DESAFÍO DE LA CIBERSEGURIDAD EN LAS ORGANIZACIONES EN EL CONTEXTO DIGITAL ACTUAL RELACIONADO CON EL ODS NÚM. 9

THE CHALLENGE OF CYBERSECURITY IN ORGANIZATIONS IN THE CURRENT DIGITAL CONTEXT RELATED TO SDG 9

Xóchitl Hernández Torres[1], Elsa Ortega Rodríguez[2] y Rodrigo Aryan Hernández García[3]

RESUMEN

El desarrollo de nuevos productos y servicios tecnológicos enfocados al internet de las cosas, la industria 4.0 transforman cada vez más la vida y la forma de trabajo en las organizaciones. La pandemia del COVID 19, nos demostró tanto el potencial que tiene el mundo digital, así como la brecha digital existente a nivel mundial. Esta investigación teórica tiene como objetivo analizar el contexto actual de la ciberseguridad en las organizaciones y los desafíos asociados al uso de las tecnologías de la información (TI) que inciden en la competitividad de las organizaciones ante los riesgos de la ciberdelincuencia que prevalecen en el contexto digital del objeto de estudio. Este estudio adopta el enfoque documental explicativo, como aspecto de mejora de procesos organizacionales. Como resultado, se identifican los aspectos que mitiguen el riesgo y los beneficios asociados a la innovación e infraestructura de TI en las organizaciones, relacionado con el ODS núm. 9.

PALABRAS CLAVE: ciberseguridad, organizaciones, contexto digital, ODS#9, innovación

ABSTRACT

The development of new technological products and services focused on the Internet of Things, Industry 4.0, are increasingly transforming life and the way organizations work. The pandemic of COVID 19, showed us both the potential of the digital world, as well as the existing digital divide worldwide. This theoretical research aims to analyze the current context of cybersecurity in organizations and the challenges associated with

[1] Universidad Veracruzana, México. Estancia postdoctoral Conacyt Colver. xhernandez@uv.mx Colaboradora del cuerpo académico UV-CA-532. Tecnologías Emergentes en las Organizaciones. https://orcid.org/0000-0003-1044-6156

[2] Universidad Veracruzana, México. Investigadora de tiempo completo IIESCA. eortega@uv.mx Integrante del cuerpo académico UV-CA-532. Tecnologías emergentes en las Organizaciones. https://orcid.org/0000-0002-1088-276X

[3] Universidad Veracruzana, México. Profesor de Asignatura. Facultad de Contaduría y Administración. rodrhernandez@uv.mx. https://orcid.org/0000-0002-2299-5366

the use of Information Technology (IT) that affect the competitiveness of organizations in the face of cybercrime risks prevailing in the digital context of the object of study.

This study adopts the explanatory documentary approach, as an aspect of organizational process improvement. As a result, aspects that mitigate the risk and benefits associated with innovation and IT infrastructure in organizations related to SDG # 9 are identified.

KEYWORDS: cybersecurity, organizations, digital context, SDG#9, innovation.

1. INTRODUCCIÓN

El presente trabajo de investigación teórica considera la Agenda 2030, la cual reúne 17 objetivos y 169 metas, presenta una visión ambiciosa del desarrollo sostenible e integra sus dimensiones económica, social y ambiental. La Agenda 2030 es un instrumento que pone de manifiesto la igualdad y dignidad de las personas y acciona una nueva cultura en pro del medioambiente; asimismo, considera aspectos de innovación que pueden relacionarse con las organizaciones en el contexto digital actual, en lo particular con su objetivo 9: Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación (Agenda 2030, 2018).

La infraestructura de las tecnologías de información y comunicaciones resulta ser un activo importante en las organizaciones que buscan aportar al desarrollo sostenible de los países, por lo que la inversión en el sector tecnológico se convierte en una fortaleza para mantener la innovación en la organización.

Por otro lado, los temas de ciberseguridad representan un desafío para las organizaciones que forman parte de la industria 4.0 y que han implementado tecnologías relacionadas con el internet de las cosas (IoT), por lo que, para ser competitivos, es necesario mitigar los ciberataques que afecten su modelo de negocios.

La tecnología es importante en las organizaciones, una herramienta para mejorar la productividad y administración de sus sistemas; en este sentido, su aplicación y uso responsable contribuyen al cumplimiento del ODS núm. 9: Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación. De tal manera que la pregunta de investigación es: ¿qué necesitan las organizaciones para hacer frente a los desafíos de seguridad actuales?, ¿cómo impacta en el ODS núm. 9 el progreso tecnológico de una organización al gestionar riesgos y beneficios?

