Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)

Mejores Prácticas en Ciberseguridad

B.18

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título *Recomendaciones de implementación: Distribución de publicaciones vía mensaje de texto (SMS)*. © (2021) Dirección Nacional de Ciberseguridad de Israel.

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) en idioma hebreo. Su traducción al idioma español fue realizada por el equipo de ciberseguridad de la división de Innovación para Servir al Ciudadano (IFD/ICS) del Banco Interamericano de Desarrollo (BID), y se incluye como capítulo de la colección "Mejores Prácticas en Ciberseguridad".

El lector debe tener presente que la ciberseguridad es un campo que evoluciona rápidamente. Aunque estos documentos reflejan principios establecidos, podrían actualizarse periódicamente según sea necesario para reflejar los avances en este campo. Adicionalmente, si bien se ha hecho lo posible para presentar las recomendaciones y recursos de manera que sean universalmente aplicables a las organizaciones de todo el mundo, el lector puede encontrar referencias que son específicas al ecosistema cibernético y contexto de Israel (tales como las sumas indicadas en Nuevos Shekels Israelíes [NIS], o referencias a la normativa israelí o a sus organismos gubernamentales).

El documento original se encuentra disponible en el siguiente enlace: **https://www.gov.il/he/pages/smsbp**. Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

"El presente documento ha sido redactado por el Dirección Nacional de Ciberseguridad con el fin de fomentar la ciberseguridad en la economía israelí. Todos los derechos reservados para el Estado de Israel - Dirección Nacional de Ciberseguridad. El documento ha sido elaborado para beneficio del público. La copia del documento o su incorporación en otros documentos estará sujeta a las siguientes condiciones: el reconocimiento de la autoría de la Dirección Nacional de Ciberseguridad en el formato que aparece a continuación; la utilización de la última versión del documento; la no realización de modificaciones en el documento. El documento contiene información de carácter profesional, cuya implementación requerirá el conocimiento de los sistemas y la adaptación a las características de estos por parte de un profesional en el ámbito de la ciberseguridad. Cualquier comentario o referencia se puede enviar por correo electrónico a: tora@cyber.gov.il."

Índice

Prólogo

La transformación digital y el reto de la ciberseguridad

A medida que la transformación digital continúa expandiéndose por todo el mundo, los gobiernos, las organizaciones, los individuos e incluso los objetos están cada vez más conectados a Internet. Aunque la digitalización ha demostrado ofrecer beneficios innegables, como la prestación eficiente de servicios públicos, el crecimiento económico y la conectividad esencial para el desarrollo de innumerables actividades, también contribuye a una creciente exposición colectiva a los riesgos de ciberseguridad. Un importante motor de este fenómeno en los últimos tiempos ha sido la pandemia mundial de la COVID-19. Como resultado de las generalizadas políticas de distanciamiento social, el número de transacciones de comercio electrónico y las comunicaciones personales en línea experimentaron un crecimiento repentino y pronunciado en un corto período de tiempo, junto con el número de empleados que comenzaron a teletrabajar por primera vez. En esta situación sin precedentes, muchos usuarios de Internet se enfrentaron a nuevas interacciones en línea sin ser suficientemente conscientes de los riesgos de seguridad que estas conllevan. Las organizaciones también tuvieron que adaptarse rápidamente a los desafíos, estableciendo flujos de trabajo totalmente remotos, a menudo sin contar con todas las medidas de seguridad necesarias ni con la orientación adecuada para los empleados.

Sin duda, los ciberdelincuentes no tardaron en explotar la incertidumbre y vulnerabilidad de los usuarios desprevenidos. Proliferaron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se detectaron casi un millón de intentos de ataque diarios contra las conexiones del protocolo de escritorio remoto (RDP), ampliamente utilizado entre las organizaciones para las conexiones remotas de los empleados. De hecho, los ataques al RDP fueron la forma más popular de ciberataque, superando incluso a los correos electrónicos de *phishing*. Durante la segunda mitad del año, a medida que más organizaciones reforzaban la seguridad de sus plataformas remotas, los *hackers* centraron sus esfuerzos en explotar las vulnerabilidades de los activos privados de los empleados y los dispositivos de acceso remoto para penetrar en sus organizaciones. Aunque estas amenazas se vieron maximizadas por este contexto global, no son novedosas ni desaparecerán; las personas siguen viviendo en un entorno de riesgo elevado, que es especialmente grave en regiones del mundo donde las políticas y tecnología de ciberseguridad están menos desarrolladas, y donde falta educación y concienciación ciudadana en torno a este tema. En otras palabras, aunque los cambios debidos a la pandemia de la COVID-19 acabarán por asentarse, estos han evidenciado la urgente necesidad de reforzar las protecciones individuales y colectivas contra los riesgos cibernéticos.

Reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, promover la confianza de las personas en las tecnologías digitales y apoyar el crecimiento económico mediante una transformación digital segura. En particular, los ciudadanos deben tener la seguridad de que los sistemas digitales que utilizan para sus actividades personales o profesionales, y también los que involucran sus datos personales, cuentan con las medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de su información y de los servicios de los que dependen. Además, los fallos de ciberseguridad tienen un impacto económico importante. Un reciente informe de McAfee estimó que la ciberdelincuencia cuesta a la economía mundial unos US$600.000 millones anuales, es decir, el 0,8% del producto interno bruto (PIB) global.

Israel, líder en ciberseguridad a nivel mundial

El ecosistema de innovación y emprendimiento de Israel es reconocido globalmente como uno de los más vibrantes del mundo, lo cual le ha ganado el nombre de *Startup Nation*. Según los indicadores de ciencia y tecnología de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de marzo de 2021, Israel es el país de la OCDE que invierte un mayor porcentaje de su PIB (4,9%) en investigación y desarrollo (I+D). Cuenta con un total de más de 300 centros de innovación, investigación y desarrollo de compañías multinacionales; de ellos, docenas están dedicadas a la ciberseguridad.

No es sorpresa entonces que el 40% de la inversión privada a nivel mundial en ciberseguridad tenga lugar en Israel, que posee también el segundo ecosistema privado más grande del mundo en esta área después de Estados Unidos. Según datos de 2021, durante ese año se invirtieron US$8,8 billones en alrededor de 131 compañías israelíes del sector, y más de 40 fueron adquiridas por un total de US$3,5 billones. El país cuenta con más de 500 *startups* de ciberseguridad y, en 2021, el 33% de la población de "unicornios" del mundo eran israelíes. En total, se estimó su exportación de productos de ciberseguridad para 2020 en US$6,85 billones.

La Dirección Nacional de Ciberseguridad de Israel (INCD) es responsable de asegurar el ciberespacio nacional y de establecer y promover la resiliencia cibernética en el país. La INCD opera a nivel nacional para elevar constantemente el nivel de seguridad de las organizaciones y ciudadanos, prevenir y gestionar los ciberataques, y reforzar las capacidades de respuesta en caso de una emergencia cibernética. Su posición como parte de la oficina del Primer Ministro demuestra claramente la centralidad e importancia de sus competencias para el país. Sus objetivos también incluyen la preparación y capacitación del sector privado israelí y del público en general para protegerse de las ciberamenazas mediante la adopción de tecnologías ciberseguras, la publicación de mejores prácticas, la formación del personal y el aumento de la concienciación. Se encarga además de establecer y reforzar la base científica y tecnológica de ciberseguridad mediante el desarrollo de un capital humano altamente cualificado, el apoyo a la investigación académica de vanguardia, la participación en una avanzada I+D tecnológica y el fomento de la ciberindustria. La INCD dedica sus esfuerzos a mantener un ciberespacio protegido, seguro y abierto para todos los habitantes y empresas del Estado de Israel y a facilitar su crecimiento y su base científica e industrial.

¿Cuál es el estado de la ciberseguridad en la región de América Latina y el Caribe?

El Banco Interamericano de Desarrollo (BID) realiza periódicamente estudios sobre la evolución de las capacidades de sus Estados miembros para defenderse de las crecientes amenazas en el ciberespacio. El *Reporte regional de madurez en ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*, elaborado en colaboración con la Organización de los Estados Americanos (OEA), mostró que los países se encontraban en diferentes etapas de desarrollo en su preparación para enfrentar los desafíos de la ciberseguridad, pero en general aún tenían un amplio margen de mejora.

