resume la relación entre la Ciberseguridad y otros dominios de seguridad. La relación entre estos dominios de seguridad y la Ciberseguridad es compleja. Algunos de los servicios de infraestructura crítica, por ejemplo el agua y el transporte, necesitan evitar impactar el estado de la Ciberseguridad de manera directa o significativa. Sin embargo, la falta de Ciberseguridad puede tener un impacto negativo en la disponibilidad de los sistemas de infraestructura de información crítica provistos por los proveedores de infraestructura crítica.

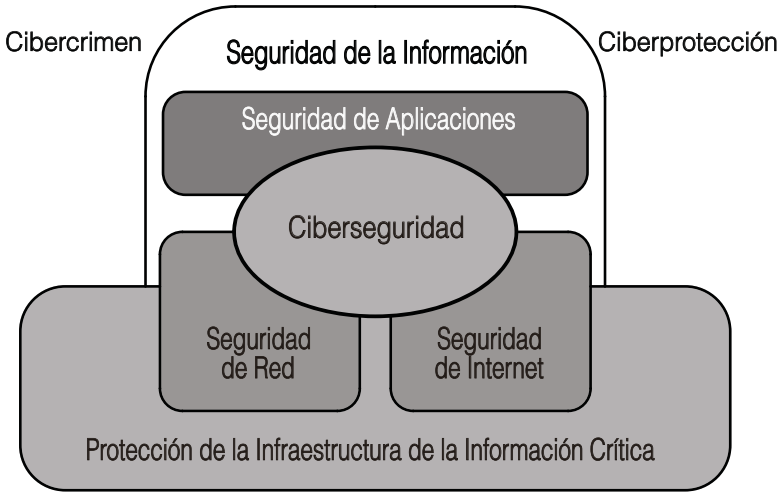

Figura 1 – Relación entre la Ciberseguridad y otros dominios de seguridad

Por otro lado, la disponibilidad y confiabilidad del Ciberespacio depende de muchas formas de la disponibilidad y confiablidad de los servicios de infraestructura crítica relacionados, tales como las infraestructuras de red de telecomunicaciones. La seguridad del Ciberespacio está también relacionada estrechamente con la seguridad de Internet, de las redes de negocio/hogar y con la seguridad de la información en general. Se debe destacar que los dominios de seguridad identificados en esta sección tienen sus propios objetivos y alcance de enfoque. Para enfrentarse a los problemas de Ciberseguridad se requieren comunicaciones y una coordinación sustanciales entre las diferentes

entidades privadas y públicas de diferentes países y organizaciones. Los servicios de infraestructura crítica son considerados como servicios relacionados con la seguridad nacional por algunos gobiernos y, por lo tanto, se podrían discutir o divulgar abiertamente. Es más, el conocimiento de las debilidades de la infraestructura crítica, si no se usa apropiadamente, puede tener una implicación directa en la seguridad nacional. Por esta razón es necesario contar con un marco básico para compartir información y coordinar los problemas o incidentes para superar las brechas y proveer una garantía adecuada a las partes interesadas en el Ciberespacio.

6.4 Modelo general

6.4.1 Introducción

Esta cláusula presenta un modelo general usado a lo largo de esta norma. Esta cláusula asume tener conocimiento sobre seguridad y no es el propósito actuar como un tutorial en esta área.

Esta norma analiza la seguridad usando un conjunto de conceptos y terminología de seguridad. Para usar esta norma de manera efectiva, es prerrequisito tener un entendimiento de estos conceptos y terminología. Sin embargo, los conceptos en sí mismos son bastante generales y no intenta limitar la clase de problemas de seguridad de TI a los que se podría aplicar esta norma.

6.4.2 Contexto de seguridad general

La seguridad se preocupa de proteger a los activos de las amenazas, categorizándolas como el abuso potencial de activos protegidos. Se deberían considerar las categorías de amenazas, pero en el dominio de la seguridad se da mayor atención a aquellas amenazas relacionadas a actividades maliciosas u otras actividades humanas. La Figura 2 ilustra estos conceptos y relaciones de alto nivel.

NOTA La Figura 2 se adaptó de ISO/IEC 15408-1:2005 *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model*.

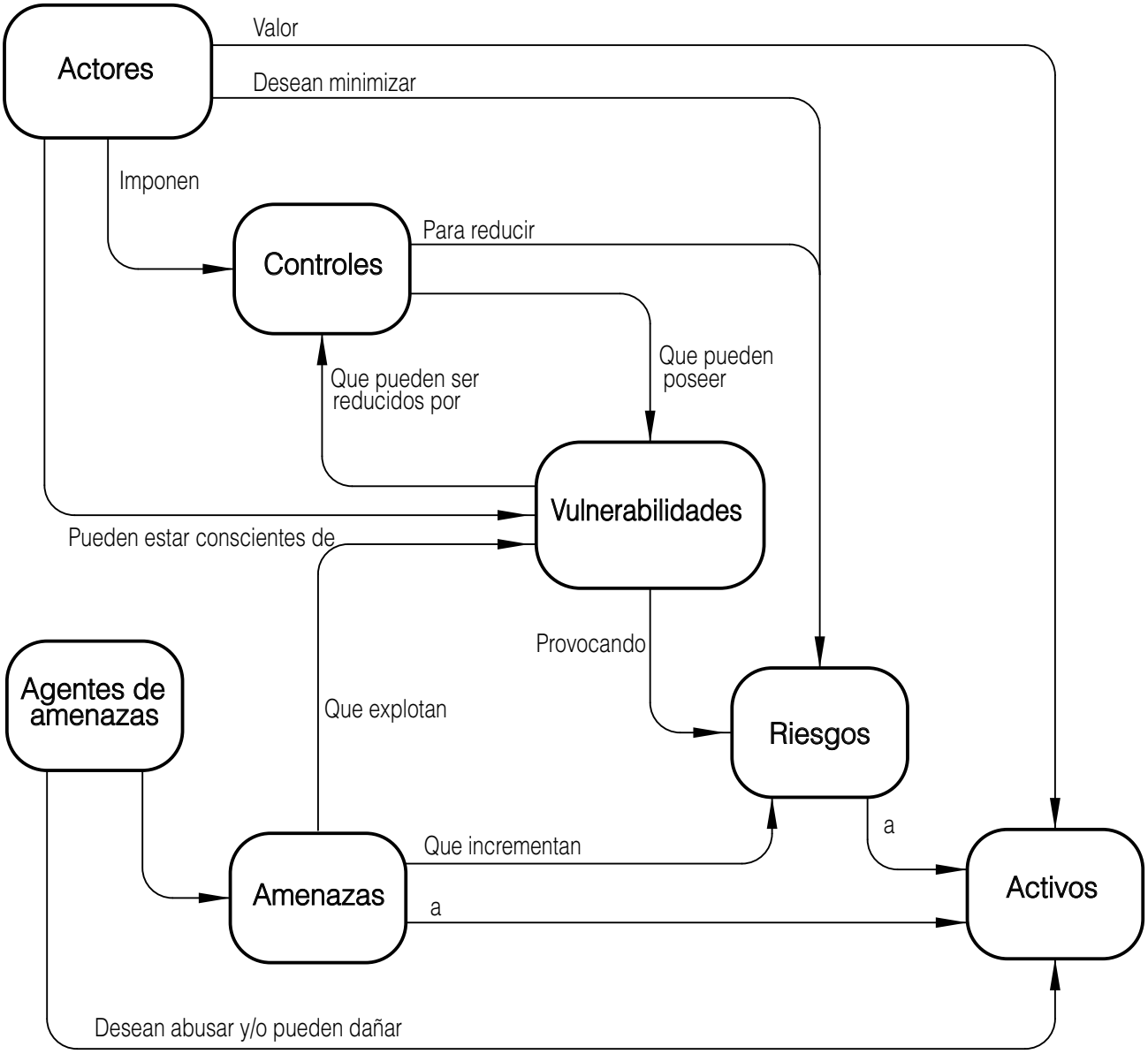

Figura 2 – Conceptos y relaciones de seguridad

El proteger los activos de interés es responsabilidad de las partes interesadas, quienes le dan valor a dichos activos. Los agentes de amenaza ya sean reales o supuestos, también pueden darle valor a los activos y tratar de abusar de éstos yendo en contra de los intereses de las partes interesadas. Las partes interesadas percibirán dichas amenazas como un potencial deterioro de los activos, que pueden reducir el valor de dichos activos para las partes interesadas. Los deterioros específicos de la seguridad generalmente incluyen, pero no se limitan a, la divulgación dañina de los activos a destinatarios no autorizados (pérdida de confidencialidad), daño a los activos a través de una modificación no autorizada (pérdida de integridad) o una privación no autorizada de acceso al activo (pérdida de disponibilidad).

Las partes interesadas evalúan los riesgos tomando en cuenta las amenazas que se aplican a sus activos. Este análisis puede ayudar en la selección de controles para contrarrestar los riesgos y reducirlos a un nivel aceptable.

Los controles se imponen para reducir las vulnerabilidades o impactos y para cumplir con los requisitos de seguridad de las partes interesadas (de manera directa e indirecta entregando órdenes a terceros). Pueden quedar vulnerabilidades residuales luego de imponer los controles. Aquellas vulnerabilidades se pueden explotar por agentes de amenaza, representando un nivel de riesgos residual para los activos. Las partes interesadas buscarán minimizar esos riesgos, en vista de otras restricciones .

Las partes interesadas necesitarán estar seguras de que los controles son los adecuados para contrarrestar las amenazas a los activos antes de permitir la exposición de éstos a las amenazas especificadas. Las partes interesadas pueden no tener por sí mismos la capacidad de juzgar todos los aspectos de los controles y, por lo tanto, pueden buscar una evaluación de los controles con la ayuda de organizaciones externas.

6.5 Enfoque

Una forma efectiva de enfrentar los riesgos de Ciberseguridad involucra una combinación de múltiples estrategias, teniendo en consideración a los varios actores. Estas estrategias incluyen:

— las buenas prácticas de la industria, en colaboración con todas las partes interesadas para identificar y abordar los problemas y riesgos de Ciberprotección;

— una amplia educación para los consumidores y empleados otorgando una fuente confiable de cómo identificar y abordar riesgos específicos de Ciberseguridad en la organización, así como en el Ciberespacio; y

— soluciones de tecnología innovadoras que ayuden a proteger a los consumidores de ataques conocidos de Ciberseguridad, para mantenerse actualizados y preparados ante nuevos abusos.

Esta directriz se enfoca en proveer buenas prácticas de la industria y una amplia educación para los consumidores y empleados para ayudar a los actores en el Ciberespacio a que tengan un rol activo para abordar los desafíos de Ciberseguridad. Esta incluye una guía para:

— los roles;

— las políticas;

— los métodos;

— los procesos; y

— los controles técnicos aplicables.

La Figura 3 proporciona una visión general de los puntos salientes en el enfoque adoptado en esta norma. Esta norma no pretende ser usada directamente para otorgar una amplia educación para los consumidores. A cambio, esta norma pretende ser usada por los proveedores de servicios en el Ciberespacio, así como por las organizaciones que otorgan una educación relacionada al Ciberespacio a los consumidores, para preparar materiales para una amplia educación al consumidor.

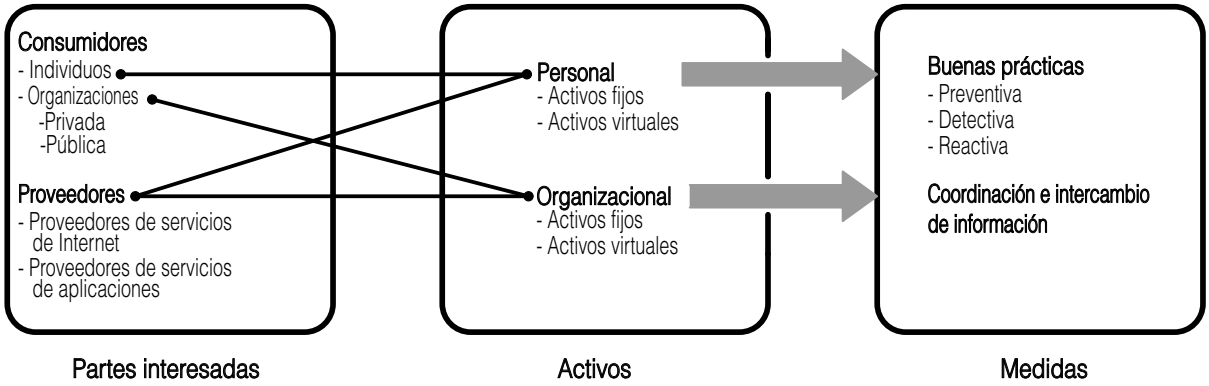

Figura 3 – Visión general del enfoque

7 Partes interesadas en el Ciberespacio

7.1 Visión general

El Ciberespacio no le pertenece a nadie, todos pueden participar y tienen intereses en él.

Para el propósito de esta norma, las partes interesadas en el Ciberespacio se categorizan en los grupos siguientes:

— consumidores, incluyendo:

  — individuos; y

  — organizaciones tanto privadas como públicas;

— proveedores, incluyendo, pero no limitados a:

  — proveedores de servicios de Internet; y

  — proveedores se servicios de aplicaciones.

7.2 Consumidores

Como se describe en Figura 3, los consumidores se refieren a los usuarios individuales y a las organizaciones tanto públicas como privadas. Las organizaciones privadas incluyen a las pequeñas y medianas empresas (PyMEs) así como a las grandes empresas. Se hace referencia de manera colectiva al gobierno y a otras agencias públicas, como organizaciones públicas. Un individuo o una organización se vuelve un consumidor cuando accede al Ciberespacio o a cualquier servicio disponible en el Ciberespacio.

Un consumidor también puede ser un proveedor si provee de regreso un servicio en el Ciberespacio o si habilita a otro consumidor para acceder al Ciberespacio. Un consumidor de un mundo virtual se puede convertir en proveedor al disponer productos y servicios virtuales para otros consumidores.

7.3 Proveedores

Los proveedores son aquellos que facilitan servicios en el Ciberespacio, así como los proveedores de servicios de Internet que habilitan el acceso de los consumidores al Ciberespacio y a los varios servicios disponibles en el Ciberespacio.

Los proveedores también se pueden entender como portadores o mayoristas, versus los distribuidores y minoristas de servicios de acceso. Esta distinción es importante desde una perspectiva de seguridad y, especialmente, desde la perspectiva de la aplicación de la ley, debido a que si en la situación de que un distribuidor o minorista no sea capaz de entregar una adecuada seguridad o acceso legal, los servicios de apoyo volverán obligadamente al portador o mayorista. Entender la naturaleza de un proveedor de servicio determinado es un elemento útil en la gestión de riesgo del ciberespacio.

Los proveedores de servicios de aplicaciones habilitan los servicios a los consumidores a través de su software. Estos servicios toman muchas formas e incluyen combinaciones de los elementos de esta lista no exhaustiva:

— edición, almacenamiento y distribución de documentos;

— entornos virtuales online para entretenimiento, comunicaciones e interacción con otros usuarios;

— repositorios de recursos digitales online con servicios agregados, indexados, de búsqueda, vitrina, catálogo, carro de compras y pago; y

— funciones de gestión de recursos de empresa tales como recursos humanos, finanzas y planillas de sueldo, gestión de cadena de suministro, relación con los consumidores y facturación.

8 Activos en el Ciberespacio

8.1 Visión general

Un activo es cualquier cosa que tenga un valor para un individuo u organización. Hay muchos tipos de activos, incluyendo, pero no limitados a:

a) información;

b) software, como un programa informático;

c) activos físicos, como un computador;

d) servicios

e) personas, sus cualificaciones, competencias y experiencia; y

f) activos intangibles, como la reputación e imagen.

NOTA 1 Usualmente los activos son vistos de manera simplificada sólo como información o como recursos.

NOTA 2 La norma ISO/IEC 15408-1:2005 define un activo como información o recursos que se deben proteger por controles de un Objetivo de Evaluación[2].

2 En inglés: *TOE, Target of Evaluation.*

NOTA 3 La norma ISO/IEC 19770-1 se ha desarrollado para habilitar a una organización para demostrar que está realizando una Gestión de Activos de Software[3] de acuerdo a un estándar suficiente para satisfacer los requisitos de gobernanza corporativa y para asegurar un apoyo eficaz para la gestión de servicios de TI en general. La norma ISO/IEC 19770 pretende alinearse estrechamente y apoyar a ISO/IEC 20000.

NOTA 4 La norma ISO/IEC 20000-1 promueve la adaptación de un enfoque de proceso integrado al momento de establecer, implementar, operar, monitorear, medir, revisar y mejorar el Sistema de Gestión de Servicios[4] para diseñar y entregar servicios que cumplan con las necesidades del negocio y los requisitos de los consumidores.

Para el propósito de esta norma, los activos en el Ciberespacio se clasifican en las clases siguientes:

— personal; y

— organizacional.

Para ambas clases, un activo se puede clasificar más detalladamente como:

— un activo físico, cuya forma existe en el mundo real; o

— un activo virtual, que sólo existe en el Ciberespacio y no se puede ver o tocar en el mundo real.

8.2 Activos personales

Uno de los activos virtuales clave es la identidad online del consumidor individual y su información crediticia online. La identidad online se considera un activo, puesto que es el identificador clave para cualquier consumidor individual en el Ciberespacio.

