Año 2025, Vol. 22, Nº 3, pp. 139- 155.
DOI: https://doi.org/10.35628/resup.v16i2.178

Ciberdefensa: Una opción para reforzar las capacidades de Ciberseguridad en el Perú

Cyberdefense: An Option to Strengthen Cybersecurity Capabilities in Peru

Recibido: 18 de agosto del 2025 | Aceptado: 05 de diciembre de 2025

José Aguirre R
https://orcid.org/0009-0006-8430-6243
Capitán de Fragata de la Marina de Guerra del Perú, Licenciado en Ciencias Marítimo Navales, Maestro en Dirección Estratégica en Telecomunicaciones, Ingeniería de Sistemas y Seguridad Informática. Doctorando en Proyecto de Ciberseguridad y Ciberdefensa, Certificaciones en Seguridad de la Información, Continuidad de Procesos, I.A. entre otros. Con amplio recorrido en soluciones seguridad, tecnologías de la información y telecomunicaciones, gestión de recursos y optimización de procesos. Docente de Ciberseguridad y TIC´s.
Email:josejo2@proton.me

Resumen: El presente artículo examina cómo las capacidades de ciberdefensa pueden apoyar y fortalecer las actividades de ciberseguridad en el contexto peruano. A través del análisis del caso de los Juegos Panamericanos y Parapanamericanos Lima 2019, se evalúa cómo la incorporación de estrategias y procedimientos operativos propios de la ciberdefensa, mejoró la resiliencia cibernética frente a posibles ciberamenazas, destacando su aplicabilidad en la protección de activos críticos nacionales. La relación entre la ciberseguridad y la ciberdefensa se discute desde un enfoque teórico y práctico, aportando una visión estratégica de cómo estas capacidades pueden integrarse para fortalecer la seguridad digital en el Perú.

Palabras Clave: Ciberdefensa, Ciberseguridad, Resiliencia Cibernética, Activos Críticos, Juegos Panamericanos Lima 2019, Perú, Estrategia Digital.

Abstract: *This article examines how cyberdefense capabilities can support and strengthen cybersecurity activities within the Peruvian context. Through the analysis of the Lima 2019 Panamerican and Parapanamerican Games case, it evaluates how the incorporation of strategies and operational procedures specific to cyberdefense enhanced cyber resilience against potential cyber threats, highlighting their applicability in protecting national critical assets. The relationship between cybersecurity and cyberdefense is discussed from both theoretical and practical perspectives, offering a strategic view of how these capabilities can be integrated to reinforce digital security in Peru.*

Keywords: *Cyberdefense, Cybersecurity, Cyber Resilience, Critical Assets, Lima 2019 Pan American Games, Peru, Digital Strategy.*

1. INTRODUCCIÓN

La creciente y vertiginosa dependencia de la tecnología en las infraestructuras críticas de un Estado, su desarrollo y las amenazas cibernéticas, han llevado a los países a adoptar medidas rigurosas de protección. En este contexto, la ciberseguridad y la ciberdefensa juegan roles centrales. La ciberseguridad se centra en proteger sistemas y redes frente a ataques cibernéticos, mientras que la ciberdefensa involucra medidas defensivas y ofensivas para salvaguardar la soberanía y seguridad nacional en el ciberespacio. Ante la creciente amenaza que los ciberataques representan, ambos conceptos han adquirido relevancia estratégica y operativa en el Perú, donde se han implementado leyes específicas para regular estas actividades (Ministerio de Defensa, 2019; Ley N° 30999, El Peruano, 2019), como se muestra en el transcurso de este texto.

El objetivo general de este artículo enfocado en la investigación, es demostrar que las capacidades de ciberdefensa pueden complementar y fortalecer las actividades de ciberseguridad en el Perú, particularmente en la protección de activos críticos nacionales (ACN). En el contexto de los XVIII Juegos Panamericanos y VI Juegos Parapanamericanos de Lima 2019, el uso de estas capacidades en la protección de infraestructuras digitales temporales se presenta como un caso de estudio relevante, para analizar cómo la ciberdefensa y la ciberseguridad pueden actuar de manera sinérgica. La hipótesis del estudio sugiere que la integración de la ciberdefensa en los procesos de ciberseguridad mejora el tiempo de respuesta frente a incidentes de seguridad y, en consecuencia, aumenta la efectividad de la protección de los activos digitales.