La pandemia por COVID 19 llevó a las organizaciones a dar un mayor uso a las tecnologías de la información (TI); si bien ya estaban presentes, muchas organizaciones no se habían

abierto al mundo digital. Incluso conceptos como POS (Point of Sale o puntos de venta en español), ERP (Enterprise Resource Planning / sistemas de planificación Empresarial), CRM (Customer Relationship Management / sistemas de administración de las relaciones con el cliente) no son nuevos para muchas de ellas; sin embargo, tras la pandemia se popularizaron.

El uso de las TI fue necesario para poder sobrevivir, y tratar de obtener una ventaja frente a la competencia; las TI e internet se convirtieron en sus aliados a través del uso de las redes sociales, el desarrollo de servicios web aplicados a la cadena de suministro, mejora de la comunicación y atención personalizada a los clientes; al desarrollo de aplicaciones móviles e incluso muchas organizaciones empezaron a utilizar diversos dispositivos de internet de las cosas (IoT), inteligencia artificial (IA) y servicios en nube para controlar y optimizar los procesos del negocio.

Las tecnologías de la información e internet contribuyeron a que las organizaciones pudieran desarrollarse, crecer y digitalizarse, ser más competitivas; con los que se demostró que son necesarias para el desarrollo sostenible, enmarcado en el ODS núm. 9 de la Agenda 2030 de las Organización de las Naciones Unidas (ONU), y poder mejorar la capacidad de innovación, la competitividad, incluso la calidad de vida de las personas; sin embargo, en este periodo de rápida aceleración de implementación de las TI, quedó demostrado que la falta de inversión en infraestructura de las mismas, genera una brecha digital importante que limita el desarrollo y la competitividad de los países subdesarrollados respecto a los desarrollados; sumado a ello, en el año 2020, la Comisión Económica para América Latina y el Caribe-CEPAL determinó que los avances realizados se vieron afectados por la pandemia del COVID-19, lo que conlleva a predecir el incumplimiento de la Agenda 2030, así como la necesidad de trabajar de forma objetiva y medible en un próximo consenso (Arce, 2022).

Aunado a lo anterior, los atacantes en materia de seguridad descubrieron nuevas formas de delinquir, que son menos riesgosas y más benéficas para ellos, trayendo así un nuevo desafío en materia de seguridad informática para las organizaciones.

Es aquí donde estas últimas se encuentran en un dilema: 1) evitar los riesgos digitales asociados a los hackeos sacrificando productividad, competitividad y desarrollo, alejándose de los compromisos de la Agenda 2030 en cuanto al ODS núm. 9 y comprometiendo, a la larga, la estabilidad y vida de la organización, 2) invertir en infraestructura de TI que les permita alinearse a un desarrollo sostenible conforme a la Agenda 2030 para obtener mayor presencia en el mercado, asumiendo los riesgos del

mundo digital, partiendo de que elijan la opción del desarrollo sostenible.

2. DESARROLLO

Este estudio adopta el enfoque documental explicativo con el objetivo de caracterizar el concepto de ciberseguridad dentro del contexto organizacional, y su relación en el ODS núm. 9 Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación, considerando las metas: 9.a Facilitar el desarrollo de infraestructuras sostenibles y resilientes en los países en desarrollo mediante un mayor apoyo financiero, tecnológico y técnico a los países africanos, los países menos adelantados, los países en desarrollo sin litoral y los pequeños Estados insulares en desarrollo; y 9.c Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a internet en los países menos adelantados, de aquí a 2030 (ONU, 2022).

La investigación se sustenta en los reportes de seguridad de empresas especializadas, identificando la tipología de las ciberamenazas y los riesgos resultantes; las contramedidas a tomar para hacer frente a los eventos de ciberataque, las pautas y soluciones para gestionar los problemas de ciberseguridad en las organizaciones.