Otros activos virtuales del consumidor individual incluyen sus referencias en los mundos virtuales. En los mundos virtuales, los miembros suelen usar avatares virtuales para representarse o identificarse a ellos mismos o para actuar en su propio nombre. Se suele usar una moneda virtual para realizar transacciones virtuales. Estos avatares y monedas se pueden considerar activos que le pertenecen a un consumidor individual.

EJEMPLO Algunos bancos operan en mundos virtuales y reconocen el dinero del mundo virtual como una moneda oficial.

En el contexto de esta norma también se consideran activos al hardware y software de TI, así como los dispositivos digitales personales o endpoints que le permiten al consumidor conectarse y comunicarse en el Ciberespacio.

8.3 Activos organizacionales

Un aspecto clave del Ciberespacio es la infraestructura que hace todo posible. Esta infraestructura es una interconexión enmallada de redes, servicios y aplicaciones que les pertenecen a muchos proveedores de servicios. Sin embargo, la confiabilidad y disponibilidad de esta infraestructura es crucial para asegurarse de que los servicios y aplicaciones del Ciberespacio estén disponibles para cualquier persona en el Ciberespacio. Si bien cualquier infraestructura que le permita a cualquier consumidor conectarse al Ciberespacio, o que le permita a cualquier consumidor acceder a los servicios en el Ciberespacio, se considera un activo físico que se debe abordar en esta norma, pueden

3 En inglés: *SAM, Software Asset Management.*

4 En inglés: *SMS, Service Management System.*

haber muchos solapamientos con las medidas de seguridad que se proponen en, por ejemplo, la CIIP, la seguridad de Internet y la seguridad de red. Sin embargo, esta norma se debe enfocar en asegurar que los problemas de seguridad que puedan afectar a estos activos organizacionales se aborden de forma apropiada sin enfatizar más de lo debido otros problemas que no estén dentro del alcance de esta norma.

Además de los activos físicos, los activos organizacionales virtuales son cada vez más valiosos. La marca online y otras representaciones de la organización en el Ciberespacio identifican de manera única a la organización y son tan importantes como el “brick-and-mortar” de dicha organización.

EJEMPLO 1 La URL y la información del sitio Web de una organización son activos.

EJEMPLO 2 Algunos países incluso han establecido embajadas en un mundo virtual importante para proteger la representación del país.

Otros activos organizacionales que se exponen a través de la vulnerabilidad en el Ciberespacio incluyen la propiedad intelectual (fórmulas, procesos propietarios, patentes, resultados de investigaciones) y planes y estrategias de negocio (lanzamiento de un producto y tácticas de marketing, información competitiva, información financiera e informe de datos).

9 Amenazas contra la seguridad del Ciberespacio

9.1 Amenazas

9.1.1 Visión general

Las amenazas que existen en el Ciberespacio se analizan en relación a los activos en el Ciberespacio.

Las amenazas al Ciberespacio se pueden dividir en dos áreas claves:

— amenazas a activos personales;

— amenazas a activos organizacionales;

9.1.2 Amenazas a activos personales

Las amenazas a los activos personales se centran principalmente en los problemas de identidad, provocados por la filtración o robo de información personal.

EJEMPLO 1 La información crediticia se puede vender en el mercado negro, lo que puede facilitar el robo de identidad online.

Si la identidad online de una persona es robada o enmascarada, se le puede privar a esa persona de acceso a servicios y aplicaciones claves. En escenarios más serios, las consecuencias pueden variar desde incidentes financieros hasta incidentes de nivel nacional.

El acceso no autorizado a la información financiera de una persona también puede abrir la posibilidad de robo del dinero de esa persona y fraudes.

Otra amenaza es la posibilidad de convertir el endpoint en un zombi o bot. Los dispositivos de computación personal se pueden ver comprometidos y así formar parte de una botnet mayor.

Además de los descritos anteriormente, otros activos virtuales que pueden ser blancos de ataques son los activos personales en los mundos virtuales y juegos online. Los activos en un mundo virtual o el mundo de los juegos online también son blancos de ataques y abusos.

EJEMPLO 2 Los detalles de avatar y la moneda virtual que pueden, en algunos casos, ser intercambiados y convertidos en el mundo real, serían los principales objetivos de ataque.

Los robos virtuales y asaltos virtuales son algunos de los nuevos términos adoptados para este tipo de ataques. La seguridad, en este caso, dependerá de la cantidad de información del mundo real que es accesible, así como del marco de seguridad del mundo virtual propiamente tal, como se define e implementa por su administrador.

Ya que aún se están escribiendo las reglas y normas para la protección de activos físicos reales en conexión con el Ciberespacio, aquellas que se aplican a los activos virtuales son casi inexistentes. Se debe tener cuidado y precaución al prometerle a los participantes que sus activos virtuales se protegerán apropiadamente.

9.1.3 Amenazas a activos organizacionales

La presencia online de las organizaciones y los negocios online suelen ser blancos de malhechores cuyas intenciones van más allá de un simple pasatiempo.

EJEMPLO 1 Los sindicatos del Cibercrimen organizado en ocasiones amenazan a las organizaciones diciendo que bajarán sus sitios Web o que les causarán vergüenzas por medio de acciones como la desfiguración de sus sitios Web.

EJEMPLO 2 Si ciberocupantes registran o roban la URL de una organización y la venden a organizaciones no relacionadas a la organización del mundo real, se puede perder la confianza online de la organización víctima.

En el caso de un ataque exitoso, la información personal de los empleados, clientes, socios o suministradores se puede divulgar y resultar en sanciones contra las organizaciones si se descubre que dicha información se gestionó o protegió de manera insuficiente, contribuyendo a su pérdida.

Las normas de clasificación financiera también se pueden violar si los resultados organizacionales se divulgan sin autorización.

Los gobiernos resguardan información sobre asuntos de seguridad nacional, militares y de inteligencia entre otros elementos relacionados al gobierno y Estado, además de una vasta matriz de información sobre individuos, organizaciones y de la sociedad en su totalidad.

Los gobiernos deben proteger su infraestructura e información del acceso inapropiado y de abusos. Con la tendencia en crecimiento y expansión de ofrecer servicios gubernamentales online a través del Ciberespacio, éste es un nuevo canal, entre otros, para lanzar ataques y acceder a la información descrita anteriormente. Si los ataques tienen éxito, pueden resultar en riesgos graves para la nación, su gobierno y su sociedad.

En una escala mayor, la infraestructura que soporta el Internet, y por ende al Ciberespacio, también puede ser blanco de ataques. Si bien esto no afectará de manera permanente al funcionamiento del Ciberespacio, sí afectará la confiabilidad y disponibilidad de la infraestructura, la que contribuye a la seguridad del Ciberespacio.

En un nivel nacional o internacional, el Ciberespacio es un área gris donde prospera el terrorismo. Una de las razones es la facilidad de comunicación provista por el Ciberespacio. Debido a la naturaleza del Ciberespacio, específicamente en relación a los desafíos de definir fronteras y límites, es difícil regular y controlar la forma en la que se puede usar.

Los grupos terroristas pueden tanto comprar de manera legítima las aplicaciones, servicios y recursos que facilitan su causa o pueden recurrir a medios ilegales para asegurar estos recursos para evitar su detección y rastreo. Esto puede incluir adquirir recursos de computación masivos a través de botnets.

9.2 Agentes de amenaza

Un agente de amenaza es un individuo o grupo de individuos que tiene cualquier rol en la ejecución o soporte de un ataque.

El entendimiento riguroso de sus motivos (religiosos, políticos, económicos, etc.), capacidades (conocimiento, financiamiento, tamaño, etc.) e intenciones (diversión, crimen, espionaje, etc.) es crucial en la evaluación de vulnerabilidades y riesgos, así como en el desarrollo y despliegue de controles.

9.3 Vulnerabilidades

Una vulnerabilidad es una debilidad de un activo o control que se puede aprovechar por una amenaza. En el contexto de un sistema de información, ISO/IEC TR 19791:2006 también define una vulnerabilidad como un defecto, debilidad o propiedad del diseño o implementación de un sistema de información (incluyendo sus controles de seguridad) o su entorno que se podría aprovechar de manera intencional o no intencional para afectar desfavorablemente los activos u operaciones de una organización.

La evaluación de vulnerabilidades debe ser una tarea continua. A medida que un sistema recibe parches, actualizaciones o se le añaden nuevos elementos, se pueden introducir nuevas vulnerabilidades. Los actores requieren un conocimiento y entendimiento rigurosos del activo o control en cuestión, así como de las amenazas, agentes de amenaza y riesgos involucrados para llevar a cabo una evaluación completa.

NOTA La norma ISO/IEC 27005 provee directrices para identificar vulnerabilidades.

Se debería mantener un inventario de las vulnerabilidades conocidas con el protocolo de acceso más estricto que exista y, preferentemente, de manera separada tanto física como lógicamente del activo o control al que es aplicable. En el caso de que se viole el acceso y se comprometa el inventario de vulnerabilidad, éste podría ser una de las herramientas más efectivas en el arsenal de un agente de amenaza para perpetrar un ataque.

Se deben buscar e implementar soluciones a las vulnerabilidades y, cuando una solución no sea posible o factible, se deben aplicar controles. Este enfoque se debería aplicar de manera prioritaria para que se aborden primero las vulnerabilidades que puedan significar un riesgo mayor. Los procedimientos de divulgación de vulnerabilidad se podrían definir bajo el marco de intercambio y coordinación de información en cláusula 13.

NOTA Una norma futura, ISO/IEC 29147, proveerá una guía sobre la divulgación de vulnerabilidad.

9.4 Mecanismos de ataque

9.4.1 Introducción

Muchos de los ataques en el Ciberespacio se llevan a cabo usando softwares maliciosos como spywares, gusanos y virus. La información se suele recolectar a través de técnicas de suplantación de identidad. Un ataque puede ocurrir como un vector de ataque único o llevado a cabo como un mecanismo de ataque combinado. Estos ataques se pueden propagar vía, por ejemplo, sitios Web sospechosos, descargas no verificadas, correos electrónicos spam, explotación remota y medios extraíbles infectados.

Los ataques pueden venir desde dos categorías principales:

— ataques desde dentro de una red privada; y

— ataques desde fuera de una red privada.

Hay casos en que los ataques son una combinación tanto desde dentro como desde fuera de una red privada. Otros mecanismos que han crecido, tanto en uso como en sofisticación, para llevar a cabo ataques, son aquellos que se basan en sitios de redes sociales y en el uso de archivos corrompidos en sitios Web legítimos.

Los individuos tienden a confiar tácitamente en mensajes y contenidos recibidos por contactos que han aceptado previamente en sus perfiles en los sitios de redes sociales. Una vez que un atacante, a través de robo de identidad, se puede disfrazar como un contacto legítimo, éste puede comprometer a otros y de este modo se abre otro camino para el lanzamiento de varios tipos de ataques discutidos anteriormente.

Los sitios Web legítimos también pueden ser víctimas de hackeos y sufrir la corrupción de sus archivos para usarlos como medios para perpetuar ataques. Los individuos tienden a confiar tácitamente en sitios Web que visitan comúnmente, normalmente añadidos a sus favoritos en sus navegadores de Internet por mucho tiempo e incluso más en aquellos que usan mecanismos de seguridades como la Capa de Conexión Segura[5]. Aunque la autenticación de las partes y la integridad de la información que se está transmitiendo o recibiendo se encuentran aun trabajando, la SSL no hace diferencia entre el contenido original y el nuevo contenido corrompido (insertado por atacantes), exponiendo así a los usuarios de dicho sitio Web a ataques.

A pesar de que la fuente se perciba como legítima, como en las instancia descritas anteriormente, los individuos deben aun así tomar las precauciones destacadas en cláusula 11 para protegerse mejor.

9.4.2 Ataques desde dentro de una red privada

Estos ataques se lanzan normalmente dentro de la red privada de una organización, típicamente la red de área local, y pueden ser iniciados por empleados o por alguien que obtenga acceso a un computador o red en las instalaciones de una organización o individuo.

EJEMPLO 1 Un caso posible es que los administradores del sistema se pueden aprovechar de los privilegios de acceso al sistema que poseen, tales como el acceso a la información de contraseña de los usuarios, y utilizarlos para iniciar un ataque. Por otro lado, los propios administradores del sistema se pueden convertir en el blanco inicial de un ataque con el fin de que el atacante obtenga información adicional (nombres de usuarios, contraseñas, etc.) antes de proceder a su blanco o blancos originales.

El atacante puede usar mecanismos como un software analizador de paquetes para obtener contraseñas u otra información de identidad. De manera alternativa, el atacante se puede enmascarar como una entidad autorizada y actuar como intermediario para robar información de identidad.

EJEMPLO 2 Un ejemplo es el uso de Puntos de Acceso[6] corruptos para robar identidades. En este caso, el atacante se puede sentar en un aeropuerto, cafetería u otros lugares públicos que ofrecen acceso gratuito Wi-Fi a Internet. En algunos casos, el atacante incluso se puede enmascarar como el dueño legítimo del punto de acceso inalámbrico en la instalación al usar el nombre de red[7] del lugar. Si un usuario accede a este AP corrupto, el atacante puede actuar como intermediario y obtener contraseñas valiosas y/o información de identidad del usuario, por ejemplo, información y contraseñas de cuentas bancarias, la contraseña de su correo electrónico, etc.

5 En inglés: *SSL, Secure Sockets Layer.*

6 En inglés: *AP, Access Points.*

7 En inglés: *SSID, Service Set IDentifier.*

EJEMPLO 3 Usualmente basta con estar cerca de una red Wi-Fi desprotegida, como sentarse en un auto fuera de una casa, para robar información en la red.

Además de los ataques lanzados por atacantes humanos, los computadores infectados por malware también lanzan varios ataques a los computadores que lo rodean dentro de una red privada.

EJEMPLO 4 Muchos malwares suelen enviar paquetes de escaneo a la red privada para encontrar computadores a sus alrededores y luego tratar de abusar de éstos.

EJEMPLO 5 Algunos malwares usan el modo promiscuo de una interfaz de red de su computador infectado para espiar el tráfico que fluye a través de la red privada.

EJEMPLO 6 Los registradores de tecla son aplicaciones de hardware o software que capturan todas las pulsaciones de teclas en el sistema objetivo. Esto se puede llevar a cabo en secreto para monitorear las acciones de un usuario. Los rastreadores de teclas a veces se usan para capturar información de autenticación desde las páginas de acceso a aplicaciones.

9.4.3 Ataques desde fuera de una red privada (ejemplo, Internet)

Hay muchos ataques diferentes que se pueden lanzar desde el exterior de una red privada, incluyendo Internet.

Si bien el ataque inicial siempre tendrá como objetivo un sistema de cara al público (por ejemplo, router, servidor, firewall, sitio Web, etc.), los atacantes pueden también buscar explotar activos que estén dentro de la red privada.

Los antiguos métodos de ataque se mejoran y se desarrollan nuevos constantemente. Los atacantes son cada vez más sofisticados y normalmente combinan diferentes técnicas y mecanismos de ataque para maximizar su éxito, lo que hace que la detección y prevención de ataques sean más difíciles.

Los escáneres de puerto son unas de las herramientas más viejas y aún eficaces utilizadas por los atacantes. Estos escanean todos los puertos disponibles en un servidor para confirmar qué puertos están “abiertos”. Este es normalmente uno de los primeros pasos ejecutados por un potencial atacante en el sistema objetivo.

Estos ataques se pueden manifestar en varios ataques DoS tanto en los servidores de aplicación u otros equipos de operaciones en red por medio de la explotación del protocolo o de las vulnerabilidades de diseño de aplicación.

EJEMPLO Con la ayuda de una botnet se pueden lanzar ataques DoS a gran escala que pueden inhabilitar el acceso de un país al Ciberespacio.

Con la proliferación de las aplicaciones de pares (peer-to-peer), usadas comúnmente para compartir archivos como música, videos y fotos digitales, entre otros, los atacantes se están volviendo cada vez más sofisticados en cómo disfrazarse a sí mismos y a sus códigos maliciosos por medio de los archivos compartidos en forma de caballos troyanos para sus ataques.

Los desbordamientos de búfer (llamados de otro modo rebasamientos de búfer) son otro método popular para comprometer servidores en Internet. Al abusar de las vulnerabilidades de código y enviar cadenas de caracteres más largas de lo esperado, los atacantes causan que el servidor opere fuera de su entorno normal (controlado), facilitando así la inserción/ejecución de códigos maliciosos.

Otra técnica es la Suplantación de IP, la que consiste en que el atacante manipula la dirección IP asociada con sus mensajes en un intento de disfrazarse como una fuente conocida y confiable, obteniendo de este modo un acceso no autorizado a los sistemas.

10 Roles de las partes interesadas en la Ciberseguridad

10.1 Visión general

Para mejorar el estado de la Ciberseguridad, las partes interesadas en el Ciberespacio necesitan tener un rol activo en su uso y desarrollo respectivos de Internet. Estos roles pueden a veces superponerse con sus roles individuales y organizacionales en sus redes personales o de organización. El término red de organización se refiere a la combinación de las redes privadas (normalmente una intranet), extranets y redes visibles públicamente de una organización. Para propósitos de esta norma, las redes visibles públicamente serán aquellas expuestas a Internet, por ejemplo, para alojar un sitio Web. Debido a esta superposición, puede parecer que estos roles no tengan un beneficio significativo o directo para el individuo y la organización afectados. Sin embargo, son significativos al mejorar la Ciberseguridad cuando todos los involucrados actúan consecuentemente.