2. MARCO TEÓRICO

De acuerdo con la Stanford University (2020) la ciberseguridad es conjunto de técnicas utilizadas para proteger la integridad de las redes, programas y datos contra ataques, daños o accesos no autorizados. En el contexto nacional, se define la ciberseguridad como la "capacidad de preservar el adecuado funcionamiento de los activos informáticos, protegiéndolos de amenazas y vulnerabilidades…" (DU N° 007-2020, El Peruano, 2020). La ciberseguridad en el Perú se fundamenta en la preservación de tres principios, que funcionan también como pilares de este concepto: disponibilidad, integridad y confidencialidad de la información en el ciberespacio, aplicables tanto a sectores públicos como privados, especialmente aquellos vinculados a los activos críticos nacionales.

Por otro lado, la ciberdefensa, con una trayectoria relativamente reciente en el Perú, surgió como una estrategia dentro del Ministerio de Defensa con la creación de los Comandos de Ciberdefensa del Ejército y la Marina entre los años 2018 y 20191. De acuerdo con Ley N° 30999 (2019), esta describe a la ciberdefensa como "la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional…"

También y de acuerdo con Sáinz (2016) la ciberdefensa no solo implica proteger los sistemas propios, sino también realizar operaciones ofensivas y de inteligencia para neutralizar amenazas. Del marco legal descrito en el párrafo precedente, se subraya la importancia de que las capacidades defensivas y ofensivas del Estado peruano en el ciberespacio sean organizadas y ejecutadas de forma que permitan responder adecuadamente a las amenazas externas, tomando en cuenta la definición que la Cooperative Cyber Defence Center Of Excellence de la NATO (2013) hace al ciberespacio, como "…el entorno en el que se desarrollan las operaciones de ciberdefensa para proteger y defender los sistemas de información y las redes contra amenazas y ataques cibernéticos".

Es importante mencionar que los incidentes de seguridad informática son recurrentes en las redes de datos de todas las organizaciones y forman el quehacer diario en los diferentes Centros de Operaciones de Seguridad (SOC) de las entidades que operan en el Estado peruano, tanto públicas como privadas. Es así que dentro de las entidades privadas en el país, cualquiera fuese su rubro, algunas de ellas se han encargado también de su propia seguridad informática; por ello han optado por gestionar la seguridad de su información, con personal y procesos propios, bajo el soporte de la tecnología necesaria y así lograr alcanzar este objetivo.

Vinculado a ello, existen otras entidades privadas que buscan tercerizar su seguridad de información e informática, con empresas dedicadas al rubro. En

este punto, cabe resaltar que existen entidades privadas que brindan servicios de protección y seguridad informática, donde se puede inferir que estas últimas al brindar estos servicios, tienen la suficiente autonomía para la protección de su propia información y redes informáticas, al contar una madurez mayor en procesos de seguridad de la información y ciberseguridad. Asimismo, tenemos a las entidades públicas, donde algunas de ellas manejan información de seguridad a nivel bajo, medio e información no sensible, generada producto de sus actividades diarias.

Por otro lado, tenemos a las entidades públicas que gestionan el manejo de información para operaciones que sostienen servicios ligados con activos críticos nacionales (ACN); estos activos críticos nacionales son de gran interés para la Nación, dado que la continuidad de sus operaciones tiene impacto directo en la ciudadanía y en las actividades que generan recursos para el Estado.