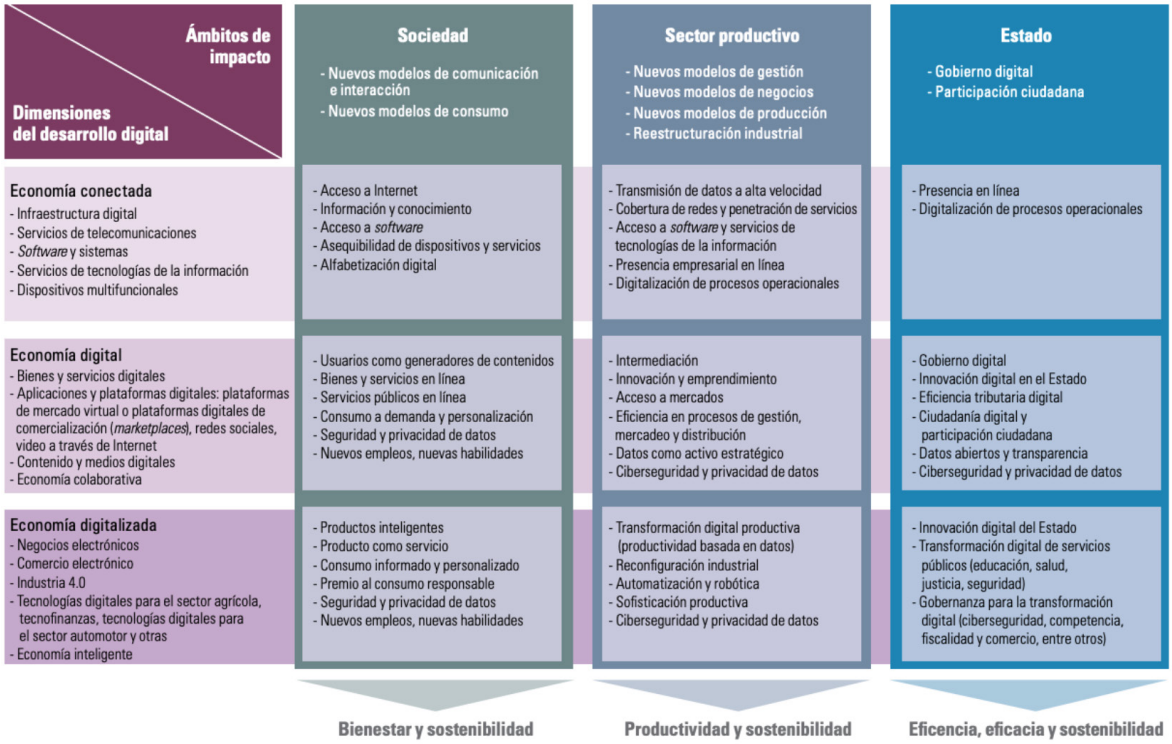
Para tal efecto, consideramos la revisión de los temas tratados en la Tercera Reunión de la Conferencia de Ciencia, Innovación y Tecnologías de la Información y las Comunicaciones de la Comisión de la América Latina y el Caribe, en donde el desarrollo y despliegue de la ciencia, las tecnologías y la innovación en la región son ejes centrales, para la obtención de la inclusión digital y el desarrollo de soluciones para un consumo y producción más sostenibles, relacionando de esta forma el ODS Innovación, Infraestructura y Tecnología.

2.1 Impacto de las TI en las organizaciones

La tecnología y el desarrollo digital impactan en el aumento del bienestar de las personas, la productividad de las organizaciones, así como el incremento de la eficiencia y la eficacia de los Estados, a través de la sinergia de sus tres dimensiones (Cepal, N. U., 2021):

i. Economía conectada: se refiere al despliegue de la infraestructura digital y la adopción creciente del uso de internet a través de diversos tipos de dispositivos.
ii. Economía digital: relacionada con los modelos de negocio basados en tecnologías digitales para la oferta de bienes y servicios.
iii. Economía digitalizada: surge al adoptar tecnologías avanzadas con efectos disruptivos, permitiendo a las industrias innovar sus modelos de negocios y producción, mediante la reconfiguración de sus cadenas de valor y la transformación de sus productos y servicios, tal como se visualiza en la (Figura 1).

Figura 1. Dimensiones y elementos del desarrollo digital y sus efectos en la sociedad, el sector productivo y el Estado



Nota: Imagen tomada de (Cepal, N. U., 2021)

El impacto de la digitalización entre los países, empresas y personas no es instantáneo ni homogéneo, por lo que se deben de considerar algunas variables identificadas comúnmente como competencia del personal, grado de adopción tecnológica y la gestión estratégica para asumir riesgos propios de la ciberseguridad, tales como la seguridad de los datos personales, la privacidad de datos, entre otros. Se requiere una visión sistémica de la digitalización, ya que el no contar con una estrategia integral de ciberseguridad, podría representar una vulnerabilidad en los bienes y servicios ofrecidos por las organizaciones, ante un entorno de riesgo cambiante.