10.2 Roles de los consumidores

10.2.1 Introducción

Los consumidores pueden ver o recolectar información, así como proveer cierta información específica en el espacio de aplicaciones en el Ciberespacio, o estar abiertos a miembros o grupos limitados dentro del espacio de aplicaciones o el público general. Las acciones llevadas a cabo por los consumidores en estos roles pueden ser pasivas o activas y pueden contribuir de manera directa o indirecta al estado de la Ciberseguridad.

10.2.2 Roles de los individuos

Los consumidores individuales del Ciberespacio pueden asumir diferentes roles en contextos y aplicaciones diferentes.

Los roles de los consumidores incluyen, pero no se limitan a:

— usuario general de aplicación del Ciberespacio o usuario general como los jugadores de juegos online, usuarios de mensajería instantánea o navegantes en la Web;

— comprador/vendedor, involucrado en poner bienes y servicios en sitios de remate y mercados online para compradores interesados y viceversa;

— blogueros y otros contribuidores de contenido (por ejemplo, un autor de un artículo en una wiki), con la publicación de información en texto o multimedia (por ejemplo, video clips) para el público en general o para el consumo de una audiencia limitada;

— un IAP dentro de un contexto de aplicación (como un juego online) o el Ciberespacio en general;

— miembro de una organización (como el empleado de una compañía u otra forma de asociación a una compañía);

— otros roles. Es posible que a un usuario se le asigne un rol de manera no intencional o sin su consentimiento.

EJEMPLO Cuando un usuario visita un sitio que requiere autorización y obtiene acceso de manera no intencional, éste se puede etiquetar como un intruso.

En cada uno de estos roles los individuos pueden ver o recolectar información, así como proveer cierta información específica en el espacio de aplicaciones en el Ciberespacio, o estar abiertos a miembros o grupos limitados dentro del espacio de aplicaciones o el público general. Las acciones llevadas a cabo por los consumidores en estos roles pueden ser pasivas o activas y pueden contribuir de manera directa o indirecta al estado de la Ciberseguridad.

EJEMPLO 1 Si un IAP provee una aplicación que contiene vulnerabilidades de protección, estas vulnerabilidades se pueden usar por Ciber malhechores como un canal para llegar a los usuarios de la aplicación.

EJEMPLO 2 Los blogueros u otros contribuidores de contenido pueden recibir una solicitud en forma de preguntas inocentes sobre sus contenidos. Al responder, pueden revelar de manera no intencional al público más información personal o de la compañía de la que se desea.

EJEMPLO 3 Un individuo que actúa como un comprador o vendedor puede participar sin saber en transacciones criminales de venta de bienes robados o actividades de lavado de dinero.

Por consiguiente, como en el mundo real, los consumidores individuales necesitan tener precaución en cada uno de los roles que poseen en el Ciberespacio.

10.2.3 Roles de las organizaciones

Las organizaciones suelen usar el Ciberespacio para publicitar compañías e información relacionadas, así como productos y servicios de mercado. Las organizaciones también usan el Ciberespacio como parte de su red para entregar y recibir mensajes electrónicos (por ejemplo, correos electrónicos) y otros documentos (por ejemplo, transferencia de archivos).

En concordancia con los mismos principios de ser un buen ciudadano corporativo, estas organizaciones deberían extender sus responsabilidades corporativas al Ciberespacio al asegurarse proactivamente de que sus prácticas y acciones en éste no introducen más riesgos de protección. Algunas medidas proactivas incluyen:

— una gestión adecuada de seguridad de la información mediante la implementación y operación de un sistema de gestión de seguridad de la información (SGSI) eficaz;

NOTA 1 La norma ISO/IEC 27001 provee requisitos para los sistemas de gestión de protección de la información.

— un seguimiento y respuesta de seguridad adecuados;

— incorporar la seguridad como parte del Ciclo de Vida de Desarrollo de Software[8] donde se necesita determinar el nivel de seguridad construido en los sistemas en base a la criticidad de los datos de la organización;

— una educación estándar sobre la seguridad para los usuarios en la organización a través de actualizaciones constantes de la tecnología y la mantención de un registro de los desarrollos más actuales de tecnología; y

— entender y usar los canales apropiados para comunicarse con los vendedores y proveedores de servicios sobre los problemas de seguridad descubiertos durante el uso.

NOTA 2 Una norma futura, ISO/IEC 29147, proveerá directrices sobre la divulgación de vulnerabilidad.

NOTA 3 La norma ISO/IEC 27031 provee directrices para la preparación de TICs para la continuidad del negocio.

8 En inglés: *SDLC, Software Development Life-cycle.*

NOTA 4 La norma ISO/IEC 27035 provee directrices para la gestión de incidentes de seguridad de la información.

NOTA 5 La norma ISO/IEC 27034-1 provee directrices para la seguridad de aplicaciones.

El gobierno, principalmente las agencias y reguladores de reforzamiento de la ley, pueden tener los siguientes roles importantes:

— aconsejar a las organizaciones sobre sus roles y responsabilidades en el Ciberespacio;

— compartir información con otras partes interesadas sobre las últimas tendencias y desarrollos en tecnología;

— compartir información con otras partes interesadas sobre los riesgos de seguridad prevalentes actuales;

— ser un conducto para recibir información, tanto abierta como cerrada, con respecto a los riesgos de seguridad para el Ciberespacio; y

— ser el coordinador primario para la divulgación de información y la orquestación de cualquier recurso requerido, tanto a nivel nacional como corporativo, en tiempos de crisis que surjan de un ciber ataque masivo.

10.3 Roles de los proveedores

Las organizaciones que proveen servicios pueden incluir dos categorías:

— proveedores de acceso a empleados y socios al Ciberespacio; y

— proveedores de servicios a los consumidores del Ciberespacio, ya sea a una comunidad cerrada (por ejemplo, usuarios registrados) o al público general a través de la entrega de aplicaciones de Ciberespacio.

EJEMPLO Algunos ejemplos de servicios son los mercados de intercambio online, servicios de plataformas de foros de discusión, servicios de plataformas de blogs y servicios de redes sociales.

Los proveedores de servicios también son organizaciones de consumidores. Por lo tanto, se espera que éstas observen los mismos roles y responsabilidades que las organizaciones de consumidores. Como proveedores de servicios, éstos tienen responsabilidades adicionales en el mantenimiento o incluso el reforzamiento de la seguridad del Ciberespacio al:

— proveer productos y servicios seguros y protegidos;

— proveer una orientación de seguridad y protección para los usuarios finales; y

— proveer aportes de seguridad para otros proveedores y para los consumidores sobre las tendencias y observaciones sobre el tráfico en sus redes y servicios.

11 Directrices para las partes interesadas

11.1 Visión general

La orientación en esta cláusula se enfoca en tres áreas principales:

— una guía de seguridad para los consumidores;

— la gestión de riesgos de seguridad de la información interna de una organización; y

— los requisitos de seguridad que los proveedores deben especificar para que los consumidores los implementen.

Las recomendaciones se estructuran de la manera siguiente:

a) una introducción a la evaluación y tratamiento de riesgos;

b) directrices para los consumidores; y

c) directrices para las organizaciones, incluyendo los siguiente elementos de los proveedores de servicios:

   — la gestión de los riesgos de seguridad de la información en el negocio; y

   — los requisitos de seguridad para alojar servicios y otros servicios de aplicación.

11.2 Evaluación y tratamiento de riesgos

La norma ISO 31000, provee los principios y directrices genéricas sobre la gestión de riesgos mientras que ISO/IEC 27005, provee directrices y procesos para la gestión de riesgos de seguridad de la información en una organización, apoyando en particular los requisitos para un SGSI de acuerdo a ISO/IEC 27001. Estas directrices y procesos se consideran suficientes para abordar la gestión de riesgos en el contexto del Ciberespacio.

La norma ISO/IEC 27005:2011 no provee ninguna metodología específica para la gestión de riesgos de seguridad de la información. Es responsabilidad de los consumidores y de los proveedores definir sus enfoques de la gestión de riesgos. Se puede usar un número de metodologías existentes bajo el marco descrito en ISO/IEC 27005 para implementar los requisitos de un SGSI.

Se deben tomar en cuenta los siguientes aspectos al momento de definir un enfoque de gestión de riesgos:

— Identificación de activos críticos: El conectarse o usar el Ciberespacio se amplía el alcance de definición de activos. Debido a que no es rentable proteger todos los activos, es esencial definir los activos críticos para tener un cuidado en particular al momento de protegerlos. La designación se debería hacer desde el contexto de negocio y a través de la consideración del impacto que la pérdida o degradación de un activo puede tener en el negocio en su totalidad.

— Identificación de riesgos: Las partes interesadas deberían considerar y abordar de manera apropiada los riesgos, amenazas y ataques adicionales que se vuelven relevantes al participar en el Ciberespacio.

— Responsabilidad: Al participar en el Ciberespacio, la parte interesada debería aceptar la responsabilidad adicional con respecto a otras partes interesadas. Esto incluye:

— Reconocimiento: Reconocer los posibles riesgos que la participación de las partes interesadas puede introducir en el Ciberespacio en general y específicamente en los sistemas de información de otras partes interesadas.

— Informar: Puede ser necesario incluir a partes interesadas fuera de la organización al momento de distribuir informes relacionados a los riesgos, incidentes y amenazas.

— Compartir información: Cuando se informe, puede ser necesario compartir información relevante con otras partes interesadas.

— Evaluación de riesgos: Es necesario determinar el alcance al cual las acciones y presencia de una parte interesada en el Ciberespacio se vuelven, o contribuyen a, un riesgo para otra parte interesada.

— Normas/Legislaciones: Al conectarse al Ciberespacio, los límites legales y normativos se hacen difíciles de distinguir y se aplican más requisitos, los que a veces pueden resultar contradictorios.

— Retiro de un sistema o servicio: Una vez que un sistema o servicio ya no se necesita, se debería retirar de manera que se asegure que los servicios o interfaces relacionados no se vean impactados. Toda la información relacionada a la seguridad se debe invalidar para asegurar que los sistemas a los cuales se hace interfaz o está relacionada no se vean comprometidos.

— Consistencia: El enfoque a la gestión de riesgos se aplica a través del Ciberespacio de manera completa. En este enfoque o metodología, los consumidores y proveedores en el Ciberespacio se les asignan responsabilidades para actividades específicas, como los planes de contingencia, la recuperación ante desastres y el desarrollo e implementación de programas protectores para los sistemas bajo su control y/o propiedad.

En general, la metodología de gestión de riesgos en ISO/IEC 27005 abarca el ciclo de vida completo de un sistema genérico, haciéndolo de esta forma utilizable para nuevos sistemas de seguridad, así como para sistemas ya existentes. Puesto a que ésta se ocupa del tratamiento de sistemas, es aplicable a todos los modelos de negocio. Los procesos del marco de trabajo pueden tratar las redes y servicios de los proveedores de servicios como un sistema integrado, consistente de subsistemas que proveen servicios públicos y subsistemas privados que soportan los servicios internos, o puede tratar cada uno de los servicios individuales (por ejemplo, hospedaje Web) de manera separada y describir su provisión en términos de sistemas interactivos separados. Puede resultar una ventaja, por la simplicidad, considerar todo lo que se necesita para soportar los servicios del proveedor como un sistema mayor que se puede descomponer en sistemas más pequeños, cada uno de los cuales provee un servicio comerciable o forma parte de la infraestructura.

Algunos aspectos importantes a recordar cuando se consideren las metas y objetivos de Ciberseguridad son:

a) proteger la seguridad general del Ciberespacio;

b) un plan para emergencias y crisis por medio de la participación en ejercicio y planes de respuesta actualizados y planes para la continuidad de las operaciones;

c) educar a las partes interesadas sobre las prácticas de gestión de riesgos y Ciberseguridad;

d) asegurar un intercambio oportuno, relevante y preciso de la información tratada entre las comunidades de reforzamiento de la ley de inteligencia y los decisores clave relevantes para el Ciberespacio; y

e) establecer mecanismos de coordinación intersectoriales y entre múltiples partes interesadas de manera eficaz para abordar las interdependencias críticas, incluyendo la conciencia situacional de incidentes y la gestión de incidentes trans-sectoriales y entre múltiples partes interesadas.

Las metas y objetivos desde a) hasta c) fluyen directamente hacia los proveedores de servicios, quienes son responsables por el equipo y los servicios que están bajo su control. En el caso de las metas y objetivos d) y e), los proveedores de servicios se involucran como participantes activos en el intercambio de información y en las actividades de coordinación.

Las metas específicas de los proveedores de servicios, como qué servicios proveer, fluyen desde el contexto del negocio.

11.3 Directrices para los consumidores

Esta norma no está dirigida a los individuos del Ciberespacio específicamente, sino que se enfoca en las organizaciones que proveen servicios a consumidores y en las organizaciones que requieren que sus empleados o usuarios finales practiquen un uso seguro del Ciberespacio para gestionar los riesgos de Ciberseguridad de manera eficaz. La guía sobre los roles y seguridad de los usuarios en el Ciberespacio y de cómo éstos pueden influenciar positivamente el estado de la Ciberseguridad busca ser una guía para el diseño y desarrollo de contenidos por estas organizaciones, en el contexto de su provisión de servicios y conciencia y programas de formación para la entrega que harán a sus usuarios finales.

Como se explica en 10.2, los consumidores pueden ver o recolectar información, así como proveer cierta información específica en el espacio de aplicaciones en el Ciberespacio, o estar abiertos a miembros o grupos limitados dentro del espacio de aplicaciones o el público general. Las acciones llevadas a cabo por los consumidores en estos roles pueden ser pasivas o activas y pueden contribuir de manera directa o indirecta al estado de la Ciberseguridad.

Por ejemplo, como un IAP, si la aplicación provista contiene vulnerabilidades de seguridad, éstas pueden resultar en el abuso de ciber malhechores quienes se aprovechan de éstas como un canal para llegar a usuarios inocentes de la aplicación. En el caso de los blogueros u otros contribuidores de contenido, éstos pueden recibir una solicitud en forma de preguntas inocentes sobre sus contenidos. Al responder, pueden revelar de manera no intencional al público más información personal o de la compañía de la que se desea. En el caso de un comprador o vendedor, éste puede participar sin saber en transacciones criminales de venta de bienes robados o en actividades de lavado de dinero. Consiguientemente, como en el mundo real, los consumidores individuales necesitan tener precaución en cada uno de los roles que poseen en el Ciberespacio.

En general, los consumidores deberían tomar nota de la guía siguiente:

a) Aprender y entender las políticas de seguridad y privacidad del sitio y aplicación que les interesa, tal como fueron publicadas por el proveedor del sitio.

b) Aprender y entender los riesgos de seguridad y privacidad involucrados y determinar los controles aplicables apropiados. Participar en foros de discusión online relacionados o preguntarle a alguien que sepa de la aplicación del sitio antes de proveer información personal o de la organización, o participar y contribuir información a la discusión.

c) Establecer y practicar una política de privacidad personal para la protección de identidad al determinar las categorías de la información personal disponible y compartir los principios relacionados a esa información.

d) Gestionar la identidad online. Usar diferentes identificadores para las aplicaciones de diferentes sitios Web y minimizar el intercambio de información personal para cada sitio Web o aplicación que requiere dicha información. Registrar (uno mismo) la identidad online en sitios de redes sociales, incluso si dicha cuenta se deja inactiva.

EJEMPLO La autenticación única es una forma de gestionar la identidad online.

e) Informar eventos o encuentros sospechosos a la autoridades respectivas (ver Anexo B, como un ejemplo de una lista de contactos disponible públicamente).

f) Como comprador o vendedor, se debe leer y entender la política de seguridad y privacidad de los sitios de mercados online y realizar los pasos para verificar la autenticidad de las partes interesadas e involucradas. No compartir datos personales, incluyendo la información bancaria, a menos que se establezca un interés genuino en vender o comprar. Usar un mecanismo de pago confiable.

g) En el caso de un IAP, éste debe poner en práctica un desarrollo de software seguro y proveer un valor hash de código online para que las partes receptoras puedan verificar el valor, si es necesario, para asegurar la integridad del código. Este debe proveer una documentación sobre las políticas y prácticas de seguridad y privacidad del código y respetar la privacidad de los usuarios del código.

h) En el caso de los blogueros u otros contribuidores de contenido (incluyendo a los mantenedores de sitios Web), éstos se deben asegurar de que la privacidad e información sensible de las partes interesadas aplicables no se divulga a través del blog o de publicaciones online. Se debe revisar los comentarios y los posteos recibidos en el sitio para asegurarse de que no contienen ningún contenido malicioso como links a sitios Web de suplantación de identidad o descargas maliciosas.

i) En el caso de los miembros de una organización, un consumidor individual debería aprender y entender la política de seguridad de información corporativa de la organización y asegurarse de que no se libere de manera intencional o accidental la información clasificada y/o sensible en ningún sitio Web en el Ciberespacio, a menos que haya una autorización previa y formalmente garantizada para dicha divulgación.

j) Otros roles. Cuando un usuario visita un sitio que requiere autorización y obtiene acceso de manera no intencional, éste se puede etiquetar como un intruso. Este se debe ir del sitio inmediatamente e informar la situación a la Autoridad Competente, ya que el hecho de que haya sido posible obtener acceso puede ser indicio de un compromiso.

11.4 Directrices para las organizaciones y proveedores de servicios

11.4.1 Visión general

Los controles para gestionar los riesgos de Ciberseguridad dependen significativamente de la madurez de los procesos de gestión de seguridad en las organizaciones (incluyendo a los proveedores de servicios). Si bien las directrices que se sugieren aquí son discrecionales para las organizaciones, se recomienda que los proveedores de servicios usen estas directrices como medidas de referencia obligatorias.