Mientras que, en 2016, año de la primera edición del informe, el 80% de los países de la región no contaba con una estrategia nacional de ciberseguridad, esta cifra se redujo al 60% en 2020. Además, solo unos pocos países gestionan la exposición de sus infraestructuras críticas —como energía, sanidad, telecomunicaciones, transporte, suministro de agua y finanzas— a ciberataques. Como revela el Reporte de 2020, solo siete de los 32 países evaluados contaban con un plan de protección cibernética de infraestructuras críticas. Esta es una de las conclusiones más preocupantes, si se tiene en cuenta el impacto catastrófico que los ataques a estos sectores podrían tener no solo en las economías nacionales, sino en la vida de todos sus ciudadanos.

En cuanto a la capacidad de los países para gestionar y responder a los incidentes de ciberseguridad, el mismo estudio relevó que el 63% de los países contaba con equipos de respuesta a incidentes de seguridad, como Equipos de Respuesta a Emergencias Informáticas (CERT) o Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Sin embargo, de los 20 países que sí los tenían, solo tres habían alcanzado una madurez avanzada en su capacidad de coordinar dichas respuestas. De hecho, 23 de los 32 países se encontraban todavía en una fase inicial de madurez en este tema. Este hallazgo llamó la atención sobre la necesidad de que los países refuercen la capacidad de sus equipos para coordinar eficazmente sus respuestas a los ciberincidentes. Además, el informe examinó la disponibilidad de oportunidades educativas y de formación en ciberseguridad y descubrió que menos de la mitad de los países de la región ofrecían educación formal en ciberseguridad, como posgrados, maestrías o títulos técnicos. No hace falta decir que contar con suficientes profesionales formados es esencial para diseñar e implementar las políticas y medidas de ciberseguridad necesarias para garantizar la resiliencia de un país frente a ciberataques cada vez más sofisticados y complejos.

¿Qué hace el BID para apoyar a la región?

Durante los últimos años, el BID ha apoyado activamente a la región en el desarrollo de la capacidad en ciberseguridad, el diseño e implementación de una política pública de ciberseguridad a nivel nacional y el fortalecimiento de las capacidades sectoriales en ciberseguridad. Este apoyo adopta diversas formas. El BID ha puesto a disposición de los países de América Latina y el Caribe (ALC) asistencia financiera por valor de decenas de millones de dólares para desarrollar capacidades nacionales de ciberseguridad a través de más de 15 operaciones de inversión en el sector público, así como una importante financiación adicional para garantizar la ciberseguridad en los proyectos de inversión en transformación digital.

También proporciona orientación técnica y lleva a cabo proyectos de ciberseguridad en toda la región en forma de consultorías, diagnósticos y proyectos de fortalecimiento de la ciberseguridad hechos a medida, en temas que incluyen la protección cibernética de infraestructuras críticas, cibercrimen y análisis forense, diseño y fortalecimiento de los CSIRT y de los Centros de Operaciones de Seguridad (SOC), y estrategias nacionales y sectoriales de ciberseguridad. Además, el BID ha realizado importantes esfuerzos para proporcionar oportunidades a los profesionales de ALC, a fin de reforzar y actualizar sus habilidades en este campo, ofreciendo regularmente talleres y actividades de formación. Estos han incluido cursos ejecutivos de ciberseguridad de dos semanas de duración, ofrecidos conjuntamente con la Universidad Hebrea de Jerusalén en Israel, así como cursos a medida sobre protección de infraestructuras críticas y otros dirigidos a sectores específicos. Por último, el BID ha elaborado varias publicaciones de gran impacto sobre cuestiones de ciberseguridad a nivel nacional y sectorial, y sigue actualizando y ampliando periódicamente este cuerpo de conocimientos.[1]

1. Véase el sitio del Clúster de Datos y Gobierno Digital (DDG) de la división Innovación para Servir al Ciudadano (ICS) de BID, disponible en: **https://www.iadb.org/es/reforma-modernizacion-del-estado/cluster-de-datos-y-gobierno-digital**.