Como se puede apreciar en la figura 1, la ciberseguridad tiene impacto en los ámbitos social, público y privado, al ser un elemento importante de las dimensiones del desarrollo digital, en virtud de que dicha transformación digital genera vulnerabilidad ante los ciberataques –los cuales pueden dañar los activos, la reputación, así como la competitividad de las organizaciones–.

En este sentido, es necesario implementar mecanismos de ciberseguridad, definida como:

> La práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil (Kaspersky, 2020).

Lo anterior nos indica que la ciberseguridad consiste en proteger la infraestructura de tecnologías de la información de ataques maliciosos, los cuales buscan obtener acceso a datos no autorizados para usos habitualmente delictivos. La seguridad informática debe garantizar la autenticidad, confidencialidad, integridad y disponibilidad de la información, pues de no hacerlo puede comprometer gravemente a las organizaciones.

2.2 Estado de la ciberseguridad en México y América Latina

Pese a que la implementación de diversos servicios de TI es indispensable para el desarrollo sostenible de las organizaciones, y que la información es un factor crítico para el éxito de estas, en la actualidad algunas organizaciones aún no toman en cuenta los riesgos y desafíos existentes en la seguridad de la información. De acuerdo con ESET Internet Security, en su reporte de seguridad de América Latina del año 2022, el país con la mayor cantidad de detecciones de malware en la región es Perú (18%), sin embargo, no tiene mucha distancia de México, que está en segundo lugar con un 17% de detecciones. El top 5 de detecciones de malware lo complementan Colombia (12%), Argentina (11%) y Ecuador (9%), respectivamente (Security Report Latinoamerica, 2022).

El crecimiento de malware no es el único problema de seguridad, de acuerdo al informe Microsoft Digital Defense Report 2022, la cantidad estimada de contraseñas vulneradas por segundo se incrementó un 74%. En el mismo reporte se indica que gran parte de los ataques fueron a través del uso de ransomware, un tipo de malware que secuestra los datos contenidos en los dispositivos infectados. Las demandas de rescate de datos también incrementó, siendo América Latina la región que ha sido mayormente golpeada por este tipo de ataques (Microsoft, 2022).

El reporte de Fortiguard Labs, unidad de la empresa de seguridad, indica que América Latina sufrió más de 289 mil millones de intentos de ciberataques en 2021, un crecimiento de cerca del 600% respecto al año 2020, en donde México fue el país que más ataques tipo denegación distribuida de servicio (DDoS) recibió: 156 mil millones; seguido de Brasil (88,5 mil millones), Perú (11,5 mil millones) y Colombia (11,2 mil millones). La suma de los ciberataques en la región representa el 10% de estos a nivel mundial. Si bien Estados Unidos, Japón, y gran parte de los países que conforman la Unión Europea

son los principales objetivos, México y América Latina cada vez empiezan a ser más objeto de mayores y sofisticados ataques, estos estudios permiten tener una visión de cómo se encuentra la situación de seguridad en la región de América Latina y en México principalmente. Los riesgos a los cuales las organizaciones se enfrentan todos los días son un desafío en aras del desarrollo, dado que implican un desgaste importante para la recuperación de la información cuando los ataques recibidos son exitosos (FortiGuard Labs, 2022).

Es por ello que, en este panorama de ciberseguridad, es importante que las organizaciones de cualquier tamaño, especialmente en nuestro país, tengan presentes los principales retos a los que se enfrentan; conocer las amenazas y poder combatirlas, así como comprender la importancia de la adquisición de infraestructura de TI, y la implementación de mecanismos de seguridad para su protección, ya que ninguna organización está exenta de sufrir algún tipo de ciberataque derivado de alguna debilidad o falla en el software, hardware o en las personas que utilizan la tecnología. De acuerdo con Fortinet®, líder mundial en soluciones de ciberseguridad amplias, integradas y automatizadas, un 86% de las pymes mexicanas no está preparada para amenazas y ocho de cada 10 no cuenta con las herramientas necesarias de protección, siendo estas más vulnerables que las organizaciones de mayor tamaño, como las grandes industrias corporativas (Fortinet, 2022).

El uso de las tecnologías de información y comunicaciones genera grandes beneficios y, al mismo tiempo, conlleva consecuencias negativas si las tecnologías son vulneradas y comprometen los recursos o activos digitales de la organización.