Las directrices en esta cláusula se pueden resumir de la forma siguiente:

— Gestionar los riesgos de seguridad de la información en el negocio.

— Abordar los requisitos de seguridad para el alojamiento Web y otros servicios de ciber-aplicación.

— Proveer una guía de seguridad a los consumidores.

11.4.2 Gestionar los riesgos de seguridad de la información en el negocio

11.4.2.1 Sistema de gestión de seguridad de la información

A nivel empresarial, las organizaciones que se conectan al Ciberespacio deberían implementar un Sistema de Gestión de la Seguridad de la Información[9] para identificar y gestionar riesgos relacionados con la seguridad de la información que puedan afectar al negocio. La serie de normas ISO/IEC 27000 para los sistemas de gestión de seguridad de la información provee la orientación y buenas prácticas requeridas para implementar dicho sistema.

Una consideración clave para implementar un SGSI es asegurarse de que la organización tenga un sistema para, de manera continua, identificar, evaluar, tratar y gestionar los riesgos de seguridad de la información relacionados al negocio, incluyendo la provisión de servicios en Internet, directamente a los usuarios finales o suscriptores, a cargo de un proveedor de servicios.

NOTA 1 La norma ISO/IEC 27005, provee directrices para la gestión de riesgos de seguridad de la información en una organización, apoyando particularmente los requisitos de un SGSI de acuerdo a ISO/IEC 27001.

NOTA 2 La norma ISO 31000, provee principios y directrices genéricas sobre la gestión de riesgos.

Las organizaciones también pueden considerar una certificación formal de su conformidad con los requisitos de un SGSI, como en ISO/IEC 27001.

Como parte de la implementación de un SGSI, una organización debería además establecer una capacidad de seguimiento de incidentes de seguridad y de respuesta y coordinar sus actividades de respuesta ante incidentes con organizaciones externas CIRT, CERT o CSIRT en el país. La provisión de una respuesta ante incidentes y emergencias debería incluir el seguimiento y evaluación del estado de la seguridad del uso de los servicios de la organización por parte de los usuarios finales y consumidores, además de proporcionar una guía para ayudar a las partes afectadas para que puedan responder a los incidentes de seguridad eficazmente.

NOTA La norma ISO/IEC 27035, provee una guía sobre la gestión de incidentes de seguridad de la información.

11.4.2.2 Proveer productos seguros

Algunas organizaciones desarrollan[10] y lanzan sus propias barras de herramientas para navegadores Web, dialers o códigos para proveer servicios de valor agregado a los usuarios finales o para facilitar el acceso a los servicios o aplicaciones de la organización. En dichas instancias, debería haber un acuerdo de usuarios finales apropiado en un lenguaje adecuado que incorpore declaraciones sobre las políticas de código, de privacidad y los medios de la organización, a través del cual los usuarios puedan cambiar su aceptación más adelante o priorizar cualquier problema que puedan tener con respecto a dichas políticas y prácticas. Cuando se usa un acuerdo de este tipo, éste se debe someter a un control de versión y la organización debería asegurarse de que los usuarios finales lo firmen constantemente.

9 En inglés: *ISMS, Information Security Management System.*

10 De manera interna o a través de un proveedor tercero.

Cuando hay un alto grado de dependencia en la seguridad de los productos de software, éstos se deberían validar de manera independiente bajo el plan de Criterios Comunes, como se describe en ISO/IEC 15408.

Las organizaciones deberían documentar el comportamiento de los códigos y hacer una evaluación de acuerdo a si el comportamiento puede caer en áreas potenciales que se pueden considerar spywares o software engañosos. En el último caso, se debería comprometer a un asesor cualificado apropiado para evaluar si el código cae en el criterio de objetivo de vendedores anti-spyware, que se adhiere a las buenas prácticas para que las herramientas de software proporcionadas por las organizaciones para los usuarios finales, no sean catalogadas como spyware o adware por los vendedores anti-spyware. Muchos vendedores anti-spyware publican sus criterios con los cuales clasifican a los softwares.

Las organizaciones deberían implementar firmas de código digitales para sus binarios, para que los vendedores anti-malware y anti-spyware puedan determinar fácilmente el propietario de un archivo y los ISVs (quienes producen consistentemente software que siguen las buenas prácticas) se categorizarán como probablemente seguros incluso antes de llevar a cabo un análisis.

En el caso de que una organización descubra técnicas de software útiles que puedan ayudar a reducir los problemas de spyware o malware, éstas deberían considerar aliarse y trabajar junto con los vendedores para habilitar ampliamente dichas técnicas.

Para cumplir con estos requisitos, es importante la educación de seguridad de los desarrolladores. Se debería usar un ciclo de vida de desarrollo de software seguro donde se puedan minimizar las vulnerabilidades de software, proporcionando así un producto de software más seguro.

NOTA La norma ISO/IEC 27034, provee directrices para definir, desarrollar, implementar, gestionar, soportar y retirar una aplicación.

11.4.2.3 Seguimiento y respuesta de red

El seguimiento de la red es usado normalmente por las organizaciones para asegurar la confiabilidad y calidad de sus servicios de red. Al mismo tiempo, esta capacidad se puede aprovechar para buscar condiciones de tráfico de red sospechosas y detectar actividades maliciosas que emerjan de la red. En general, las organizaciones deben trabajar de la manera siguiente:

— Entender el tráfico de la red: qué es normal y qué es anormal.

— Usar una herramienta de gestión de red para identificar peaks en el tráfico, tráfico/puertos “no usuales” y asegurarse de que hayan herramientas disponibles para precisar y responder a la causa.

— Probar la capacidad de respuesta antes de ser necesaria frente a un evento real. Refinar las técnicas, procesos y herramientas de respuesta en base al resultado de simulacros constantes.

— Entender los constituyentes de manera individual. Si alguien quien normalmente es un usuario inactivo repentinamente empieza a llegar al límite del 100% del ancho de banda disponible, puede ser necesario aislar al usuario que no se está comportando adecuadamente hasta que se encuentre la razón. El aislamiento de red puede prevenir la propagación de malwares, aunque algunas implementaciones pueden requerir el consentimiento del usuario o actualizaciones de los Términos de Servicio.

— Considerar el seguimiento de la actividad de puntos inteligentes en una red, tales como un DNS y filtros de mensajería, que pueden también servir a los dispositivos flag que han sido comprometidos con malwares, pero que, por una variedad de razones, no se ven afectados por los servicios antivirus o de IDS.

EJEMPLO Debido al volumen de información en una red, las herramientas como un IDS y un IPS se pueden usar para monitorear excepciones que se puedan informar.

11.4.2.4 Soporte y escalado

Los negocios, incluyendo a los proveedores de servicios y a las organizaciones gubernamentales, normalmente tienen un servicio de soporte para responder a las consultas de los consumidores y proveer una asistencia y soporte técnicos para abordar los problemas de los usuarios finales. Con la creciente proliferación de malwares en Internet, una organización proveedora de servicios puede recibir informes relacionados a infecciones por malware y spyware y a otros problemas de Ciberseguridad. Esta información es importante y útil para que los vendedores pertinentes evalúen la situación de riesgo y de malware y proporcionen actualizaciones a las herramientas necesarias para asegurarse de que cualquier malware o spyware nuevos detectados se puedan remover o inhabilitar de manera eficaz. A este respecto, una organización debería establecer contacto con los vendedores de seguridad y enviar los reportes pertinentes y muestras de malware a los vendedores para un seguimiento, en particular si se observa la prevalencia de un peak. Muchos vendedores mantienen una lista de correos electrónicos para recibir dichos informes o muestras para su análisis y seguimiento. Por ejemplo, ver Anexo B, Tabla B.1.

11.4.2.5 Mantenerse al tanto de los últimos desarrollos

Como parte de la implementación de un SGSI para gestionar los riesgos de seguridad de la información de una empresa, además de asegurarse de que las organizaciones continúen el seguimiento de las buenas prácticas de la industria y estén al tanto de las últimas vulnerabilidades y situaciones de abusos/ataques, las organizaciones deberían participar en foros de comunidades o industrias pertinentes para compartir sus buenas prácticas y aprender de los colegas proveedores.

11.4.3 Requisitos de seguridad para el alojamiento Web y otros servicios de ciber-aplicación

Muchos proveedores de servicios proveen servicios de hosting en sus redes y centros de datos como parte de sus servicios comerciales. Estos servicios, que incluyen sitios Web y otras aplicaciones online, en ocasiones son re-empaquetados y re-vendidos por los suscriptores de hosting a otros consumidores, como pequeños negocios y usuarios finales. Si los suscriptores de hosting establecen un servidor inseguro, o alojan contenidos maliciosos en sus sitios o aplicaciones, la seguridad de los consumidores se verá afectada de manera adversa. Debido a esto, es importante que los servicios, como mínimo, cumplan con estándares de buenas prácticas al seguir con la política o los términos de acuerdos.

En el caso de usar múltiples proveedores, se debería analizar la interacción entre los proveedores y los acuerdos de servicio deberían abordar cualquier interacción crítica. Por ejemplo, las actualizaciones o parches para los sistemas de un proveedor se debería coordinar con otros proveedores, ya que dicha actualización podría derivar en una interacción negativa.

Los términos de acuerdos deberían al menos cubrir los elementos siguientes:

a) Notificaciones Claras que describan las prácticas de seguridad y privacidad del sitio online o aplicación, las prácticas de recolección de datos y el comportamiento de cualquier código (por ejemplo, un Objeto Ayudante del Navegador) que el sitio online o aplicación puede distribuir y ejecutar en el escritorio de los usuarios finales, en los entornos de navegadores Web.

b) El Consentimiento del Usuario para facilitar el acuerdo o desacuerdo del usuario con los términos de los servicios descritos en las Notificaciones. Esto le permitirá al usuario tener prudencia y determinar si puede aceptar los términos de servicios en conformidad.

c) Controles de Usuario, para facilitar que los usuarios cambien sus configuraciones o, de otra forma, terminar su aceptación en cualquier momento, en el futuro, después del acuerdo inicial.

Las condiciones son importantes para asegurar que los usuarios finales tengan claridad con respecto al comportamiento y prácticas de la aplicación o sitio online, en relación a la privacidad y seguridad de los usuarios finales. Las condiciones se deben desarrollar con la ayuda de un profesional legal para asegurarse de que éstos además indemnizarán al proveedor de servicios por las potenciales acciones legales que pueden tomar los usuarios finales como resultado de pérdidas específicas o daños ocurridos debido a contenidos maliciosos o políticas y prácticas no claras en el sitio Web.

Además de la protección de datos y las provisiones de privacidad personal en la aplicación o sitio online, los proveedores de servicios deberían requerir que las aplicaciones o sitios online alojados en sus redes implementen un conjunto de controles de seguridad de buenas prácticas a nivel de aplicación antes de lanzarse en funcionamiento. Estos deberían incluir, pero no están limitados a los ejemplos dados en 12.2.

Como parte de la infraestructura de hosting de un proveedor de servicios, los servidores se deben proteger contra los accesos no autorizados y de la habilidad de alojar contenidos maliciosos. Ver 12.3 para revisar ejemplos de controles.

Para permitir el reforzamiento de estos controles de seguridad, particularmente, aquellos relacionados con la seguridad de sitios online y aplicaciones, los proveedores de servicios deberían considerar la incorporación de estas provisiones en los términos de acuerdos de servicios.

11.4.4 Orientación de seguridad para los consumidores

Los proveedores de servicios deben otorgar una guía a los consumidores sobre cómo permanecer seguro online. Para los usuarios, los proveedores de servicios pueden crear una guía de manera directa o hacer referencia a los sitios con orientación disponible que puedan proporcionar los contenidos. Es de suma importancia educar a los usuarios finales sobre cómo ellos pueden contribuir a un Internet seguro en relación a los múltiples roles que éstos pueden tener en el Ciberespacio, como se describe en cláusula 7. Además, a los usuarios finales se les debería aconsejar para que tomen los controles de seguridad técnicos necesarios, acción en la cual los proveedores de servicios también tienen un rol activo, como se describe en 11.3. Ejemplos de actividades para entregar orientación:

a) Boletines informáticos de seguridad periódicos (por ejemplo, mensuales) sobre técnicas de seguridad específicas (por ejemplo, cómo elegir una buena contraseña), actualizaciones sobre las tendencias de seguridad y proveer notificaciones de webcasts de seguridad, otros videos on-demand, audios broadcasts e información de seguridad que estén disponibles desde el portal Web de la organizaciones u otros proveedores de contenido de seguridad.

b) Difusiones directas de videos on-demand de educación de seguridad o webcasts que cubran una variedad de temas de seguridad para mejorar las prácticas de seguridad y conciencia de los usuarios finales.

c) Incorporar una columna de seguridad en el boletín informativo impreso del proveedor de servicios que se envíe a las direcciones residenciales o laborales de los usuarios finales para destacar eventos o contenidos de seguridad claves.

d) Seminarios o exposiciones itinerantes sobre la seguridad de los usuarios finales de manera anual o periódica, posiblemente con la colaboración de otros agentes de la industria, vendedores y gobiernos.

Los proveedores de servicios que usen el correo electrónico como su medio primario para comunicarse con los usuarios finales, les deberían ayudar a resistir los ataques de ingeniería social. Particularmente, se les debería recordar a los usuarios finales que en los correos electrónicos no solicitados por parte del proveedor de servicios, nunca se solicitarán:

— información personal;

— nombres de usuario;

— contraseñas; y

— jamás incluirán links relacionados a la seguridad para que el lector les haga click.

Cuando un proveedor de servicios desea que un usuario vaya a su sitio online por información, éste le debe decir al usuario cómo conectarse de manera segura a la URL requerida. Por ejemplo, le puede pedir al usuario que escriba en su navegador una URL citada y asegurarse de que dicha URL no contenga un link clickleable.

Como parte de la educación y orientación en relación a la seguridad, hacia el usuario, en contra de softwares engañosos y spywares, las organizaciones y proveedores de servicios deberían aconsejar a sus usuarios finales sobre el uso de controles de seguridad técnicos adecuados para proteger sus sistemas contra abusos y ataques conocidos. Como guía general, se debería motivar a los consumidores a implementar los controles descritos en 12.4.

El Anexo B provee una lista ejemplo de referencias y recursos online que se podrían usar como apoyo para la implementación de las recomendaciones anteriores.

12 Controles de Ciberseguridad

12.1 Visión general

Una vez que se identifican los riesgos a la Ciberseguridad y se bosquejan las directrices apropiadas, se pueden seleccionar e implementar los controles de Ciberseguridad que apoyan a los requisitos de seguridad. Esta cláusula da una visión general de los controles clave de Ciberseguridad que se pueden implementar para apoyar las directrices especificadas en esta norma.

12.2 Controles a nivel de aplicación

Los controles a nivel de aplicación incluyen los siguientes:

a) Exponer notificaciones cortas con resúmenes claros, concisos y de una sola página (con un lenguaje simple) de las políticas online esenciales de la compañía. Mediante estas notificaciones, los usuarios pueden tomar decisiones más informadas acerca de compartir su información online. Estas notificaciones cortas deberían estar en conformidad con todos los requisitos normativos y proveer links a declaraciones completas y otra información relevante, para que los consumidores que quieran más detalles puedan hacer click fácilmente para leer la versión completa. Con una sola notificación, los consumidores pueden tener un acercamiento más consistente acerca los bienes de la compañía, con los mismos estándares y expectativas de privacidad, que se extienden a numerosos sitios.

b) Asegurar el manejo de sesiones para las aplicaciones Web. Esto puede incluir mecanismos online como cookies.

c) Asegurar la validación y manejo de las entradas para prevenir ataques comunes, tales como la Inyección SQL. En base en que los sitios Web, los cuales en general se consideran como confiables, se están usando cada vez más para la distribución de códigos maliciosos, la validación de entrada y salida se debe realizar mediante un contenido activo y mediante un contenido dinámico.

d) Asegurar el scripting de la página Web para prevenir ataques comunes como las Secuencias de Ordenes en Sitios Cruzados o Cross-site Scripting.

e) Revisar y testear la seguridad de los códigos por medios de entidades cualificadas apropiadamente.

f) El servicio de la organización, ya sea provisto por la organización o por una parte que represente a la organización, se debería proveer de manera que el consumidor pueda autentificar dicho servicio. Esto puede incluir haciendo que el proveedor use un sub-dominio desde un nombre de dominio con marca registrada de la organización y posiblemente el uso de credenciales HTTPS registradas a nombre de la organización. El servicio debería evitar el uso de métodos engañosos donde los consumidores tengan dificultades para determinar con quien se está relacionando.