El BID y la INCD: uniendo esfuerzos

Los retos de la ciberseguridad, como los de la propia Internet, son de naturaleza global, por lo que compartir el conocimiento y herramientas para afrontarlos beneficia a la población en su conjunto. Reconociendo esta realidad, la INCD y el BID se han asociado para poner la experticia israelí a disposición de los países de ALC. La colaboración entre ambas instituciones ha proporcionado un fuerte apoyo a la región, en forma de capacitaciones ejecutivas y técnicas sobre temas avanzados de ciberseguridad, conferencias de vanguardia para funcionarios públicos de ALC y profesionales en el campo, y proyectos innovadores de asistencia técnica. La presente publicación es un producto más de esta colaboración. Consiste de una serie de guías metodológicas de ciberseguridad para organizaciones desarrollada por la INCD a la luz de su análisis sobre riesgos, métodos de ataque, incidentes cibernéticos y estándares globalmente aceptados. Estas guías han sido traducidas al español y al inglés, en una actividad conjunta de ambas organizaciones, con el objetivo de permitir el acceso a este cuerpo de conocimiento por parte de audiencias de toda la región de ALC, y así contribuir a aumentar su resiliencia cibernética.

Esta colección ofrece una orientación práctica sobre una serie de cuestiones metodológicas y técnicas relevantes para el fortalecimiento de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

El reto de proteger el espacio digital seguirá creciendo, junto con la necesidad de contar con experiencia probada para afrontarlo. Las reflexiones aquí contenidas pretenden servir como recurso para potenciar la tan necesaria formación profesional en ciberseguridad que se observa actualmente en ALC. Estas guías contribuirán a elevar los estándares organizacionales, a promover mayor conciencia y cultura de ciberseguridad dentro de las organizaciones y en el público en general, y a informar a los tomadores de decisiones, gerentes y líderes en sus iniciativas de ciberseguridad. Confiamos en que estas guías servirán de hoja de ruta para los profesionales y líderes de ALC, trabajando juntos para construir un futuro más seguro y próspero.

/01.
Objetivo

Este documento contiene recomendaciones de implementación para la distribución de publicidad por mensajes de texto (SMS, por sus siglas en inglés).

/02.
Descripción de las principales amenazas

La distribución de SMS a clientes puede exponer tanto a la organización emisora como al destinatario a una serie de riesgos cibernéticos. Entre estos riesgos, cabe destacar los siguientes:

01

Daños a la imagen de la organización emisora como resultado de una campaña de suplantación de identidad que opera paralelamente a una "ola de publicidad" de la organización emisora legítima, con el objetivo de recopilar información o infiltrar *software* malicioso a los usuarios finales.

02

Exposición jurídica de la organización emisora como resultado de realizar una actividad de manera contraria a requisitos legales y reglamentarios, tales como la Ley de Correo Electrónico No Deseado, la transferencia de información entre organismos públicos, regulaciones en materia de protección de la privacidad, etc.

03

Si la actividad se realiza a través de un proveedor de servicios de distribución SMS externo, la organización emisora está expuesta a riesgos cibernéticos que se originan en la cadena de suministro.[2]

2. Para obtener más información, consulte el documento ***Cadena de suministro***, disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/cadena-de-suministro-cuando-todos-los-eslabones-son-fuertes-su-organizacion-esta-protegida-mejores**.

04

Amenazas adicionales relacionadas con los medios de identificación. Para conocerlas, consulte el documento ***Autenticación multifactor avanzada ante amenazas de ciberseguridad***.[3]

El Cuadro 1 a continuación describe las principales amenazas que resultan del envío de publicidad por SMS.