La transformación digital ha originado que las organizaciones puedan padecer algún tipo de ataque informático, puesto que las economías y sociedades dependen cada vez más de productos inteligentes que están expuestos a diversas amenazas que aprovechan las vulnerabilidades de la infraestructura digital. Estos tipos de ataques pueden incidir en los datos, como el simple robo de información de una empresa, robo de dinero en cuentas bancarias, hasta amenazar la seguridad humana, a través de vulnerar diversos dispositivos conectados a internet (IoT), tales como dispositivos para monitoreo de la salud, de vehículos, de edificios e incluso ciudades inteligentes (Smarts cities).

Lo anterior es generado por causas variadas, entre las que se encuentran: alguna vulnerabilidad o falla en los sistemas, uso inadecuado o malintencionado en el manejo de información confidencial o por el uso de ingeniería social, entre otras; lo que origina problemas de pérdida de información, indisponibilidad o alteración de datos, fallas en los sistemas operativos, estratégicos y financieros.

Tipos de ciberamenazas en las organizaciones

Como comenta Argueta (2022): "Los ciberataques no discriminan el tamaño o el tipo de organización. Existen advertencias de organismos internacionales ante esta situación, en el caso de México algunas organizaciones no toman las medidas adecuadas, en especial las más pequeñas".

Por lo que a través de esta investigación se identifica la importancia de que las organizaciones conozcan los principales tipos de ataques que son susceptibles de recibir y tomar conciencia de los riesgos que implican para prevenir y contener dichos ataques. Dentro de estos tipos de ataques podemos identificar en la tabla 1 los siguientes:

Tabla 1. Descripción de los diferentes tipos de ataques informáticos

Tipo de ataque	Descripción
Ataques de Denegación de servicios (DoS)	Envío de tráfico que interrumpe los servicios de red hasta superar su capacidad y dejarlos sin funcionar, existe una variante de este tipo de ataques, que se da de forma distribuida, desde varios equipos ubicados en diferentes países, a estos se les conoce como Ataques de denegación de servicios distribuidos (DDoS).
Ataques de ingeniería social:	El método de este ataque se centra en la manipulación psicológica, al tratar de engañar al usuario para que realice alguna acción que comprometa la seguridad de la empresa, dentro de estos tipos de ataques se encuentra el *Phishing* y sus variantes.
Phishing:	Consiste en suplantar la identidad de alguien más, este tipo de ataques maliciosos provenientes de correos electrónicos, mensajes en redes sociales o apps de mensajería que contienen información que pareciera provenir de fuentes confiables, y que ponen en riesgo la información personal o empresarial al dirigirlos a páginas ficticias con logos y marcas casi idénticas a las originales, es común hacerse pasar un banco, otra empresa, o incluso envío de archivos cfdi de supuestas compras.
Ataques de Malware:	Se refiere al uso de código malicioso que compromete la seguridad digital dentro de una organización, dentro de este concepto se considera a los virus, gusanos, caballos de troya, ransomware, spyware, entre otros, y buscan robar, secuestrar, eliminar información de los equipos de cómputo.
Ransomware:	Consiste en la inyección de un Malware para bloquear un dispositivo electrónico y cifrar sus archivos, impidiendo el acceso a la información almacenada en éstos. Para liberar la información los atacantes solicitan un rescate, habitualmente un pago en criptomonedas, sin embargo, rara vez otorgan las claves, por lo cual se considera en pérdida total de la información.
Ataques de fuerza bruta de	Intentan descifrar la contraseña del usuario, con el fin de tener acceso a su información personal o cuentas. No se requiere que el usuario de clic en algún enlace, ya que el atacante emplea palabras y combinaciones

contraseñas:	de información de uso común por el usuario para acceder a las cuentas, o el uso de software especializado para generar contraseñas a partir de diccionarios de datos, hasta que encuentra la combinación correcta.
Inyección SQL:	Este tipo de ataque informático es considerado de los más graves, ya que se infiltra código malicioso aprovechando errores y vulnerabilidades de un sistema, con conexión a bases de datos tipo SQL, para así tomar acceso de administrador, robar o manipular la información contenida en dichos sistemas.
***Cross Site Scripting*:**	Implementación de scripts maliciosos en sitios web habitualmente de tipo Javascript, que, aprovechando vulnerabilidades de los sitios, permiten ejecutar código malicioso
***Spyware*:**	Es un tipo de código malicioso que rastrea los movimientos de los usuarios, servicios a los que acceden, sitios web, horas, frecuencia, para construir un perfil de la víctima.
RAT *Remote Administration Tools*	Son herramientas que pueden ser instaladas mediante un *Malware* y el uso de ingeniería social, y que permiten tomar el control total de un dispositivo de forma remota
Nota: Estos no son los únicos tipos de ataques, pero si los más representativos y utilizados por los cibercriminales. Datos sintetizados de la información proporcionada ESET(2022), Microsoft(2022), FortiGuard Labs(2022).	