12.3 Protección del servidor

Los controles siguientes se pueden usar para proteger a los servidores contra accesos no autorizados y el hosting de contenido maliciosos en dichos servidores:

a) Configurar los servidores, incluyendo los sistemas operativos subyacentes, de acuerdo a una guía de configuración de seguridad base. Esta guía debería incluir una definición apropiada de los usuarios de los servidores versus los administradores, reforzar los controles de acceso en los directorios y archivos de programa y sistema y habilitar el registro de auditoría de, particularmente, la seguridad y otros eventos de fallas en el sistema. Es más, se recomienda instalar un sistema mínimo en un servidor para reducir el vector de ataque.

b) Implementar un sistema para probar e implementar actualizaciones de seguridad y asegurarse de que el sistema operativo y aplicaciones del servidor se mantengan actualizados rápidamente cuando estén disponibles nuevas actualizaciones de seguridad.

c) Realizar seguimiento del desempeño de seguridad del servidor a través de revisiones constantes de los registros de auditoría.

d) Revisar la configuración de seguridad.

e) Ejecutar controles anti software malicioso (como spyware o malware) en el servidor.

f) Escanear todo el contenido alojado y subido, de manera regular, usando controles actualizados anti software malicioso. Reconocer que un archivo puede, por ejemplo, aún ser un spyware o malware si no se detecta con los controles actuales debido a limitaciones o a información incorrecta.

g) Realizar evaluaciones de vulnerabilidades y pruebas de seguridad de manera constante para aplicaciones y sitios online para asegurase de que se mantiene su seguridad de manera adecuada.

h) Hacer escaneos constante en busca de compromisos.

12.4 Controles para los usuarios finales

La siguiente es una lista incompleta de controles que los usuarios finales pueden usar para proteger sus sistemas contra ataques y abusos conocidos:

a) Usar sistemas operativos compatibles con los parches de seguridad más actualizados que han sido instalados. Los consumidores organizacionales tienen una responsabilidad de estar conscientes de, y seguir, una política organizacional relacionada a los sistemas operativos compatibles. Los consumidores individuales deberían estar conscientes de, y considerar el uso, sistemas operativos recomendados por el proveedor. En todos los casos, el sistema operativo se debería actualizar con respecto a los parches de seguridad.

b) Usar las últimas aplicaciones de software compatibles con los parches más actualizados instalados. Los consumidores organizacionales tienen una responsabilidad de estar consiente de, y seguir, una política organizacional relacionada a los sistemas operativos compatibles. Los consumidores individuales deberían estar conscientes de, y considerar el uso, de sistemas operativos recomendados por el proveedor. En todos los casos, el software de aplicación se debería actualizar con respecto a los parches de seguridad.

c) Usar herramientas anti-virus y anti-spywares. Si es factible, un proveedor de servicios como un ISP debería considerar trabajar en conjunto con vendedores de seguridad confiables, para ofrecerle a los usuarios finales dichas herramientas como parte del paquete de suscripción al servicio, para que los controles de seguridad estén disponibles luego de registrar la suscripción o luego de su renovación. Los consumidores organizacionales tienen la responsabilidad de estar consciente de, y seguir, una política organizacional relacionada al uso de herramientas de software de seguridad. Los consumidores individuales deberían usar las herramientas de software de seguridad. Estos se deberían dirigir al proveedor por cualquier software de seguridad recomendado, provisto o discontinuado. En todos los casos, el software de seguridad se debería actualizar con respecto a los parches de seguridad y a las bases de datos de firmas.

d) Implementar dispositivos de seguridad anti-virus y anti-spywares apropiados. Los navegadores Web y barras de herramientas de navegador comunes incorporan actualmente capacidades como bloqueadores de pop-ups que evitan que sitios Web maliciosos muestren ventanas que contienen spywares o softwares engañosos que puedan abusar de las debilidades del sistema o navegador o usar la ingeniería social para engañar a los usuarios para que los descarguen e instalen en sus sistemas. Las organizaciones deberían establecer una política para habilitar el uso de dichas herramientas. Las organizaciones proveedoras de servicios deberían recopilar una lista de herramientas recomendadas y se debe fomentar su uso entre los usuarios finales, con una orientación sobre sus habilitaciones y permisos concedidos para los sitios Web a los que los usuarios desearían acceder.

e) Habilitar bloqueadores de script. Habilitar bloqueadores de script o una configuración de seguridad Web más alta para asegurarse de que sólo se ejecuten en un computador local los scripts que provengan de fuentes confiables.

f) Usar filtros de suplantación de identidad. Los navegadores Web y barras de herramientas de navegador comunes suelen incorporar esta capacidad, la que podría determinar si el sitio que está visitando el usuario se encuentra en una base de datos de sitios Web de suplantación de identidad conocidos, o si contiene patrones de script que sean similares a aquellos que se consideren como típicos sitios de suplantación de identidad. El navegador podría proveer alertas, normalmente en forma de resaltos codificados con color, para advertir a los usuarios del potencial riesgo. Las organizaciones deberían establecer una política para habilitar el uso de dicha herramienta.

g) Usar otros elementos de seguridad disponibles, para los navegadores Web. Constantemente, a medida que surgen nuevos riesgos de Ciberseguridad, los proveedores de navegadores Web y de barras de herramientas de navegador agregan nuevas capacidades de seguridad para proteger a los usuarios en contra de riesgos. Los usuarios finales se deberían mantener actualizados acerca de estos desarrollos, al aprender acerca de dichas actualizaciones que son provistas normalmente por los proveedores de herramientas. Las organizaciones y proveedores de servicios deberían revisar de manera similar estas nuevas capacidades y actualizar las políticas y servicios pertinentes para cumplir de mejor manera las necesidades de sus organizaciones y consumidores, así como abordar los riesgos relacionados a la Ciberseguridad.

h) Habilitar un firewall y un HIDS personales. Los firewalls y HIDS personales son herramientas importantes para controlar los servicios de red que acceden al sistema de un usuario. Varios sistemas operativos nuevos tienen firewalls y HIDS personales incorporados. Si bien estos elementos están habilitados de manera predeterminada, los usuarios o aplicaciones pueden inhabilitarlos, lo que conlleva a exposiciones no deseadas de la seguridad de la red. Las organizaciones deberían adoptar una política sobre el uso de un firewall y un HIDS personales y evaluar herramientas o productos adecuados para implementar que se habilite su uso por defecto a todos los empleados. Los proveedores de servicios deberían fomentar el uso de funciones de firewall y HIDS personales y/o sugerir otros productos de firewall y HIDS personales de terceros que han sido evaluados y considerados como confiables, además de educar y ayudar a los usuarios a habilitar una seguridad de red básica a nivel de sistema de usuario final.

i) Habilitar actualizaciones automáticas. Si bien los controles de seguridad técnicos descritos anteriormente son capaces de lidiar con la mayoría de los softwares maliciosos en sus respectivos niveles operacionales, éstos no son muy efectivos en contra del abuso de vulnerabilidades que existen en los productos de sistemas operativos y aplicaciones. Para prevenir dichos abusos, la función de actualización disponible en los sistemas operativos, así como aquellas provistas por las aplicaciones en las que confían los usuarios (por ejemplo, productos anti-spyware y anti-virus evaluados por terceros confiables) se deberían habilitar para que realicen actualizaciones automáticas. Esto asegurará que los sistemas se actualicen con los últimos parches de seguridad cada vez que estén disponibles, cerrando la brecha de tiempo para que se lleven a cabo los abusos.

12.5 Controles contra los ataques de ingeniería social

12.5.1 Visión general

Los Cibercriminales recurren cada vez más a tácticas psicológicas o de ingeniería social para tener éxito.

EJEMPLO 1 El uso de correos electrónicos que contienen un URL que dirige a los usuarios desprevenidos a sitios Web de suplantación de identidad.

EJEMPLO 2 Correos electrónicos fraudulentos que le piden a los usuarios dar su información de identificación personal o información relacionada a propiedad intelectual corporativa.

La proliferación de las redes sociales y los sitios de comunidad provee nuevos vehículos que habilitan aún más la realización de fraudes y estafas insólitas. De manera creciente, dichos ataques también están trascendiendo la tecnología, más allá de los sistemas de PC y de la conectividad de red tradicional, aprovechando el uso de teléfonos móviles, redes inalámbricas (incluyendo Bluetooth) y Voz sobre IP (VoIP).

Esta cláusula provee un marco de controles aplicable para gestionar y minimizar los riesgos de Ciberseguridad en relación a los ataques de ingeniería social. La orientación provista en esta cláusula se basa en la noción de que la única forma eficaz de mitigar la amenaza de ingeniería social es través de la combinación de:

— tecnología de seguridad;

— políticas de seguridad que establezcan reglas básicas para el comportamiento personal, tanto como individuo como en forma de empleado; y

— una educación y formación apropiadas.

Por lo tanto, el marco de trabajo abarca:

— políticas;

— métodos y procesos;

— personas y organizaciones; y

— controles técnicos aplicables.

12.5.2 Políticas

En la misma línea de las prácticas comunes para la gestión de riesgos de seguridad de la información, se deberían determinar y documentar políticas básicas que gobiernen la creación, recopilación, almacenamiento, transmisión, intercambio, procesamiento y uso general de la información personal y organizacional y de la propiedad intelectual en Internet y en el Ciberespacio. Particularmente, esto se relaciona con las aplicaciones como la mensajería instantánea, el blogging, el intercambio de archivos P2P y las redes sociales, las que normalmente están más allá del alcance de la red empresarial y la seguridad de la información.

Como parte de las políticas corporativas, declaraciones y sanciones relacionadas al mal uso de las aplicaciones del Ciberespacio se deberían también incorporar, para disuadir las prácticas de mal uso por parte de los empleados y terceros en las redes corporativas o sistemas que acceden al Ciberespacio.

Se deberían desarrollar y publicar políticas administrativas que promuevan la conciencia y entendimiento de los riesgos de Ciberpseguridad y fomentar, u obligar, el aprendizaje y desarrollo de competencias en contra de ataques de Ciberseguridad, particularmente, de ataques de ingeniería social. Esto debería incluir requisitos para la asistencia constante a sesiones informativas y capacitaciones.

Al promover políticas y una conciencia adecuadas sobre los riesgos de ingeniería social, los empleados ya no se pueden declarar ignorantes frente a dichos riesgos y requisitos y, al mismo tiempo, sobre el desarrollo del entendimiento de las buenas prácticas y políticas esperadas de las redes sociales externas y otras aplicaciones del Ciberespacio, por ejemplo, el acuerdo de política de seguridad del proveedor de servicios.

12.5.3 Métodos y procesos

12.5.3.1 Categorización y clasificación de la información

Para apoyar las políticas para promover una conciencia y protección de la información corporativa clasificada y sensible personal, incluyendo las propiedades intelectuales, se deberían implementar procesos para la categorización y clasificación de la información.

Para cada categoría y clasificación de la información involucrada, se deberían desarrollar y documentar controles de seguridad específicos para la protección contra la exposición accidental y el acceso no autorizado intencional.

Los usuarios en las organizaciones podrían de esta manera hacer la diferencia entre las diferentes categorías y clasificación de la información que generan, recolectan y manejan. Los usuarios pueden así ejercer la precaución necesaria y hacer uso de los controles protectores cuando utilicen el Ciberespacio.

También se deberían desarrollar y publicar procedimiento de cómo manejar las propiedades intelectuales de una compañía, los datos personales y otra información confidencial.

12.5.3.2 Conciencia y formación

La conciencia y formación de seguridad, incluyendo la actualización constante de conocimientos y aprendizajes pertinentes, son elementos importantes para contrarrestar ataques de ingeniería social.

Como parte del programa de Ciberseguridad de una organización, a los empleados y subcontratistas se les debería requerir que cursen un número mínimo de horas de formación para asegurar que estén conscientes de sus roles y responsabilidades en el Ciberespacio, además de los controles técnicos que éstos deberían implementar como individuos al usar el Ciberespacio. Además, como parte del programa para contrarrestar los ataque de ingeniería social, dicha formación debería incluir contenidos como los siguientes:

a) Las últimas amenazas y formas de ataques de ingeniería social, por ejemplo, cómo ha evolucionado la suplantación de identidad desde los sitios Web falsos hasta una combinación de Spams, Cross Site Scripting y ataques de Inyección SQL.

b) Cómo la información individual y corporativa se puede robar y manipular a través de ataques de ingeniería social, otorgando un entendimiento de cómo los atacantes se pueden aprovechar de la naturaleza humana, cómo lo es la tendencia a estar de acuerdo con las peticiones hechas con autoridad (aunque ésta pueda ser falsa), conductas amigables, presentarse como víctima y la reciprocidad entregando algo de valor o prestar ayuda.

c) Qué información necesita estar protegida y cómo protegerla, de acuerdo con la política de seguridad de la información.

d) Cuándo informar o escalar un evento sospechoso o aplicación maliciosa para dirigirse a las autoridades u organismo de respuesta, y la información disponible sobre estos contactos. Por ejemplo, ver Anexo B.

Las organizaciones que proveen aplicaciones y servicios online en el Ciberespacio deberían proveer materiales que cubran los contenidos anteriores dentro del contexto de sus aplicaciones o servicios, para promover la conciencia entre los suscriptores o consumidores.

12.5.3.3 Pruebas

Los empleados deberían firmar una aceptación de que ellos aceptan y entienden los contenidos de la política de seguridad de la organización. Como parte del proceso para mejorar la conciencia y asegurar que se preste atención a los riesgos, una organización debería considerar la ejecución de pruebas periódicas para determinar el nivel de conciencia y conformidad con las políticas y prácticas pertinentes. Los empleados pueden contestar una prueba escrita o cursar una CBT para determinar si entienden los contenidos de las políticas de seguridad de la organización. Dichas pruebas pueden incluir, pero no se limitan a, la creación de sitios dirigidos y controlados de suplantación de identidad, Spams y correos electrónicos fraudulentos, usando contenidos de ingeniería social verosímil. Al conducir dichas pruebas, es importante asegurarse de que:

a) los servidores y contenidos de prueba estén todos dentro del control y comando del equipo de prueba;

b) se involucren, si es posible, a profesionales que tienen experiencia previa en la conducción de dichas pruebas;

c) los usuarios estén preparados para dichas pruebas por medio de programas de conciencia y formación; y

d) se presenten todos los resultados en un formato global, para proteger la privacidad de un individuo, puesto que el contenido presentado en dichas pruebas puede avergonzar a los individuos y causar preocupaciones sobre la privacidad, si es que no se maneja adecuadamente.

NOTA Se puede tener en consideración la ética y la legislación de cada país.

12.5.4 Personas y organización

Si bien los individuos son los primeros blancos de los ataques de ingeniería social, una organización también puede ser una potencial víctima. Sin embargo, las personas siguen siendo el punto de entrada principal para los ataques de ingeniería social. Como tal, las personas necesitan estar conscientes de los riesgos relacionados en el Ciberespacio, y las organizaciones deberían establecer políticas pertinentes y dar pasos proactivos para patrocinar programas relacionados para asegurar la conciencia y competencia de las personas.

Como guía general, todas las organizaciones (incluyendo empresas, proveedores de servicios y gobiernos) deberían motivar a los consumidores en el Ciberespacio a aprender y entender los riesgos de ingeniería social en el Ciberespacio y los pasos que deberían dar para protegerse a sí mismos contra ataques potenciales.

12.5.5 Técnicos

Además de establecer políticas y prácticas en contra de ataques de ingeniería social, se deberían considerar también controles técnicos y, donde sea posible, adoptarlos para minimizar la exposición y potencial de abusos por parte de ciber malhechores.

En el nivel del personal, los usuarios del Ciberespacio deberían adoptar la guía analizada en 11.3.

Las organizaciones y los proveedores de servicios deberían dar los pasos relevantes descritos en 11.4.4, para facilitar la adopción y uso, por parte de los usuarios, de los controles técnicos de seguridad.

Las organizaciones y proveedores de servicios también debería adoptar las guías provistas en 11.4, las que son importantes como controles básicos en contra de los ataques de ingeniería social en el Ciberespacio.

Además, se deberían considerar los siguientes controles técnicos, útiles en contra de ataques específicos de ingeniera social:

a) Cuando hay información sensible personal o corporativa involucrada en aplicaciones online, se debe considerar la provisión de soluciones de autenticación sólidas, ya sea como parte de la autenticación de acceso y/o cuando se ejecuten transacciones críticas. Una sólida autenticación se refiere al uso de dos o más factores adicionales de verificación de identidad sobre o más allá del uso del ID y contraseña de un usuario. El segundo factor y los factores adicionales pueden ser provistos utilizando una tarjeta inteligente, tokens biométricos u otros tokens de seguridad de mano.

b) Para los servicios basados en Web, las organizaciones deberían considerar usar un “Certificado de Alta Seguridad” para proporcionar una seguridad adicional a los usuarios online. Muchas Autoridades Comerciales (CA) y navegadores de Internet son capaces de soportar el uso de dichos certificados, lo que reduce la amenaza de ataques de suplantación de identidad.

c) Para garantizar la seguridad de los computadores de los usuarios que se conectan al sitio o aplicación de la organización, o del proveedor de servicios en el Ciberespacio, se deberían considerar controles adicionales para asegurar un nivel mínimo de seguridad, tales como la instalación de las últimas actualizaciones de seguridad. El uso de dichos controles se debería publicar en el Acuerdo de Servicios de los Usuarios Finales y/o en la Política de Seguridad y Privacidad del Sitio, según proceda.

12.6 Disposición de la Ciberseguridad

El Anexo A describe controles técnicos adicionales que se pueden aplicar para mejorar la disposición en el área de detección de eventos, a través de una Darknet para Seguimiento; la investigación, a través de Tracebacks; y la respuesta, a través de una Operación Sinkhole, como parte de la Ciberseguridad de una organización.

12.7 Otros controles

Otros controles pueden incluir algunos relacionados a la alerta y cuarentena de dispositivos que están comprometidos en actividades sospechosas u observadas, a través de la correlación de eventos desde los elementos del proveedor de servicios y/o empresa como los servidores DNS, el flujo de red de router, la filtración de mensajes salientes y las comunicaciones peer-to-peer.