Cuadro 1. Principales amenazas en la distribución de publicidad por SMS

N.°	Tipo de amenaza	Descripción
1	Envío de un SMS de suplantación de identidad (*phishing* por SMS, también conocido como "*smishing*") que se haga pasar por un mensaje legítimo de la organización	Dirigir al usuario a un sitio web malicioso (ataque de abrevadero [*watering hole attack*]) desde el que se descargue una herramienta de ataque (*drive-by attack*) que se activa en el dispositivo móvil del usuario.
2		Dirigir al usuario a un sitio web malicioso (ataque de abrevadero) que se haga pasar por el sitio web legítimo de la organización y solicitar datos de identificación u otra información sensible/confidencial.
3		A través de un SMS solicitar información sensible/confidencial, como datos de identificación para acceder a un servicio en línea, que el usuario debe proporcionar en un mensaje de respuesta.
4		El enlace del mensaje contiene *software*/código malicioso que se ejecuta en el dispositivo móvil del usuario (en ocasiones incluso sin necesidad de una acción activa por parte del usuario).
5	Control del sistema de distribución por parte de una entidad o actor malicioso	Control del sistema de distribución por parte de una entidad o actor malicioso, lo que le permite propagar *software*/código malicioso transversalmente.
6		Enviar un mensaje de texto que contenga *software*/código malicioso a la interfaz del sistema de distribución, lo que puede afectar negativamente la disponibilidad, confidencialidad o fiabilidad de la información, incluyendo el envío de mensajes maliciosos desde el sistema de distribución oficial.
7	Filtración de la base de datos de clientes	A causa de una negligencia en la ciberseguridad y/o protección de la privacidad por parte del proveedor de servicios que envía el SMS.
8		Debido a una acción maliciosa por parte del proveedor de servicios que envía el SMS.
9		Dada una acción maliciosa por parte de un trabajador (amenaza interna) del proveedor de servicios que envía el SMS.
10		Enviar información sensible/confidencial al destinatario equivocado debido a una falla o a un error humano.
11		Enviar información prohibida según lo estipulado en la Ley de Correo Electrónico No Deseado, la Ley de Comunicaciones, la Ley de Protección de la Privacidad u otra ley que aplique.

3. El documento ***Autenticación multifactor avanzada ante amenazas de ciberseguridad*** será publicado próximamente dentro de esta serie de guías de buenas prácticas en ciberseguridad.

/03. Recomendaciones de implementación

En primer lugar, debe realizarse un proceso de evaluación de riesgos y diferenciar entre el tipo y nivel de riesgo de la información que puede enviarse a través de un sistema de distribución de mensajes que se considere no seguro, y los casos en los que se requiera actuar a través de otro canal de distribución.

Como parte de las consideraciones, entre otras cosas, pueden examinarse el canal de flujo de la información (si se trata de información unidireccional del distribuidor al cliente final o bidireccional), si el mensaje es informativo (por ejemplo, una actualización sobre horarios de visita o de apertura) o si es un mensaje en el que se proporciona información personal o personalizada para el cliente que recibe el mensaje de texto, si el mensaje incluye un enlace a un sitio web en el que se pide al cliente que entre, y si dicho sitio web requiere datos de identificación o está abierto a todas las personas por igual y no requiere un procedimiento de identificación, etcétera. Por lo general, la distribución de publicidad por SMS no está definida como una práctica recomendada a causa de los riesgos que resultan de esta forma de trabajo, tanto para la organización como para sus clientes. Sin embargo, en los casos en que a pesar de ello la organización haya decidido utilizar esta tecnología, existen varias medidas de protección que pueden implementarse para ayudar a reducir los riesgos, entre las que cabe destacar las que se mencionan a continuación:

01

Paralelamente a la distribución del SMS, presente la información sobre el tema en el sitio web de su organización. Comunique en el sitio web la existencia de una campaña de contacto, datos sobre el canal para comunicarse y hacer preguntas. También, configure un centro de llamadas telefónicas para atender a las personas que se contacten y asegúrese de que sea accesible al público en términos de idioma, visibilidad y reconocimiento. Considere publicar en las redes sociales la existencia de una campaña de contacto con los clientes y también los medios para tener una mayor precaución y verificar la autenticidad del remitente.

02

Establezca una política organizacional de acciones “permitidas y no permitidas” con respecto a los SMS. Publique esta política en el sitio web de la organización. Por ejemplo, esta política puede incluir frases cortas y claras como: “Nuestros representantes nunca le pedirán su contraseña por teléfono ni por SMS” o “Nunca nos ponemos en contacto con nuestros clientes para solicitarles información crediticia por SMS.”

03

Si el sistema de mensajería está concebido para enviar información sensible/personal, considere soluciones que permitan firmar digitalmente los SMS y utilizar el cifrado de extremo a extremo de la información. Es preferible mantener la información sensible en el servidor bajo su control y proporcionar un enlace al cliente, en lugar de enviar un archivo sensible al dispositivo de los clientes.