2.4 Mecanismos de protección y minimización de riesgos en ciberseguridad

En el contexto actual, las organizaciones no están exentas de incurrir en riesgos de ciberseguridad, por lo que en la tabla 2 se enuncian algunas recomendaciones como medidas básicas preventivas de protección para disminuir los efectos de un ataque de seguridad, y aunque parecieran ser de conocimiento general, en muchos de los casos son obviadas.

Tabla 2. Principales tipos de ataques y medidas preventivas

Tipo de ataque	Medidas preventivas de protección
Denegación de servicio (DoS)	- Mantener actualizados los sistemas y el software asociado (parches de seguridad) - Monitorear el tráfico y los datos con el fin de identificar picos de actividad inusual o posibles amenazas
Phishing	- Revisar la dirección del remitente sobre todo en correos extraños o de desconocidos, sin olvidar revisar los provenientes de usuarios de confianza que parezcan dudosos. - Leer el correo electrónico antes de dar clic, sobre todo en enlaces de remitentes desconocidos - En caso de que solicite información fuera de lo común algún usuario de confianza, llamar o verificar con éste antes de entregarla. Recordar que las organizaciones “casi nunca” solicitan información personal por correo.

Malware	- Evitar dar clic en enlaces o descargas de fuentes desconocidas, que pueden contener código malicioso. - Realizar actualizaciones periódicas del software y programas utilizados tales como los sistemas operativos. - Instalación de equipos de seguridad para proteger los equipos en red. - Realizar respaldos periódicos de la información (copias de seguridad), verificando la correcta realización de una restauración.
Ataques de contraseña	- Revisar periódicamente sitios o boletines de seguridad que informen de servicios comprometidos o hackeados, en donde la organización pueda tener almacenadas información y contraseñas. Un sitio puede ser *Have i been pwned* - https://haveibeenpwned.com/ el que menciona sitios que fueron comprometidos y si algún correo conocido está dentro de éste. - Utilizar contraseñas seguras y variar en sus diferentes cuentas. Cambiarlas periódicamente - No almacenar las contraseñas en archivos almacenados en sus dispositivos inteligentes - Generar contraseñas robustas con al menos 14 caracteres, letras mayúsculas y minúsculas, caracteres especiales. Se puede utilizar gestores de contraseñas. - Utilizar autenticación multifactor, por ejemplo, la verificación de dos pasos de WhatsApp, de los tokens bancarios, etc.

Nota: La tabla muestra las recomendaciones básicas para los principales tipos de amenazas, sin embargo, existen tipos de ataques más especializados para los cuales se requiere tomar otras medidas.

Además de las recomendaciones mencionadas, existen instituciones que brindan orientación para defenderse de ataques específicos, por ejemplo, el proyecto OWASP, del inglés: Open Web Application Security Project, organización sin fines de lucro que busca concientizar a las organizaciones sobre la seguridad de información en los servicios web y que, cada cierto tiempo, realiza un estudio en el cual establece las principales fallas y ataques utilizados para vulnerar a las organizaciones y que puedan tenerlas como un foco de atención que proteger; en la última edición se contemplan los principales objetivos de ataques al año 2021, siendo los siguientes los más socorridos por los criminales: (OWASP, 2022).

- Pérdida de control de acceso
- Fallas criptográficas
- Inyección
- Diseño inseguro
- Configuración de seguridad incorrecta
- Componentes vulnerables y desactualizados

- Fallas de identificación y autenticación; en el software y en la integridad de los datos; en el registro y monitoreo
- Falsificación de solicitudes del lado del servidor (SSRF)

Dichos mecanismos de protección deben ser considerados en las acciones de ciberseguridad, alineadas a los objetivos estratégicos de la organización, con el propósito de asegurar la continua operación de la organización. Para ello, se requiere identificar los activos críticos de la empresa (sistemas y servicios informáticos, así como los dispositivos móviles que acceden a la información corporativa y de los usuarios); implementar políticas y controles de seguridad digital, con el compromiso de la organización desde la alta dirección e incluyendo a todos los empleados que tengan acceso a la información a proteger; contar con personal capacitado y especializado en seguridad informática con un perfil de investigación, que realice los análisis de riesgos, defina planes de contingencia en caso de que se produzca un incidente de seguridad, asignando los recursos de seguridad disponibles para controlar dicho riesgo, conforme a los estándares de seguridad tales como ISO27001/ISO207002, COBIT, entre otros.