En ese sentido, las entidades que administran los ACN se convierten en un interesante blanco para los ciberataques, los cuales podrían ser realizados por los siguientes actores y sus respectivas capacidades:

FIGURA 1

Escala de actores vs. sus capacidades en el ciberespacio (Ecosistema de las ciberamenazas)

Fuente: Unidades de Ciberinteligencia y ciberguerra al servicio de Estados (Cubeiro E. 2021)

El vínculo entre ciberseguridad y ciberdefensa en el Perú se podría establecer a través de la coordinación de sus capacidades, sin perjuicio de las normas mencionadas en los párrafos precedentes y que describen sus funcionalidades. La ciberseguridad, desde un enfoque preventivo y reactivo, implica la capacidad de detectar y reaccionar frente a ataques para proteger la integridad de los sistemas. La ciberdefensa, por su parte y en adición, aporta capacidades de explotación y respuesta, siendo esta última la proyección del poder en el ciberespacio para contrarrestar a adversarios, de forma preventiva y correctiva. De este modo, ambas capacidades se complementan: mientras la ciberseguridad protege a los sistemas de ataques, la ciberdefensa amplía este rol al crear una estrategia ofensiva para enfrentar a actores hostiles (Faliero, 2020, p. 65).

3. BREVE RESEÑA DE LA METODOLOGÍA

La investigación para este artículo utiliza una metodología de revisión documental y análisis de caso. En primer lugar, se realizó una revisión sistemática de la legislación y teorías asociadas a la ciberseguridad y la ciberdefensa, tanto en el ámbito nacional como internacional, con especial enfoque en los conceptos de ciberespacio, ciberseguridad y ciberdefensa, y la interrelación y vínculos en las actividades de estos conceptos. En segundo lugar, se analizó el caso de éxito de los Juegos Panamericanos y Parapanamericanos de Lima 2019, evento en el cual se implementaron capacidades de ciberdefensa y ciberseguridad para proteger la infraestructura digital del evento. La hipótesis se valida a través de indicadores, como el tiempo de reacción frente a incidentes de seguridad, y la efectividad de los procedimientos operativos de ciberdefensa implementados.

Análisis del Caso de Éxito: Juegos Panamericanos y Parapanamericanos Lima 2019

Los Juegos Panamericanos y Parapanamericanos de Lima 2019 representaron un evento de gran magnitud en el Perú, considerado un activo crítico nacional temporal. En este contexto, la infraestructura digital del evento fue objeto de una estrategia de ciberseguridad y ciberdefensa que incluyó la implementación de un Centro de Operaciones de Seguridad (SOC). Este centro tuvo la finalidad de monitorear y proteger los sistemas y redes del evento. La Marina de Guerra del Perú fue la entidad responsable de liderar las actividades de ciberdefensa, en coordinación con el Proyecto Especial de los Juegos Panamericanos y Parapanamericanos (PEJP), y el sector privado, que incluyeron a las empresas nacionales e internacionales líderes en el aseguramiento en transmisión de datos y su respectiva seguridad informática.

El SOC, implementado en las instalaciones del Centro de Convenciones de Lima (CCL), contó con personal de la Marina y de otras fuerzas, quienes implementaron una serie de procedimientos operativos para monitorear y responder ante incidentes de seguridad en tiempo real. Los procedimientos de ciberdefensa incluyeron actividades de detección de malware, ataques DDoS, amenazas en redes sociales y amenazas de ransomware. En términos de métricas, el SOC logró reducir el tiempo de reacción frente a incidentes de seguridad, mediante la implementación de protocolos de ciberdefensa que optimizaron la respuesta y mitigación de los ataques detectados. Este caso permitió demostrar que la combinación de ciberseguridad y ciberdefensa mejoró significativamente la resiliencia cibernética en un evento de alto perfil.

Resultados de la investigación

El análisis del caso de los Juegos Panamericanos y Parapanamericanos de Lima 2019 evidenció una clara mejora en las capacidades de respuesta ante incidentes de seguridad, gracias a la integración de procedimientos de ciberdefensa en las actividades de ciberseguridad. Las métricas de tiempo de reacción, comparadas con los tiempos promedio de incidentes gestionados en otros contextos, demostraron que el uso de protocolos de ciberdefensa permitió responder de manera más rápida y efectiva.

Además, el caso evidenció que los procedimientos de ciberdefensa influyeron positivamente en la protección de los activos críticos del evento, al establecer una barrera adicional frente a ciberamenazas avanzadas (Rodríguez, 2020, p. 86).