04

Considere la posibilidad de que los clientes firmen para indicar su reconocimiento de los riesgos que implique la recepción de SMS, así como el envío de recomendaciones en materia de protección al obtener dichas firmas (eliminar la información sensible enviada en los SMS después de leerlos, crear una contraseña en el dispositivo al que se envíen los SMS, utilizar contraseñas únicas para el servicio de su organización, etc.).

05

Publique en un lugar claramente visible del sitio web cómo ponerse en contacto con el responsable de ciberseguridad de la organización para cualquier pregunta sobre este asunto o para reportar fallas y sospechas de incidentes.

/04. Recomendaciones ampliadas

Cuadro 2. Listado de recomendaciones ampliadas

N.°	Recomendación
	Características del SMS
1	Se recomienda que la organización aclare en el mensaje que el SMS es meramente informativo, y que no incluya información sensible/confidencial, enlaces, mensajes multimedia (MMS, por sus siglas en inglés) o archivos adjuntos.
2	Se sugiere que la organización adjunte a cada mensaje un identificador aleatorio que sea válido durante las 72 horas posteriores al envío del mensaje y que permita al usuario verificar la autenticidad del mensaje en el sitio web de la organización. Al implementar esto, asegúrese de que no se dirija al usuario al sitio web de la organización a través de un enlace.
3	Se recomienda que la organización se asegure de que el número de teléfono desde el que se envía el SMS sea permanente, esté registrado como operador autorizado por el Ministerio de Comunicaciones, se utilice únicamente para distribuir mensajes de texto y aparezca en el campo "Remitente".
4	Se aconseja que la organización se asegure de que los datos de contacto del proveedor de servicios de distribución de SMS externo aparezcan en cada mensaje, incluyendo el nombre y el número de teléfono del proveedor de servicios.
	Consideraciones a la hora de elegir un proveedor de servicios de distribución
5	Se recomienda que antes de establecer la relación laboral la organización se asegure de que el proveedor de servicios (incluyendo su infraestructura y sistemas) cumpla con los requerimientos de la ***Metodología de ciberdefensa para organizaciones*** (en su última versión).[4]
6	Se recomienda que antes de establecer la relación laboral la organización se asegure de que la interfaz de programación de aplicaciones (API, por sus siglas en inglés) del proveedor de servicios cumpla con los siguientes requisitos: • El desarrollo se ha llevado a cabo de acuerdo con los principios aceptados para un desarrollo seguro. • El proceso de identificación incluye el uso de autenticación mutua basada en certificados digitales (autenticación mutua de seguridad de la capa de transporte [mTLS, por sus siglas en inglés]). El uso de un nombre de usuario y contraseña, de una contraseña compartida (*pre-shared password*), etc. no cumple con este requisito. • El acceso a la API puede realizarse desde direcciones de protocolo de Internet (IP, por sus siglas en inglés) definidas según la lista de usuarios autorizados. • Se ha utilizado un dispositivo de seguridad para proteger contra ciberataques (como cortafuegos de aplicaciones web/autoprotección de aplicaciones en tiempo de ejecución [WAF/RASP, por sus siglas en inglés]).

4. El documento ***Metodología de ciberdefensa para organizaciones 2.0*** se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad, a través del siguiente enlace: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-20-mejores-practicas-en-ciberseguridad**.