En este sentido, para contribuir al logro del ODS núm. 9 de la Agenda 2030, es conveniente que las organizaciones independientemente de su sector y tamaño, innoven en sus procesos, implementando tecnologías de la información disruptivas como la inteligencia artificial, Big data, y los servicios en nube; asimismo, es necesario fomentar la capacitación del recurso humano e invertir en los aspectos de ciberseguridad a fin de proteger a la cadena de valor, y propiciar un desarrollo económico sostenible, y sustentable.

Tener en cuenta la implementación de mecanismos de ciberseguridad conlleva a que las organizaciones sean resilientes ante el contexto global, en el que la innovación de sus procesos a través de las TI juegan un papel vital en la competitividad y desarrollo, toda vez que las organizaciones comparten información, forman cadenas de valor, promoviendo entre ellas la capacidad tecnológica y la gestión de la innovación que les permiten un crecimiento sostenible.

3. CONCLUSIONES

La dimensión transfronteriza que implica la economía digital permite utilizar los lineamientos internacionales establecidos para las áreas que la integran, además de trabajar en un marco institucional nacional que fortalezcan la competitividad e impulsen la inclusión, la equidad y la innovación.

Es por ello que se requiere de una visión estratégica para la implementación de acciones y políticas públicas que permitan el fortalecimiento de las tecnologías de información,

su aprovechamiento en el uso continuo a partir de la oportuna identificación de los beneficios y riesgos que conlleva la digitalización en las organizaciones, para contribuir a una transformación de interacción social, de consumo y de producción, lo que implica un desarrollo sostenible y de impacto económico para la sociedad. Dentro de estas tecnologías digitales podemos mencionar las redes móviles, el internet de las cosas (IoT), la computación en la nube, la inteligencia artificial, Big data, entre otras.

La Agenda 2030 enfatiza la recomendación de la gobernanza del desarrollo digital en el que las organizaciones puedan crear políticas digitales que permitan su impulso y ordenamiento, con el fin de incorporarlas en la economía y en la sociedad, sobre todo en aquellos países subdesarrollados que presentan una importante brecha digital sobre los desarrollados.

A partir de lo anterior, se deberán actualizar los marcos legales en diferentes ámbitos como las telecomunicaciones, particularmente en áreas como la ciberseguridad, la protección de datos personales y la aplicación de la inteligencia artificial, entre muchos otros. Dicha gobernanza deberá impulsar un modelo de producción competitivo y sustentable basado en las nuevas tecnologías, a fin de avanzar en la conformación de una sociedad digital inclusiva, la transformación digital del sector productivo, así como fortalecer la confianza y la seguridad digital (ciberseguridad).

A partir de esta investigación, se analizó la necesidad de visualizar sistémicamente a la digitalización en las organizaciones como parte de una estrategia integral de ciberseguridad para resistir la vulnerabilidad ante un entorno de riesgo cambiante, por lo que las organizaciones deberán asumir que la ciberseguridad es un proceso continuo de mejora que requiere de políticas y controles internos que atiendan las amenazas y minimicen riesgos de ataques que comprometan la integridad, confidencialidad y disponibilidad de la información.

Así como crear conciencia de la importancia de la ciberseguridad siendo un aspecto de atención primordial, por lo que elevar el nivel de defensa ante posibles ataques, mediante la adquisición de infraestructura de TI y la implementación de mecanismos de seguridad para su protección deben ser parte de acciones integrales alineadas a los objetivos estratégicos de la organización.

Para que las organizaciones sean competitivas en un entorno global, es necesario que comprendan la importancia de proteger sus activos digitales e infraestructura de tecnologías de la información, el papel que juegan los mismo en la innovación, en la mejora de sus procesos organizacionales, en la inclusión de sus colaboradores en la cultura digital, así como en la cadena de valor, marcado por la alta digitalización.

En este contexto, y como parte de futuras investigaciones, se recomienda que las organizaciones consideren los marcos normativos en paralelo con la generación de lineamientos de trabajo en materia de tecnologías de información, con la premisa de que la digitalización, puede mejorar los procesos a través de la innovación y fortalecimiento de infraestructura tecnológica coadyuvando a reducir riesgos en la seguridad de la información, con impacto en el ODS núm. 9.