13 Marco del intercambio y coordinación de información

13.1 General

Los incidentes de Ciberseguridad a menudo cruzan las fronteras geográficas y organizacionales nacionales y la velocidad del flujo y de los cambios de información, desde el despliegue del incidente, suele dar un tiempo limitado para que los individuos y organizaciones que responden, puedan actuar. Un sistema necesita estar establecido para el intercambio y coordinación de información para ayudar a la preparación y respuesta ante eventos e incidentes de Ciberseguridad. Este es un paso importante que las organizaciones deberían dar como parte de sus controles de Ciberseguridad. Este sistema de intercambio y coordinación de información debería ser seguro, eficaz, confiable y eficiente.

El sistema debería ser seguro, para asegurar que la información que está siendo intercambiada, incluyendo detalles sobre la coordinación de actividades, protección en contra de accesos no autorizados, particularmente por parte del perpetrador del incidente. La seguridad de la información relacionada a eventos de Ciberseguridad, también es necesaria para prevenir interpretaciones erróneas y causar pánico excesivo o alarmas en el público. Al mismo tiempo, la integridad y autenticidad de la información son cruciales para asegurar su exactitud y confiabilidad, independientemente si dicha información se comparte en un grupo cerrado o se divulga públicamente. El sistema debería ser eficaz y eficiente para que cumpla su propósito con recursos mínimos y dentro del tiempo y espacio requeridos.

Esta cláusula provee un básico marco de trabajo, con el objeto de implementar un sistema para el intercambio y coordinación de información. El marco incluye cuatro áreas para considerar, específicamente, políticas, métodos y procesos, personas y elementos técnicos.

NOTA La Comisión de Estudio 17 del UIT-T está llevando a cabo un trabajo exhaustivo acerca del intercambio de información de Ciberseguridad. Para más información, ver Tabla C.17 Intercambio de información de Ciberseguridad.

13.2 Políticas

13.2.1 Organizaciones proveedoras de información y organizaciones receptoras de información

Para el propósito de este marco de trabajo, se introducen dos tipos de organizaciones de intercambio de información:

— Organizaciones proveedoras de información[11]; y

— Organizaciones receptoras de información[12].

En el caso de una IPO, se deben determinar las políticas básicas con respecto a la clasificación y categorización de la información, la gravedad de los eventos e incidentes y la forma de intercambio posible se antes de la ocurrencia de cualquier incidente de Ciberseguridad o antes de realizar cualquier intercambio (en el caso de que una IPO se convierta en una IRO, para compartir la información recibida con otras entidades autorizadas en la cadena de información).

En el terminal de recepción, la IRO debería estar de acuerdo con reforzar la protección de seguridad y los procedimientos relevantes, luego de recibir información de la IPO, en conformidad con el acuerdo alcanzado previamente y en base a la clasificación y categorización de la información involucrada.

13.2.2 Clasificación y categorización de la información

Las IPOs deberían determinar las diferentes categorías de la información que recolectan, recopilan, mantienen a salvo y distribuyen. Algunos ejemplos de categorías de información pueden incluir eventos de seguridad, amenazas de seguridad, vulnerabilidades de seguridad, perfiles de perpetradores sospechosos/confirmados, grupos organizados, información de víctimas y categorías de perfiles de sistemas TIC.

Cada categoría se debería dividir en dos o más clasificaciones, basadas en los contenidos de la información involucrada. La clasificación mínima puede ser sensible y sin restricciones. Si la información contiene datos personales, también se puede aplicar a las clasificaciones de privacidad.

11 En inglés: *IPOs, Information Providing Organization*.

12 En inglés: *IROs, Information Receiving Organization.*

13.2.3 Minimización de la información

Para cada categoría y clasificación, una IPO debería tomar las precauciones para minimizar la información que se distribuirá. La minimización es necesaria para prevenir la sobrecarga de información en el terminal de recepción y asegurar un uso eficiente del sistema de intercambio, sin comprometer su eficacia. Otro objetivo de la minimización es omitir la información sensible para preservar la privacidad de las personas en una IPO e IRO. Con respecto a esto, las IPOs e IROs deberían determinar el nivel deseado de detalles, en la medida de lo posible, para cada categoría y clasificación de información que pueda ser identificada antes de realizar el intercambio.

13.2.4 Audiencia limitada

En concordancia con el principio de minimización, es necesario contar con una política para limitar la audiencia, que puede ser una persona de contacto específico, grupo u organización, para la distribución cuando se comparta la información que contenga datos privados o confidenciales. En el caso de la información menos sensible, se debe considerar una política para prevenir la sobrecarga de información, a menos que los beneficios de la distribución máxima (como el intercambio de alertas de seguridad críticas) sopesen el impacto de la sobrecarga de información para la IRO.

13.2.5 Protocolo de coordinación

Se debería establecer una política de alto nivel para coordinar la petición y distribución (ya sea iniciadas por una IPO o una IRO). Tal política formaliza el protocolo involucrado, el cual provee los medios para que la IPO y la IRO respondan de manera eficaz y eficiente. Se podrían, entonces, construir procedimientos de autenticación y verificación mutuos sobre dicho protocolo, para asegurar la autenticidad de origen y el comprobante de entrega donde se desee, particularmente, para la información sensible, personal y/o confidencial.

13.3 Métodos y procesos

13.3.1 Visión general

Se deberían desarrollar e implementar métodos y procesos relacionados, para ejecutar las políticas de intercambio de información y asegurar la consistencia de la práctica y la eficacia, eficiencia y confiabilidad de ejecución. Estos métodos y procesos se deberían basar en estándares válidos. En caso contario, en la validación operacional, éstos se pueden formalizar para su estandarización. Las siguientes cláusulas proveen una orientación sobre los métodos y procesos que usan comúnmente las organizaciones en la industria para lograr los objetivos y políticas relevantes de intercambio y coordinación de información, en el contexto de la Ciberseguridad.

13.3.2 Clasificación y categorización de la información

La información que será compartida provendrá tanto de fuentes abiertas como cerradas. La información de fuente abierta se suele encontrar en Internet o en otras fuentes públicas, como diarios. La información de fuente abierta pertenece generalmente a la clasificación más baja, puesto que los que originan dicha información pueden ser múltiples o desconocidos, la antigüedad de la información se puede indeterminar y se puede cuestionar su precisión. La información de fuente cerrada no está disponible públicamente y se atribuye normalmente a una fuente y tiene una antigüedad reconocible. Algunos ejemplos de información de fuente cerrada incluyen investigaciones y análisis patentados y la inteligencia recolectada empíricamente.

NOTA La orientación para esta cláusula puede estar basada en el resultado del Período de Estudio en este tópico, haciendo referencia al estándar si el SP procede a realizar un desarrollo, o adopta un resumen del texto del SP si éste termina sin desarrollo adicional.

13.3.3 Acuerdo de no divulgación

Un NDA se puede usar para al menos dos propósitos en el contexto del intercambio y coordinación de información para mejorar la Ciberseguridad. Un uso típico de un NDA es asegurar el manejo y protección adecuados de información sensible, personal y/confidencial compartida entre una IPO y una IRO, y pre-establecer la condición de dicho intercambio y la distribución y uso posteriores de dicha información.

En el contexto de responder a los eventos de Ciberseguridad, el preestablecimiento de un NDA permite un rápido intercambio y distribución entre las entidades autorizadas, para que se lleven a cabo de manera eficiente, incluso si la clasificación de la información no se ha definido claramente.

13.3.4 Código de práctica

Un método comúnmente usado para asegurar el intercambio y el manejo adecuados de información sensible, es establecer un código de práctica que cubra procedimientos detallados, responsabilidades y compromisos de las organizaciones, parte interesada (es decir, IPOs e IROs) para las respuestas y acciones que serán llevadas a cabo por las entidades respectivas involucradas, para cada categoría y clasificación de la información.

EJEMPLO Ver la futura norma ISO/IEC 29147.

13.3.5 Pruebas y simulacros

Para asegurar la eficacia y confiabilidad y para lograr el nivel deseado de eficiencia, se deberían desarrollar métodos y procesos para conducir pruebas constantes y ejercitar supuestos y simulacros.

Se debería usar una metodología estándar como referencia para las pruebas de seguridad con el fin de adaptarla para que se ajuste a las metas y necesidades de la organización.

Las pruebas de seguridad se pueden realizar en activos de alto riesgo. Esto se puede ejecutar mediante el uso de la propia nomenclatura de clasificación de datos de la organización.

Las evaluaciones de seguridad se deberían realizar constantemente en los elementos siguientes:

— Aplicación.

— Sistema Operativo.

— Sistema de Gestión de la Base de Datos.

13.3.6 Coordinación del tiempo y programación para el intercambio de información

El requisito para compartir información, tanto de manera proactiva como durante una respuesta ante un incidente, variará de entidad a entidad. Algunas organizaciones tendrán requisitos para la información en tiempo real: en el momento en que una alerta o alarma ocurre, desearán que la inteligencia realice un análisis detallado. Otras entidades no tendrán los recursos para gestionar el intercambio de información en tiempo real. Es más, muchas organizaciones pueden carecer de la habilidad de gestionar un intercambio de información programado en cualquier intervalo.

La coordinación del tiempo y programación del intercambio de información se debería establecer de manera clara, con objetivos específicos a nivel de servicios, definidos para relaciones voluntarias y acuerdos a nivel de servicios para relaciones comerciales.

13.4 Personas y organizaciones

13.4.1 Visión general

Las personas y las organizaciones son los determinantes clave para el éxito de la Ciberseguridad. Las personas se refieren a los individuos involucrados en la ejecución de métodos y procesos para el intercambio y coordinación de información con el fin de influir de manera positiva en los resultados de los eventos de Ciberseguridad. Las organizaciones se refieren a los grupos de personas en una compañía, incluso la compañía completa, involucrados en dichas actividades. Para lograr la eficacia y eficiencia, se deben considerar las necesidades tanto de las personas como de las organizaciones.

13.4.2 Contactos

Se debe compilar una lista de contactos por parte de la IPO y de la IRO, la que se debe intercambiar de manera mutua para que cada entidad pueda identificar a la persona que requirió o envió información en la comunidad de intercambio.

También se pueden desarrollar y compartir listas de contactos más detalladas en conformidad con una audiencia limitada (ver 13.2.4) y políticas de clasificación y categorización de información (ver 13.2.2).

La lista de contactos no debería incluir información personal sensible, en conformidad con la política de minimización de información (ver 13.2.3). Para propósitos de la privacidad, se puede considerar un alias en vez de un nombre completo. La información mínima para la lista de contactos debería incluir nombre (o alias), números de contacto (número de teléfono móvil, si es posible) y dirección de correo electrónico. También se puede establecer un contacto alternativo para cada persona clave en la lista de contactos.

Además de una lista de contactos para el intercambio y coordinación de información, se puede compilar una lista de contactos separada para la priorización de incidentes con tal de facilitar el escalado rápido. Una lista como esa suele incluir contactos externos que no están en la red de intercambio. Por ejemplo, ver Anexo B.

Como mínimo, la lista de contactos debería estar protegida contra modificaciones no autorizadas para prevenir una corrupción y mantener su integridad. Se deben aplicar controles técnicos (ver 13.5), si es apropiado.

13.4.3 Alianzas

Para facilitar el intercambio de información y establecer prácticas comunes y consistentes regidos por un código de prácticas acordado y/o un NDA, las organizaciones y grupos de individuos deben formar alianzas basadas en sus áreas de interés, como la industria, tecnología u otras áreas de interés especiales. Ver Anexo B para una lista de muestra de alianzas existentes y organizaciones sin fines de lucro que sirve para dicho propósito.

13.4.4 Conciencia y formación

Las personas en las organizaciones deberían estar conscientes de los nuevos y emergentes riesgos de Ciberseguridad y estar capacitadas para que desarrollen las competencias y experticias requeridas para responder eficaz y eficientemente cuando se encuentren con riesgos específicos, o reciban información que requiera sus acciones para mitigar o mejorar alguna situación. Para lograr estos objetivos, se requiere:

— Realizar sesiones informativas sobre el estado y descubrimientos de riesgos de Ciberseguridad que le conciernan a la organización y a la industria.

— Diseñar, organizar y entregar sesiones de formación enfocadas en escenarios simulados de Ciber-ataques y talleres sobre áreas de acción específicas, requeridas para los nuevos miembros del grupo/organización, con actualizaciones regulares.

— Pruebas constantes con tutoriales de supuestos o escenarios relevantes, para asegurar un entendimiento y habilidad con el fin de ejecutar procedimientos y herramientas específicas.

Estas acciones de conciencia, formación y prueba se pueden realizar por expertos internos involucrados, consultores externos u otros expertos de miembros de las alianzas relacionadas involucradas en los esfuerzos de intercambio y coordinación de información.

El uso de supuestos como parte de los procesos de formación y testeo, es considerablemente recomendado, puesto que un enfoque como este le permite a los individuos tener una experiencia cercana a la vida real de situaciones relevantes, y aprender y practicar las respuestas requeridas. Además, se pueden usar incidentes pasados como parte de los supuestos, para maximizar el intercambio de lecciones aprendidas y la comprensión adquirida, de dichas situaciones.

13.5 Técnicos

13.5.1 Visión general

Se pueden usar controles técnicos y una estandarización para mejorar la eficiencia, reducir los errores humanos y fortalecer la seguridad involucrada en los procesos de intercambio y coordinación de información. Se puede diseñar, desarrollar e implementar un número de sistemas y soluciones técnicos. Esta norma provee algunos de los enfoques y técnicas usados comúnmente que han adoptado algunas organizaciones, y que se pueden adaptar posteriormente para mejorar las necesidades y procesos de intercambio y coordinación de información para lidiar con el entorno cambiante de riesgos de Ciberseguridad.

13.5.2 Estandarización de los datos para un sistema automatizado

Como parte de la red de intercambio, se pueden desarrollar e implementar sistemas automatizados entre las organizaciones coordinadas, con el fin de recolectar datos en los eventos en evolución de la Ciberseguridad, para evaluar y analizar en tiempo real y offline, con tal de determinar el estado de seguridad actual en el Ciberespacio dentro del límite de las organizaciones involucradas. Dichos datos pueden incluir datos del tráfico de la red, actualizaciones de seguridad para los sistemas de software y los dispositivos de hardware, datos de vulnerabilidades de seguridad y datos de malwares, spam y spyware, incluyendo las cargas e información interceptada. Los sistemas automatizados que apoyan a los primeros intervinientes y al escalado de incidentes, como se describe en 13.4.2, también podrían contener datos relacionados a las organizaciones y personas. En vista de la sensibilidad y volumen de los contenidos de los datos involucrados en estos sistemas, las organizaciones (particularmente, las alianzas de organizaciones) deberían evaluar el esquema y contenidos de los datos para determinar controles técnicos apropiados para mejorar la eficiencia, eficacia y seguridad. Estos pueden incluir, pero no se limitan a, los siguientes:

a) la estandarización del esquema de datos para cada categoría y clasificación de datos recolectados, reforzando la minimización de información y la política de privacidad y proporcionando una seguridad técnica a todas las entidades y dueños de información participantes de dicha práctica;

b) la estandarización del formato de los datos para facilitar el intercambio y mejorar el almacenamiento, transmisión, manejo e interoperabilidad entre los sistemas, por ejemplo, ver ITU-T X.1205; y

c) la estandarización de la funcionalidad y algoritmos de procesamiento de datos utilizados, por ejemplo, una función y procedimientos hash para el anonimato de dirección IP y otros requisitos de pre-procesamiento.

13.5.3 Visualización de datos

Se debe considerar el uso de técnicas de visualización de datos, para presentar la información de los eventos, lo que ayuda a mejorar la visibilidad de los cambios y del incidente de seguridad emergente que en desarrollo, sin la necesidad de que los operadores lean los detalles de cada evento en el momento en que emergen. Por ejemplo, ver Anexo A que presenta una representación visual de actividades de Darknet, las que facilitan una repuesta más eficiente ante los cambios.

13.5.4 Intercambio de claves criptográficas y respaldos de software/hardware

Para facilitar el intercambio de información confidencial, se debe considerar implementar un sistema criptográfico, incluyendo un sistema para el intercambio de claves que se podría implementar rápidamente. El sistema debería incluir respaldos adecuados para el software y hardware, así como las claves usadas en la preparación para propósitos de intercambio y necesidades de recuperación de emergencia.

13.5.5 Seguridad en el intercambio de archivos, mensajería instantánea, portal Web y foro de discusión

Para facilitar la interacción online y un intercambio de información seguro y rápido, el que puede incluir el intercambio de contenidos digitales como archivos de texto y multimedia, además de discusiones tanto online como offline, las organizaciones que llevan a cabo estos intercambios (IPOs e IROs) deberían considerar herramientas adecuadas de intercambio de archivos, una mensajería instantánea y herramientas de foros de discusión online para que puedan cumplir con las necesidades de seguridad, eficacia, eficiencia y confiabilidad.

Se deberían implementar la transmisión del suministro de portal Web sobre los eventos y estatus de la Ciberseguridad como una forma de comunicación hacia la comunidad pública y la privada, interesadas e involucradas, respectivamente. Cuando se usa un portal Web, debería haber una propiedad y responsabilidad administrativas claras para asegurar su seguridad y disponibilidad. Además se deberían proveer áreas privadas para la información de una audiencia limitada, cuando sea necesario.