N.°	Recomendación
	Consideraciones a la hora de elegir un proveedor de servicios de distribución (cont.)
7	Se aconseja que antes de establecer la relación laboral la organización se asegure de que el proveedor de servicios cumpla con los siguientes requisitos: • Todo desarrollo se lleva a cabo de acuerdo con los principios aceptados para un desarrollo seguro. • El proceso de identificación de sus empleados incluye el uso de autenticación multifactor (MFA, por sus siglas en inglés). Esto puede lograrse mediante la implementación/adquisición de una solución MFA empresarial de una organización reconocida como Microsoft, Cisco o similar. El uso de una contraseña temporal/permanente más una contraseña por SMS no cumple con este requisito. • Se utiliza un dispositivo de seguridad para proteger contra ciberataques (como WAF/RASP).
8	Se recomienda que antes de establecer la relación laboral la organización se asegure de que el proveedor de servicios no haya sufrido un incidente de ciberseguridad y/o un incidente de protección de la privacidad durante los últimos siete años.
9	Se aconseja que antes de establecer la relación laboral la organización se asegure de que el proveedor de servicios disponga de un responsable de protección de la información y de ciberseguridad que esté subordinado al director general de la organización y que cuente con los conocimientos y recursos necesarios para cumplir su función adecuadamente.
10	Se sugiere que antes de establecer la relación laboral la organización lleve a cabo pruebas de resiliencia para comprobar el nivel de resistencia de la infraestructura y los sistemas del proveedor de servicios. En caso de encontrarse fallas de grado medio o superior, no debe establecerse una relación laboral con el proveedor.
11	Se recomienda que la organización solicite al proveedor de servicios firmar un acuerdo legal que sea aprobado por el asesor jurídico de la organización y que haga referencia a cuestiones como: • Acuerdo de confidencialidad • Prevención de conflictos de intereses • Deber del proveedor de cumplir con los requisitos de ciberseguridad y protección de la información • Deber del proveedor de no hacer un uso indebido de la información que reciba de la organización • Concepto de indemnización sin obligación de demostrar el daño • Deber de eliminar irreversiblemente la información después de su distribución • Deber del proveedor de cumplir con los requisitos legales y las regulaciones

N.°	Recomendación
	Aseguramiento del proceso de transferencia de archivos entre la organización y el proveedor de servicios
12	Se recomienda que la organización se asegure de que el proceso de transferencia de archivos entre la organización y el proveedor cumpla con los requisitos del documento ***Seguridad en la transferencia gestionada de archivos (MFT)***.[5]
	Actividades intraorganizacionales
13	Se recomienda que la organización realice una vez al año un estudio de riesgos sobre las consecuencias derivadas del uso de publicidad a través de SMS, incluyendo un examen de la eficacia de los controles de protección.
14	Se aconseja que la organización lleve a cabo pruebas de resiliencia periódicamente para comprobar el nivel de resistencia de la infraestructura y los sistemas del proveedor de servicios. En caso de encontrarse fallas de grado medio o superior, debe rescindirse la relación laboral con el proveedor.
15	Se sugiere que la organización se asegure de que la información transmitida al proveedor de servicios sea lo más reducida posible. Por ejemplo, no incluir información que no sea necesaria, como la dirección residencial, el apellido, el número del documento de identidad, etcétera.
16	Se recomienda que la organización realice comprobaciones aleatorias en las instalaciones del proveedor de servicios para asegurarse de que este elimina la información de la organización después de su distribución.

5. El documento ***Seguridad en la transferencia gestionada de archivos (MFT)*** será publicado próximamente dentro de esta serie de guías de buenas prácticas en ciberseguridad.

N.°	Recomendación
Actividades intraorganizacionales (cont.)	
17	Se aconseja que la organización se asegure de que los ciberactivos involucrados en el proceso de envío no sean accesibles directamente por Internet. Alternativamente, puede utilizarse la infraestructura de escritorio virtual (VDI, por sus siglas en inglés) u otra solución para navegar por Internet.
18	Se sugiere que la organización utilice servicios aceptados para la protección de marca (protección de riesgos digitales [DRP, por sus siglas en inglés]) a fin de detectar, identificar e impedir actividades de suplantación de identidad en el ciberespacio.
19	Se recomienda que la organización se asegure de cumplir con los requerimientos de la ***Metodología de ciberdefensa para organizaciones*** (en su última versión, véase el enlace en la pág. 15 de este documento).
20	Se aconseja que la organización realice un seguimiento continuo del envío de publicidad a los usuarios, incluyendo los porcentajes de fallas, etcétera.
21	Se recomienda que la organización solicite a los usuarios que confirmen cada cierto tiempo que el número de teléfono utilizado para recibir SMS es correcto.
Asistencia para usuarios/clientes	
22	Para atender las consultas de los usuarios, se recomienda que la organización cuente con un centro de asistencia humano, disponible las 24 horas del día los 365 días del año, completamente subordinado al responsable de ciberseguridad y protección de la información de la organización. Cabe señalar que el uso de un centro de servicio convencional o de respuestas automatizadas no es una alternativa adecuada.
23	Se recomienda que la organización se asegure de que el centro de asistencia opere según un procedimiento de trabajo que incluya casos y respuestas, y que se examine al menos una vez al año si dicho procedimiento está actualizado, después de lo cual deberá ser aprobado por la dirección de la organización.
24	Se aconseja que la organización publique en los distintos canales de servicio las instrucciones para los usuarios sobre cómo hacer frente a las amenazas derivadas de la recepción de SMS maliciosos, incluyendo la información de contacto del centro de asistencia.