4. FUENTES DE CONSULTA

Agenda 2030. (Enero de 2018). CEPAL. Obtenido de Agenda 2030 y los Objetivos de Desarrollo Sostenible Una oportunidad para América Latina y el Caribe: https://repositorio.cepal.org/bitstream/handle/11362/40155.4/S1700334_es.pdf?sequence=18&isAllowed=y

Ahmed, N. (Oct de 2019). Cyber Criminals and Attack Types. Obtenido de https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=b3971f90-1808-46e1-9c2e-72835032aaff%40redis

Arce, K. (2022). Políticas públicas sobre tecnologías de la información y comunicación (TIC): el ODS 9 de la Agenda 2030. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Letras y Ciencias Humanas, Escuela Profesional de Bibliotecología y Ciencias. Obtenido de Repositorio institucional Cybertesis UNMSM.

Argueta, E. L. (2 de Septiembre de 2022). Aumenta vulnerabilidad de pymes ante ciberataques; México el más afectado en Latinoamérica. . Obtenido de El Economista. : https://www.eleconomista.com.mx/el-empresario/Aumenta-vulnerabilidad-de-pymes-ante-ciberataques-Mexico-el-mas-afectado-en-Latinoamerica-20220901-0108.html

CEPAL. (01 de junio de 2022). Pandemia del COVID-19 pone en riesgo la integralidad de la Agenda 2030 debido al dispar avance de los ODS, advierte Alicia Bárcena. Obtenido de Cepal: https://www.cepal.org/es/noticias/pandemia-covid-19-pone-riesgo-la-integralidad-la-agenda-2030-debido-al-dispar-avance-ods

Cepal, N. U. (13 de diciembre de 2021). Innovación para el desarrollo. La clave para una recuperación transformadora. Obtenido de Tercera Reunión de la Conferencia de Ciencia, Innovación y TIC de la CEPAL: https://innovalac.cepal.org/3/sites/innovalac3/files/c2100805_web.pdf

Cepal, N. U. (05 de Agosto de 2021). La Inversión Extranjera Directa en América Latina y el Caribe 2021. Obtenido de Repositorio: https://www.cepal.org/es/publicaciones/47147-la-inversion-extranjera-directa-america-latina-caribe-2021

Cisco. (s.f.). ¿Qué es la ciberseguridad? Recuperado el 20 de Noviembre de 2022, de Cisco.com: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

FortiGuard Labs. (02 de agosto de 2022). América Latina sufrió más de 289 mil millones de intentos de ciberataques en 2021. Obtenido de Fortinet: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021

Fortinet. (28 de abril de 2022). Riesgo aumenta con brecha de habilidades en ciberseguridad, mientras que el 87% de las empresas latinoamericanas revela

haber sido hackeadas en el último año. Obtenido de Fortinet: https://fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-2022-cybersecurity-skills-gap-survey

Kaspersky. (2020). ¿Qué es la ciberseguridad? Obtenido de Kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

MAURER, T. M. (octubre de 2014). Compilation of Existing Cybersecurity and Information Security Related Definitions. . Obtenido de Federal Department of Foreign Affairs, Switzerland. : https://d1y8sb8igg2f8e.cloudfront.net/documents/compilation-of-existing-cybersecurity-and-information-security-related-definitions.pdf

Microsoft. (2022). Microsoft Digital Defense Report 2022: Illuminating the threat landscape and empowering a digital defense. Obtenido de https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

OECD. (03 de Febrero de 2021). Background report: Responsible management, handling and disclosure of digital security vulnerabilities. Obtenido de OECD: https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf

OECD. (2021). Enhancing the digital security of products: A policy discussion. Obtenido de OECD Digital Economy Papers, No. 306, OECD Publishing, Paris: https://doi.org/10.1787/cd9f9ebc-en

OECD. (2022). Obtenido de Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415

OECD. (Febrero de 2022). OECD work on digital security policy. Obtenido de https://www.oecd.org/digital/ieconomy/digital-security/oecd-work-on-digital-security-policy.pdf

ONU. (2022). Objetivos de desarrollo sostenible. Obtenido de Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación: https://www.un.org/sustainabledevelopment/es/infrastructure/

OWASP. (2022). Top 10: 2021. Obtenido de https://owasp.org/Top10/es/

Security Report Latinoamerica 2022. (julio de 2022). Obtenido de We Live Security: https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf

Tascón, M. (2016). Big data y el internet de las cosas: qué hay detrás y cómo nos va a cambiar. Los Libros de la Catarata. Obtenido de https://ojs.uv.es/index.php/eutopias/article/view/18701