Ahora bien, en el análisis de los resultados se analizarán las diferencias entre los tiempos de reacción, sometiendo las métricas obtenidas a los cálculos de las fórmulas establecidas (ensayos propios) para su evaluación. Se emplearán los siguientes cálculos:

- IPC = ∑ PROCEDIMIENTOS VINCULADOS DE CIBERDEFENSA (PVCD)
- PR = ∑ PROCEDIMIENTOS REGULARES DE CIBERSEGURIDAD (PRCS)
- TRA = ∑ TIEMPO DE ACTIVIDADES DONDE SE CONSIDERAN PROCEDIMIENTOS DE CIBERDEFENSA (TAPCD)
- TR = ∑ TIEMPO DE ACTIVIDADES DONDE NO SE CONSIDERAN PROCEDIMIENTOS DE CIBERDEFENSA (TANPCD)

En ese sentido de la siguiente formula general:

$$Si,\ IPC \geq PR \Rightarrow TRA < TR$$

Obtendremos la siguiente formulada detallada con las métricas a calcular:

$$SI,\ \sum(PVCD) > \sum(PRCS) \Rightarrow \sum(TAPCD) < \sum(TANPCD)$$

En análisis comparativo, se trataron los eventos e incidentes de seguridad informática con la intervención de las actividades de ciberseguridad, respecto a la posterior implementación de los procedimientos de ciberdefensa asociados a cada uno de los eventos e incidente de seguridad.

A continuación, presento el cuadro resumen, para visualizar de forma clara los tiempos mínimos tomados en las actividades de ciberseguridad y los procedimientos de ciberdefensa, con respecto a los eventos e incidentes de seguridad informática:

TABLA 1

Cuadro resumen con las métricas tomadas de las actividades de ciberseguridad y los procedimientos de ciberdefensa.

	EVENTOS E INCIDENTE DE SEGURIDAD INFORMÁTICA	ACTIVIDADES DE CIBERSEGURIDAD	TIEMPO EMPLEADO PARA REACCIÓN	PROCEDIMIENTO DE CIBERDEFENSA ASOCIADO	TIEMPO MÍNIMO ALCANZADO PARA LA REACCIÓN
1	Ataque por inserción de virus	Actividad de detección y reacción	51 minutos	Procedimiento para la detección de virus/malware	28 minutos
2	Ataque por inserción de malware de tipo gusano y troyano	Actividad de reacción antimal-ware	38 minutos	Procedimiento para la detección de malwares de tipo gusano/ troyanos	32 minutos
3	Ataque por inserción de malware de tipo spyware/ rootkit/otros	Actividad de reacción antimalware	38 minutos	Procedimiento para el ataque de malware tipo spyware/rootkit/ otros	26.5 minutos
4	Ataque de denegación de servicio simple y distribuida	Acción automáti-ca de reacción ante ataque DoS y DDoS	Inmediato, a re-acción de la her-ramienta (hasta una capacidad "Y" en GB)	Procedimiento para el ataque de DDoS	Inmediato, a reacción de la herramienta (hasta una capacidad "Y + 15" en GB)
5	Ataque a las páginas Web de los JPP	Actividad de reacción ante defacement	75 minutos	Procedimiento para el ataque web defacement y otros	13 Minutos
6	Amenazas mediante redes sociales	Actividad de detección y reacción ante amenazas por redes sociales	125 minutos	Procedimiento para las amenazas por redes sociales de los JPP	36 Minutos
7	Ataques que ocasionan la pérdida de conectividad de las redes inter-nas y externas de los JPP	Actividad de reacción ante pérdidas de conectividad	55 minutos	Procedimiento para la pérdida de conectividad por ataques	38 minutos