N.°	Recomendación
Asistencia para usuarios/clientes (cont.)	
25	Se sugiere que la organización realice publicaciones periódicas para incrementar la concienciación de los usuarios sobre el tipo de información siendo enviada y la naturaleza del servicio, indicando la información de contacto del centro de asistencia.
26	Se recomienda que la organización ofrezca una indemnización sin prueba de daños a los usuarios que resulten perjudicados directa y/o indirectamente por la recepción de un SMS de parte de la organización.
27	Se aconseja que la organización se asegure de que el usuario tenga acceso a una copia del contenido del mensaje enviado por SMS a través de un canal de servicio alternativo (por ejemplo, en un sitio web accesible después de iniciar sesión), incluyendo parámetros suficientes para demostrar la autenticidad del SMS recibido inicialmente como la fecha, la hora, la identidad del remitente y una copia del mensaje.

La distribución de publicidad por mensajes de texto (SMS) puede exponer tanto a la organización emisora como al destinatario a una serie de riesgos cibernéticos. Entre estos riesgos, caben destacar daños a la imagen de la organización como resultado de una campaña de suplantación de identidad (*phishing*), exposición jurídica como resultado de realizar actividades de manera contraria a requisitos legales para la transferencia de información y protección de la privacidad y riesgos en la cadena de suministro.

Como consecuencia de esto, la distribución de publicidad por SMS no es una práctica recomendada tanto para la organización como para sus clientes. Sin embargo, en los casos en que a pesar de ello la organización haya decidido utilizar esta tecnología, existen varias medidas de protección que pueden implementarse para ayudar a reducir los riesgos.

Este documento describe las principales amenazas que resultan del envío de publicidad por SMS y, sobre esta base, ofrece una serie de recomendaciones de implementación y mejores prácticas para ayudar a las organizaciones a mejorar sus procesos internos asociados a la transmisión de material informativo vía mensajes de texto y a minimizar los riesgos relativos a esta práctica.

El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que una organización esté preparada para defenderse de las amenazas cibernéticas, debe dominar una gran cantidad de especializaciones: tecnológicas, organizativas y de procesos. La lista de capítulos presentada a continuación refleja el estado de la colección al momento de la publicación de este documento.

Volumen A: Un enfoque metodológico

Volumen B: Un enfoque técnico

- **B.01** Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)
- **B.02** Seguridad de infraestructuras Access Point Name (APN)
- **B.03** Endurecimiento de sistemas informáticos
- **B.04** Reducción de riesgos de ciberseguridad en cámaras de videovigilancia
- **B.05** Reducción de los riesgos de ciberseguridad en los puntos finales de la organización
- **B.06** Seguridad de sistemas de planificación de recursos empresariales (ERP)
- **B.07** Preparación y respuesta ante un ataque de *ransomware* en la organización
- **B.08** Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.09** Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.10** Seguridad de infraestructuras de voz sobre protocolo de internet (VoIP)
- **B.11** Autenticación multifactor avanzada ante amenazas de ciberseguridad
- **B.12** Principales amenazas de ciberseguridad de las plataformas de asistencia remota a usuarios
- **B.13** Prevención y respuesta ante un secuestro de Border Gateway Protocol (BGP Hijacking)
- **B.14** Preparación ante ataques distribuidos de denegación de servicio (DDoS)
- **B.15** Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)
- **B.16** Ciberseguridad por medio de sistemas de gestión de dispositivos móviles (MDM/EMM)
- **B.17** Seguridad en la transferencia gestionada de archivos (MFT)
- **B.18** Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)
- **B.19** Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí
- **B.20** Seguridad de los sistemas multimedia
- **B.21** Integración de principios de ciberseguridad en los procesos de respaldo y recuperación

Volumen C: Desarrollo seguro de *software*