13.5.6 Sistemas de prueba

Si bien cada sistema técnico, y métodos y procesos relacionados se deberían testear de manera rigurosa para asegurar su confiabilidad e integridad, se deberían considerar uno o más sistemas técnicos dedicados a mejorar la eficiencia y eficacia de dicho testeo, particularmente, la prueba de supuestos. Dicho sistema puede tener la forma de un sistema de simulación para simular los entornos operativos como son percibidos por cada organización en el Ciberespacio, y la situación de la evolución de la Ciberseguridad, proporcionando la capacidad de introducir una serie de eventos de seguridad para facilitar la prueba requerida a realizar.

13.6 Guía de implementación

La implementación de este tipo de marco de trabajo requiere la colaboración de las organizaciones e individuos para que juntos (virtual o físicamente) determinen una política, controles y pasos específicos que llevar a cabo para lograr sus objetivos para un intercambio y coordinaciones de seguridad segura, eficaz, confiable y eficiente en respuesta a los incidentes emergentes de Ciberseguridad. Los siguientes pasos de alto nivel se recomiendan como una guía para implementación:

a) Identificar y recolectar organizaciones e individuos relevantes para formar la comunidad de red de intercambio y coordinación de información requerida, de manera tanto informal como formal.

b) Determinar el (los) rol(es) para cada organización/individuo involucrados tanto como una IPO, una IRO o ambas (ver 13.2.1).

c) Establecer el tipo de información y coordinación requeridas que podrían ser beneficiosas para la comunidad.

d) Realizar la categorización y clasificación de la información para determinar si hay información sensible y/o privada involucrada (ver 13.2.2).

e) Establecer políticas y principios que rijan a la comunidad y a la información involucrada (ver 13.2).

f) Determinar los métodos y procesos requeridos para cada categoría y clasificaciones de la información involucrada (ver 13.3).

g) Determinar los requisitos y criterios de desempeño y establecer un Código de Práctica y firmar un NDA, en caso de ser necesario (ver 13.3.3 y 13.3.4).

h) Identificar los estándares y sistemas técnicos requeridos y apropiados para apoyar la implementación y operaciones de la comunidad (ver 13.5).

i) Estar preparado para operar, recopilar la lista de contactos y conducir talleres de conciencia y formación para preparar a las partes interesadas.

j) Realizar pruebas contantes, incluyendo recorridos y simulación de supuestos, cuando sea necesario (ver 13.3.5 y 13.5.6).

k) Conducir revisiones post-pruebas y post-incidentes para mejorar los sistemas de intercambio y coordinación, incluyendo a las personas, procesos y tecnología involucrados. Si es necesario, se debe expandir o reducir el tamaño de la comunidad.

NOTA Las normas ISO/IEC 27001 e ISO/IEC 27003, proveen requisitos y una orientación de implementación respectivamente.

Anexo A
(informativo)

Disposición de la Ciberseguridad

A.1 Visión general

Los controles de Ciberseguridad descritos en cláusula 12 minimizan la exposición y los riesgos de las organizaciones y usuarios finales de los ataques de Ciberseguridad conocidos. Después que emergen incidentes de Ciberseguridad, el marco para el intercambio y coordinación de información descrito en cláusula 11 ayuda a establecer un sistema para el intercambio y coordinación de información con tal de prepararse para responder ante los eventos e incidentes de Ciberseguridad. Dicha información es protegida adecuadamente entre la IPO y la IRO.

Si bien estos controles reducen los riesgos y mejoran el manejo y gestión de incidentes, los ciber criminales u otros malhechores continuarán desarrollando nuevos ataques y evolucionando ataques existentes para superar las protecciones actuales. Por lo tanto, también es importante para las organizaciones implementar sistemas e infraestructuras que habiliten un enfoque más dinámico y riguroso para la detección, investigación y respuesta frente a ataques de seguridad.

La norma ISO/IEC 27031 provee una orientación sobre los sistemas de gestión y procesos relacionados para preparar el sistema de TIC de una organización para que detecte y responda ante los eventos de seguridad, incluyendo los eventos de Ciberseguridad. Esta orientación destaca enfoques técnicos adicionales que son aplicables para mejorar la disposición en el área de detección de eventos, a través del Darknet para Seguimiento; la investigación, a través Tracebacks; y la respuesta, a través de una Operación Sinkhole, de la Ciberseguridad de una organización.

Las organizaciones, particularmente las CIIPs, deberían considerar aprovechar estos enfoques para fortalecer la Ciberseguridad y, por lo tanto, su estatus.

A.2 Darknet para seguimiento

A.2.1 Introducción

La Darknet es un conjunto de direcciones IP que no se usan en las organizaciones. Las direcciones IP en una Darknet no están asignadas a ningún sistema de servidores/PC operacional. Al usar paquetes monitoreados en los dominios IP de la Darknet, las organizaciones podrían observar ataques de red emergentes, incluyendo el escaneo de red iniciado por malwares, comportamientos de infección por malware y las Retro dispersiones DDoS. Debido a que las direcciones IP de la Darknet son públicas, pero no están designadas a hosts legítimos, todo el tráfico entrante que le pertenece a los dominios IP de la Darknet se puede inferir como consecuencia ya sea de actividades maliciosas o por causa de configuraciones incorrectas.

En general, hay tres métodos usados comúnmente en una Darknet para observar tráficos relacionados a actividades maliciosas en Internet, específicamente, el Seguimiento de Agujero Negro y el Seguimiento de Interacción Baja y Alta.

A.2.2 Seguimiento de agujero negro

El seguimiento de Agujero Negro se refiere a los sistemas de seguimiento que no responden a nada en contra de los paquetes entrantes encontrados en los dominios IP de una Darknet. Este tipo de sistema de seguimiento se suele usar para observar silenciosamente los escaneos de puertos de red realizados por malwares y el comportamiento de infección por malware (un UDP con carga incluyendo shellcode) y Retro difusiones de DDoS. El escaneo de puertos de red suele ser el paso inicial que llevan a cabo los atacantes en busca de sistemas de host vulnerables de los que puedan abusar. Los comportamientos de infección por malware son normalmente los pasos de seguimiento que llevan a cabo los atacantes luego de identificar los sistemas de host vulnerables. Dichas acciones de infección se suelen observar para usar un UDP con carga en el seguimiento de agujero negro. Es más, las Retrodispersión de DDoS se observan también mediante el seguimiento de Agujero Negro en el caso de falsificar direcciones IP fuentes (atacantes) y el blanco de un DDoS se puede reconocer por el tráfico de Retrodispersión. La Figura A.1 muestra una captura de pantalla de una visualización de las actividades de malware detectadas por un sistema de seguimiento de Agujero Negro. En el siguiente link se puede ver un video de muestra: https://www.youtube.com/watch?v=asemvKgkib4&feature=related.

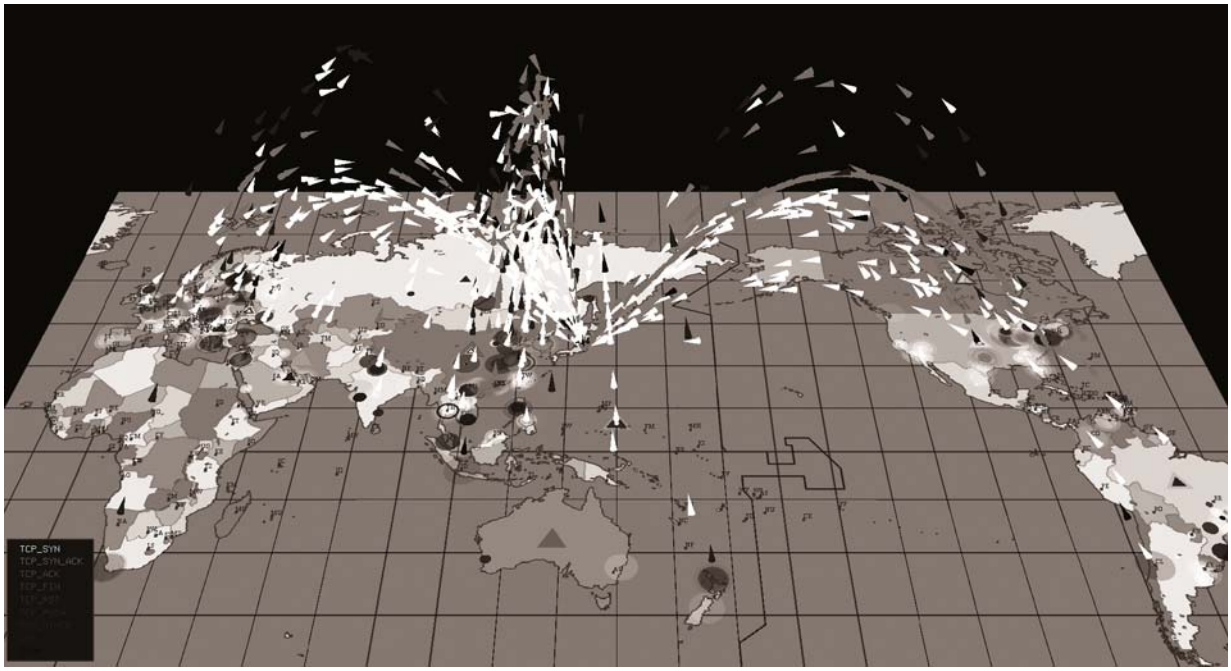

Figura A.1 – Ejemplo de una visualización de actividades de malware por medio de un sistema de seguimiento de Agujero Negro

Las “flechas” encima del mapa mundial (ver Figura A.1) muestran el cruce de los paquetes IP desde fuentes hacia las ubicaciones objetivo. Las diferentes sombras (colores en el video) muestran el tipo de paquete (por ejemplo, TCP SYN, TCP SYN-ACK, otros tipos de TCP, UDP e ICMP). La altitud de cada flecha está en proporción con su número de puerto.

A.2.3 Seguimiento de interacción baja

Un sistema de seguimiento de interacción baja es un sistema de seguimiento de Darknet que responde a los paquetes IP de Darknet al intentar conectarse nuevamente con los sistemas de host sospechosos. El propósito de la conexión que se intenta es obtener más información con respecto a los sistemas de host atacantes, los caminos de red de ataque usados y otra información relacionada a los ataques, si es posible. El sistema de seguimiento se suele configurar para disfrazarse como un sistema con

vulnerabilidades no reparadas para atraer a los atacantes. El sistema de seguimiento de interacción baja también se usa para observar reacciones más desarrolladas de comportamientos y actividades maliciosos, como la ejecución de Shell Scripts luego de los escaneos de puertos de red iniciales.

A.2.4 Seguimiento de interacción alta

Un sistema de seguimiento de interacción alta (también llamado como honeypot de interacción alta) también es un sistema de seguimiento de Darknet que responde a los paquetes IP de Darkent detectados al intentar conectarse nuevamente con los sistemas de host sospechosos e interactuar con los sistemas lo más posible. El propósito de la interacción es obtener información más profunda, incluyendo la estrategia para abusar de las vulnerabilidades, malwares ejecutables inyectados luego de los abusos y el comportamiento del malware infeccioso. El sistema de seguimiento de interacción alta se puede implementar en sistemas de operación reales o virtuales con vulnerabilidades sin arreglar para que éstos llamen la atención de los atacantes, sean abusados y finalmente se puedan capturar muestras del malware inyectado.

A.3 Operación Sinkhole

Una operación Sinkhole se define como un método para redirigir un tráfico IP específico a un dispositivo sinkhole (por ejemplo, un router sinkhole) para el propósito de analizar tráficos, desviar ataques y detectar comportamientos anómalos en una red. Por ejemplo, si una operación de negocio de un sistema blanco es interrumpida por medio de un ataque DDoS, una de las soluciones eficaces es iniciar una operación Sinkhole al inyectar una ruta alternativa para el blanco y redirigir el tráfico del DDoS a través de dicha ruta en vez de permitir que este fluya al blanco original. El dispositivo sinkhole es capaz de absorber, analizar y/o desechar el tráfico del DDoS. La ruta de redireccionamiento del blanco, la que se dirige a un router sinkhole, es liberada normalmente por un router BGP. La operación sinkhole por medio de la configuración BGP, se describe en RFC 3882. Una desventaja de este método es que la dirección IP que está siendo atacada no se puede usar para comunicarse con otros usuarios de red hasta que se retire el router.

Las operaciones de sinkhole se suelen usar para la protección en contra de ataques DDoS, como se describe anteriormente. También se han implementado para ofrecer una protección en contra de ataques de botnet al re direccionar el Comando y Control (C&C) de una botnet a un dispositivo sinkhole. Puesto que cada bot necesita establecer conexiones con un servidor C&C para recibir instrucciones de ataques desde un controlador botnet, éstos envían consultas DNS para resolver la URL del servidor C&C. Luego los servidores DNS envían una dirección IP del dispositivo sinkhole a los bots en vez de la dirección IP genuina del servidor C&C. Por consiguiente, se le priva al controlador botnet de la conexión con los bots para que no pueda enviarles instrucciones de ataque.

A.4 Traceback

Para automatizar o hacer expedito el seguimiento manual en contra de ataques maliciosos como los ataques DoS, por medio de los cuales se falsifica el host originario, se han estudiado muchas técnicas automáticas de traceback. Las técnicas de traceback se reconocen como técnicas que reconstruyen el camino de ataque y ubican los nodos del atacante por medio de la corrección del tráfico de ataque, información de localización, paquetes marcados o del registro de auditoría del tráfico de ataque.

Todavía no se emplean o practican técnicas de traceback en el entorno operante de red real, las que pueden reconstruir el camino de ataque a través de varios dominios de red. Las dificultades de implementación de técnicas de traceback de inter-dominios (a través de varios dominios de red) derivan de los problemas operacionales siguientes:

a) Para el propósito de un traceback inter-dominio, el intercambio de información sensible, como la topología de la red troncal detallada, puede causar problemas graves para los operadores de red.

b) Debido a que una operación de traceback puede estar ligada estrechamente a la seguridad de red troncal ISP, no se aceptarán ensayos arbitrarios de intentos de traceback hechos por personas no autorizadas para la mayoría de los ISPs. De esta forma, se teme al mal uso de la técnica de traceback por parte de terceros en cada dominio de red.

c) Si una técnica de traceback inter-dominio única y específica se aplica a través de varios dominios de red, esta sola y única técnica se debería implementar por los Sistemas Autónomos (AS) participantes al mismo tiempo. Aún más, los atacantes más pronto que tarde desarrollarán ataques de evasión. Muchos ISPs emplean múltiples herramientas de detección y de traceback en sus redes.

Los problemas operacionales anteriores surgen cuando un ensayo de traceback se intenta expandir más allá de los límites de red. Las técnicas de traceback deberían considerar los límites de las operaciones de red y las diferencias de las políticas operacionales entre los diferentes dominios de red. Se cree firmemente que los traceback inter-dominio y los mecanismos de mitigación de ataques se deben implementar a través de Internet.

En el desarrollo de técnicas de traceback inter-dominio y de sistemas en práctica, se debería considerar la arquitectura de traceback siguiente:

a) Para mantener los límites de operación de red, la arquitectura de traceback debe dejar que cada AS decida que su política operacional herede una petición de seguimiento.

b) La arquitectura de traceback también debería dejar que cada AS decida si investigar o no el interior de su propio dominio de red de manera más profunda.

c) La arquitectura también debería permitir que cada subdominio de un AS decida dejar que su política de operación inspeccione o no cada red de subdominio. La operación de traceback consumirá muchos recursos en los ASes relacionados y, por esto, la arquitectura de traceback no debería enviarle mensajes de solicitud a los ASes que no tengan relación con el ataque montado.

d) Para reducir el daño de los malos usos, el mensaje no debería transportar este tipo de información sensible que pueda causar la filtración de secretos o de la confianza de un AS. De este modo, la arquitectura de traceback no debería revelar la información sensible de un AS a otros.

e) Incluso cuando ocurre un mal uso o una acción comprometida, la rastreabilidad del mensaje identificará al criminal y, de esta forma, un mensaje intercambiado en la arquitectura debería tener su propia rastreabilidad para probar o confirmar al distribuidor.

f) Si la arquitectura depende de una técnica de traceback específica, los atacantes desarrollarán ataques de evasión y ocultarán las ubicaciones de los nodos de los atacantes. Para superar los ataques de evasión, la arquitectura de traceback debería ser independiente de las técnicas de traceback específicas.

g) Muchos sistemas de operación vienen para apoyar a la pila dual de IPv4/IPv6 y varios ataques pasan a través de un túnel 6to4 IPv6. Si la arquitectura de traceback no puede hacer un reseguimiento de los ataques en la red IPv6 o de los ataques a través de algunos traductores, la mayoría de los ataques cambiarán a un ataque más complejo. De esta forma, la arquitectura de traceback debería hacer un reseguimiento de un ataque en un entorno de pila dual, incluso cuando el ataque emplea algunas técnicas de traducción de dirección.

h) Para automatizar el proceso de mitigación de ataques, la arquitectura debería ser capaz de exportar el resultado de un ensayo de traceback como un detonante de la mitigación de ataques. De esta forma, la arquitectura de traceback debería permitir que cada AS tome otra acción junto con un resultado de seguimiento como un filtro u otro tipo de seguimiento.

i) La arquitectura debería tener la capacidad de cooperar con los sistemas de detección o con los sistemas de protección.

j) Un atacante puede cambiar el patrón de tráfico de ataque para evitar el efecto de dichas acciones de mitigación. Al combatir con los cambios de un ataque complejo, el tiempo empleado en el seguimiento de un camino de ataque debería ser lo más corto posible. De esta forma, la arquitectura debería excluir la interacción humana lo más posible.

Anexo B
(informativo)

Recursos adicionales

B.1 Referencias online de seguridad y anti-spyware

Hay algunos sitios Web que se pueden citar y aprovechar para obtener más información relacionada a la protección de Internet y Ciberseguridad. Las siguientes es una lista no exhaustiva de ejemplos:

— **Coalición Anti-Spyware** (http://www.antispywarecoalition.org/): Es un grupo dedicado a construir un consenso sobre las definiciones y buenas prácticas en el debate sobre los spyware y otras tecnologías no deseadas potenciales. Se compone de compañías de software anti-spyware, académicos y grupos de consumidores y busca reunir un conjunto de perspectivas sobre el problema de controlar los spyware y otras tecnologías no deseadas potenciales.

— **APWG** (http://www.antiphishing.org/): Sitio para la conciencia y educación sobre la Suplantación de Identidad que suministra informes actualizados de manera trimestral sobre las tendencias, distribución, impactos y noticias relacionadas a los ataques.

— **Be Web Aware** (http://www.bewebaware.ca): Programa educacional público, bilingüe y nacional sobre la protección de Internet diseñado para asegurar que los jóvenes canadienses se beneficien de Internet, manteniéndose al mismo tiempo a salvo y siendo responsables de sus actividades online.

— **Centro para el Uso Seguro y Responsable de Internet** (http://csriu.org): Organización que provee servicios de participación que abordan los problemas relacionados al uso seguro y responsable de Internet.

— **Childnet Internacional** (http://www.childnet.com/): Organización sin fines de lucro que trabaja en colaboración con otros individuos alrededor del mundo para ayudar a hacer el Internet un gran y seguro lugar para los niños.

— **ECPAT** (http://www.ecpat.net/): Red de organizaciones e individuos que trabajan juntos para eliminar el comercio sexual infantil.

— **GetNetWise** (http://www.getnetwise.org/): Servicio público ofrecido por una coalición de corporaciones de la industria de Internet y organizaciones de interés público que buscan que los usuarios estén a “solo un click de distancia” de los recursos que necesitan para tomar decisiones informadas sobre ellos mismos y sus familias por medio de Internet.

— **Alianza de Infraestructura Global para la Protección en Internet** (GIAIS)[13] (http://www.microsoft.com/es-es/security/default.aspx): Una alianza de algunos Proveedores de Servicios que se han organizado para mejorar la protección y seguridad en la Web, gestionar amenazas de manera consistente a través de un amplio espectro e identificar y mitigar vulnerabilidades existentes.

13 En inglés: *Global Infrastructures Alliance for Internet Safety, GIAIS.*

— **INHOPE** (http://www.inhope.org): Asociación internacional que apoya las líneas directas de Internet en su búsqueda por responder a los informes con contenido ilegal para hacer más seguro Internet.

— **Grupo de Protección de Internet** (http://www.netsafe.org.nz/): El sitio Web de NetSafe es el home online del Grupo de Seguridad de Internet de Nueva Zelanda (ISG)[14] y de Héctor, el Protector.

— **Interpol** (http://www.interpol.int): Organización de la policía internacional que facilita la cooperación de la policía transfronteriza y apoya y ayuda a todas las organizaciones, autoridades y servicios cuya misión es prevenir o combatir el crimen internacional.

— **iSafe** (http://www.isafe.org): Líder mundial en la educación de protección en Internet. Incorpora un curriculo de sala de clase con la participación dinámica de la comunidad para empoderar a los estudiantes, profesores, padres, reforzadores de la ley y adultos interesados para hacer del Internet un lugar más seguro.

— **ISECOM** (http://www.isecom.org/): Metodologías libres de fuente abierta (FDL) sobre el Testeo de Seguridad Profesional (evaluación de vulnerabilidades, prueba de penetración, hackeo ético) y la Evaluación de Riesgos Técnicos (RAVs, etc.). El ISECOM dirige el OSSTMM (Manual de Metodología de Testeo de Seguridad de Fuente Abierta), una norma mundial de facto para ejecutar pruebas de seguridad de TI/TIC (http://www.osstmm.org).

— **COP** (http://www.itu.int/cop/): La Protección de Niños Online (COP)[15] es un proyecto especial llevado a cabo por la ITU (Unión Internacional de Telecomunicación) y otras agencias/firmas especializadas que proveen directrices de Seguridad para: Niños, Padres, Guardianes y Educadores, la Industria y los Formuladores de Políticas.

— **Seguridad en Casa Microsoft** (http://www.microsoft.com/protect): Información y recursos para ayudar al público a proteger sus computadores, a ellos mismos y a sus familias.

— **Instituto Nacional de Tecnología de la Comunicación, INTECO** (http://www.inteco.es, http://cert.inteco.es, http://www.osi.es, http://observatorio.inteco.es): Servicio público gratuito ofrecido por una administración pública española para promover la confianza y seguridad en Internet para los ciudadanos, PyMEs, técnicos, niños, etc., a través de un Equipo de Respuesta ante Emergencias Informáticas (INTECO-CERT), una Oficina de Seguridad del Internauta (OSI) y un Observatorio de Seguridad de la Información.

— **Net Family News** (http://netfamilynews.org): Servicio público sin fines de lucro que provee un foro y “noticias de tecnología para niños” para padres y educadores en más de 50 países.

— **NetAlert Limitada** (http://www.netalert.net.au): Organización comunitaria sin fines de lucro establecida por el gobierno australiano para proveer consejos y una educación independiente sobre la gestión del acceso a contenidos online.

— **NetSmartzKids** (http://www.netsmartzkids.org): NetSmartz es un recurso de protección interactivo y educativo del Centro Nacional para Niños Perdidos y Abusados (NCMEC)[16] y Clubes de Niños y Niñas en América (BGCA)[17] para niños entre 5 y 17 años, padres, guardianes, educadores y reforzadores de la ley que utiliza actividades 3-D apropiadas para dichas edades para enseñarle a los niños a cómo mantenerse seguros en Internet.

14 En inglés: *Internet Safety Group, ISG.*

15 En inglés: *Children Online Protection, COP.*

16 En inglés: *National Centre for Missing and Exploited Children, NCMEC.*

17 En inglés: *Boys and Girls Clubs of America, BGCA.*

— **Saferinternet.be** (www.saferinternet.be): Este sitio Web ofrece información útil sobre los riesgos y contenidos dañinos principales con los que se pueden encontrar menores de edad online y sobre el campo de la TIC en general (también a través de redes de teléfonos móviles, etc.), es decir, pornografía infantil, racismo y discriminación, sectas, prácticas comerciales ilegitimas y fraudes y, finalmente, riesgos técnicos. El sitio Web, el cual también presenta estrategias para lidiar correctamente con estos riesgos, consiste de varias secciones que se centran en varios grupos blanco. Provee, entre otras cosas, archivos pedagógicos y técnicos para los educadores (padres y profesores), juegos para los niños (entre 6 y 12 años) y un sitio completamente separado (web4me.be) para adolescentes.

— **SafeKids.com** (http://www.safekids.com): Recursos para ayudar a las familias a hacer divertidos, seguros y productivos el Internet y la tecnología.

— **StaySafe.org** (http://www.staysafe.org): Sitio educativo que busca ayudar a los consumidores a entender los aspectos positivos de Internet y cómo gestionar una variedad de problemas de seguridad y protección que existen online.

— **UNICEF** (http://www.unicef.org): Defensor global para la protección de los derechos de los niños dedicado a proveer una ayuda humanitaria de desarrollo a largo plazo a niños y padres en países en vías de desarrollo.

— **WebSafe Crackerz** (http://www.websafecrackerz.com): Juegos y puzles interactivos diseñados para ayudar a los adolescentes y ofrecer estrategias para lidiar con diferentes situaciones online incluyendo el spam, la suplantación de identidad y las estafas.

B.2 Lista de muestra de contactos de escalamiento de incidentes

La Tabla B.1 a continuación provee una lista no exhaustiva de ejemplos de contactos de escalamiento de incidentes de seguridad de Internet:

Tabla B.1 – Lista de muestra de información de contactos de escalamiento de la seguridad

Organizaciones	Contacto
Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
Microsoft Corporation	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
Foro de Respuestas ante Incidentes y Equipos de Seguridad (FIRST)	http://www.first.org/about/organization/teams
Los equipos CERT nacionales respectivos (ejemplos:)	
Instituto Nacional de Tecnología de la Comunicación, INTECO, España	http://cert.inteco.es (Inglés: https://www.incibe.es/home/national_cybersecurity_institute/?postAction=getCertHome)
Telecom-ISAC Japón	https://www.telecom-isac.jp/contact/index.html
KrCERT/CC (Centro de Seguridad de Internet de Corea)	http://www.krcert.or.kr/index.jsp

Anexo C
(informativo)

Ejemplos de documentos relacionados

C.1 Introducción

Este anexo provee una lista no exhaustiva de ejemplos de documentos que pueden ser útiles al momento de considerar la Ciberseguridad. No busca ser una lista completa de Normas Internacionales e Informes Técnicos para Ciberseguridad.

C.2 ISO e IEC

Tabla C.1 – Sistemas de gestión de seguridad de la información

Referencia	Título
ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary.
ISO/IEC 27001	Information technology - Security techniques - Information security management systems - Requirements.
ISO/IEC 27002	Information technology - Security techniques - Code of practice for information security management.
ISO/IEC 27003	Information technology - Security techniques - Information security management system implementation guidance.
ISO/IEC 27010	Information technology - Security techniques - Information security management for intersector communications.

Tabla C.2 – Gestión de riesgos

Referencia	Título
ISO/IEC 27005	Information technology - Security techniques - Information security risk management.
ISO/IEC 16085	Systems and software engineering - Life cycle processes - Risk management.

Tabla C.3 – Evaluación de la seguridad de TI

Referencia	Título
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security.
ISO/IEC 18045	Information technology - Security techniques - Methodology for IT security evaluation.
ISO/IEC TR 19791	Information technology - Security techniques - Security assessment of operational systems.

Tabla C.4 – Garantía de seguridad

Referencia	Título
ISO/IEC TR 15443	Information technology - Security techniques - A framework for IT Security assurance.
ISO/IEC 15026	Systems and software engineering - Systems and software assurance.

Tabla C.5 – Diseño e implementación

Referencia	Título
ISO/IEC 12207	Systems and software engineering - Software life cycle processes.
ISO/IEC 14764	Software Engineering - Software Life Cycle Processes - Maintenance.
ISO/IEC 15288	Systems and software engineering - System life cycle processes.
ISO/IEC 23026	Software Engineering - Recommended Practice for the Internet - Web Site Engineering, Web Site Management, and Web Site Life Cycle.
ISO/IEC 42010	Systems and software engineering - Architecture description.

Tabla C.6 – Subcontratación y servicios de terceros

Referencia	Título
ISO/IEC TR 14516	Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services.
ISO/IEC 15945	Information technology - Security techniques - Specification of TTP services to support the application of digital signatures.

Tabla C.7 – Seguridad de red y de aplicaciones

Referencia	Título
ISO/IEC 18028	Information technology - Security techniques - IT network security.
ISO/IEC 18043	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems.
ISO/IEC 27033	Information technology - Security techniques - Network security.
ISO/IEC 27034	Information technology - Security techniques - Guidelines for application security.

Tabla C.8 – Gestión de la continuidad e incidentes

Referencia	Título
ISO/IEC TR 18044	Information technology - Security techniques - Information security incident management.
ISO/IEC 24762	Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services.
ISO/IEC 27031	Information technology - Security techniques - Guidelines for ICT readiness for business continuity.
ISO/IEC 27035	Information technology - Security techniques - Information security incident management.

Tabla C.9 – Gestión de identidad

Referencia	Título
ISO/IEC 24760	Information technology - Security techniques - A framework for identity management.

Tabla C.10 – Privacidad

Referencia	Título
ISO/IEC 29100	Information technology - Security techniques - Privacy framework.

Tabla C.11 – Gestión de activos

Referencia	Título
ISO/IEC 19770	Information technology - Software asset management.

Tabla C.12 – Gestión de Servicios

Referencia	Título
ISO/IEC 20000	Information technology - Service management.

C.3 ITU-T

Tabla C.13 – Ciberseguridad

Referencia	Título
ITU-T X.1200 - Serie X.1299	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Cyberspace security.
ITU-T X.1205	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Overview of Cybersecurity.

Tabla C.14 – Gestión de continuidad e incidentes

Referencia	Título
ITU-T X.1206	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - A vendor-neutral framework for automatic notification of security related information and dissemination of updates.

Tabla C.15 – Software no deseado

Referencia	Título
ITU-T X.1207	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Guidelines for Telecommunication Service Providers for Addressing the Risk of Spyware and Potentially Unwanted Software.

Tabla C.16 – Spam

Referencia	Título
ITU-T X.1231	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Technical strategies for countering spam.
ITU-T X.1240	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Technologies involved in countering e-mail spam.
ITU-T X.1241	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Technical framework for countering email spam.
ITU-T X.1244	Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Overall aspects of countering spam in IP-based multimedia applications.

Tabla C.17 – Intercambio de información de Ciberseguridad

Referencia	Título
ITU-T X.1500 - Serie X.1598 (CYBEX)	Series X: Data networks, Open System Communications and Security - Cybersecurity Information Exchange.

NOTA A septiembre de 2011, debido a que el trabajo de CYBEX se encuentra actualmente en progreso en la ITU-T, sólo están disponible X.1500, X.1520, X.1521 y X.1570 como Recomendaciones o bosquejos. En el futuro se lanzarán más documentos por lo que se recomienda que los usuarios verifiquen el sitio Web de la ITU-T para ver la última información disponible.

Anexo D
(informativo)

Bibliografía

[1] An Autonomous Architecture for Inter-Domain Trace back across the Borders of Network Operation (iscc06).

[2] IETF RFC 3882, Configuring BGP to Block Denial-of-Sevice Attacks.

[3] ISO Guide 73:2009, *Risk management - Vocabulary*.

[4] ISO/IEC 12007:2008, *Systems and software engineering - Software life cycle processes*.

[5] ISO/IEC 15408-1, *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model*.

[6] ISO/IEC 19770-1, *Information technology - Software asset management - Part 1: Processes and tiered assessment of conformance*.

[7] ISO/IEC TR 19791, *Information technology - Security techniques - Security assessment of operational systems*.

[8] ISO/IEC 20000-1, *Information technology - Service management - Part 1: Service management system requirements.*

[9] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*.

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

[11] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management.*

[12] ISO/IEC 27010, *Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications*.

[13] ISO/IEC 27031, *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity*.

[14] ISO/IEC 27033 (todas las partes), *Information technology - Security techniques - Network security*.

[15] ISO/IEC 27034 (todas las partes), *Information technology - Security techniques - Application security.*

[16] ISO/IEC 27035, *Information technology - Security techniques - Information security incident management*.

[17] ISO/IEC 29147, *Information technology - Security techniques - Vulnerability disclosure*.[18]

[18] ISO 31000, *Risk management - Principles and guidelines*.

[19] ITU-T X.1200 - X.1299, Series X: Data Networks, Open System Communications and Security, Telecommunications Security - Ciberspace security.

[20] ITU-T X.1500 - X.1598, Series X: Data Networks, Open System Communications and Security - Cybersecurity Information Exchange.

NOTA EXPLICATIVA NACIONAL

La equivalencia de las Normas Internacionales señaladas anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma Internacional	Norma nacional	Grado de correspondencia
ISO Guide 73:2009	NCh-ISO GUIA 73:2012	Idéntica
ISO/IEC 12007:2008	No hay	-
ISO/IEC 15408-1	NCh2820/1:2003	La Norma Chilena NCh2820/1:2003 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 15408-1:1999.
ISO/IEC 19770-1	No hay	-
ISO/IEC TR 19791	No hay	-
ISO/IEC 20000/1	NCh-ISO 20000/1:2013	La Norma Chilena NCh-ISO 20000/1:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 20000-1:2011.
ISO/IEC 27001	NCh-ISO 27001:2013	La Norma Chilena NCh-ISO 27001:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27001:2013.
ISO/IEC 27002	NCh-ISO 27002:2013	La Norma Chilena NCh-ISO 27002:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27002:2013.
ISO/IEC 27005	NCh-ISO 27005:2014	La Norma Chilena NCh-ISO 27005:2014 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27005:2011.
ISO/IEC 27010	No hay	-
ISO/IEC 27031	NCh-ISO 27031:2015	La Norma Chilena NCh-ISO 27031:2015 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27031:2011.
ISO/IEC 27033 (todas las partes)	No hay	-

(continúa)

18 En preparación.

(conclusión)

ISO/IEC 27034 (todas las partes)	No hay	-
ISO/IEC 27035	No hay	-
ISO/IEC 29147	No hay	-
ISO 31000	NCh-ISO31000:2012	La Norma Chilena NCh-ISO 31000:2012 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO 31000:2009.

Anexo E
(informativo)

Justificación de los cambios editoriales

Tabla E.1 – Cambios editoriales

Cláusula/subcláusula	Cambios editoriales	Justificación
En toda la norma	Se reemplaza “Esta Norma Internacional” por “esta norma”.	La norma es de alcance nacional.
1	Se reemplaza “Alcance” por “Alcance y campo de aplicación”.	De acuerdo con estructura de NCh2.
3 y Anexo D	Se agrega Nota Explicativa Nacional.	Para detallar la equivalencia y el grado de correspondencia de las Normas Internacionales con las Normas Chilenas.
Anexo D	Se reemplaza “Bibliografía” por “Anexo D (informativo) Bibliografía”.	De acuerdo con estructura de NCh2.