8	Ataque de tipo ransomware	Actividad de reacción ante eventos de tipo ransomware	Indeterminado	Procedimiento para el ataque de tipo ransomware	6 Minutos, para el aislamiento del equipo y pasa a forense
9	Identificación de amenazas latentes en la red en contra de los JPP	Indeterminado	Indeterminado	Procedimientos para la activación de la capacidad de explotación	37 Minutos
10	Ataque al funcionamiento del SIEM	Indeterminado	Indeterminado	Procedimiento ante caída del SIEM por ataques externos e interno	8.3 Minutos
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Actividad de reacción ante fallas de seguridad por usuarios	Entre 40 a 50 minutos, varios casos	Procedimientos ante fallos de operación o manipulación de usuarios	Entre 15 y 20 minutos, varios casos
12	Generación de eventos disruptivos	Protocolos ante eventos sísmicos o siniestros	10.5 minutos	Procedimientos ante eventos disruptivos (Desastres naturales)	2.7 minutos
13	Generación de siniestros y otros	Protocolos ante eventos sísmicos o siniestros	10.5 minutos	Procedimiento ante eventos de siniestros, inundaciones, otros	1.4 minutos

Fuente: Elaboración propia.

Ahora bien, como se puede apreciar en el cuadro N° 1, en la gran mayoría de los casos los procedimientos de ciberdefensa implementados tienen menores tiempos de reacción que las actividades de ciberseguridad por sí solas. Menciono en la mayoría de los casos, dado que para algunos eventos de seguridad no se implementaron actividades de reacción en ciberseguridad, como son los casos de los ataques de tipo ransomware, las amenazas identificadas y latentes en contra de los JPP, ataque a la operatividad del Gestor de Eventos de Seguridad de la Información o conocido por su traducción al inglés, como Security Information

and Event Management (SIEM), entre otros. En ese sentido, en ese momento los procedimientos de ciberdefensa abordaron todos esos eventos, y donde estos procedimientos tuvieron coincidencia con las actividades de ciberseguridad, los tiempos de reacción favorecieron a estos procedimientos de ciberdefensa versus las actividades de ciberseguridad. Resumiendo, este punto distingue a los procedimientos de ciberdefensa, al estar altamente entrenados con protocolos bien definidos, una distinción que marcaría una gradual mejora en este caso en particular, sobre las actividades de ciberseguridad en los Juegos. A continuación, se muestra un detalle de las diferencias:

TABLA 2

Cuadro con métricas comparadas y sus respectivos porcentajes por eventos e incidentes de seguridad.

	EVENTOS E INCIDENTE DE SEGURIDAD INFORMÁTICA	ACTIVIDADES DE CIBERSEGURIDAD	PROCEDIMIENTO CIBERDEFENSA	RESULTANTE A FAVOR DE PROCEDIMIENTOS	PORCENTAJE DISMINUCIÓN
1	Ataque por inserción de virus	51 minutos	28 minutos	**23 Minutos Menos**	**45.10%**
2	Ataque por inserción de malware de tipo gusano y troyano	38 minutos	32 minutos	**6 Minutos Menos**	**15.79%**
3	Ataque por inserción de malware de tipo spyware/ rootkit/otros	38 minutos	26,5 minutos	**11,5 Minutos Menos**	**30.27%**
4	Ataque de denegación de servicio simple y distribuida	Inmediato, a reacción de la herramienta (hasta una capacidad "Y" en GB)	Inmediato, a reacción de la herramienta (hasta una capacidad "Y + 15 en GB)	**Mejora en la capacidad de la herramienta de 22 a 37 GB.**	**68% (Aumento en capacidad)**
5	Ataque a las páginas Web de los JPP	75 minutos	13 minutos	**62 Minutos Menos**	**82.67%**
6	Amenazas mediante redes sociales	125 minutos	36 Minutos	**89 Minutos Menos**	**71.20%**

7	Ataques que ocasionan la pérdida de conectividad de las redes internas y externas de los JPP	55 minutos	38 minutos	**17 Minutos Menos**	**30.91%**
8	Ataque de tipo ransomware	Indeterminado	6 Minutos, para el aislamiento del equipo y pasa a forense	Sin Cálculo	**100.00%**
9	Amenazas latentes en la red en contra de los JPP	Indeterminado	37 Minutos	Sin Cálculo	**100.00%**
10	Ataque al funcionamiento del SIEM	Indeterminado	8.3 Minutos	Sin Cálculo	**100.00%**
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Entre 40 a 50 minutos, varios casos	Entre 15 y 20 minutos, varios casos	30 Minutos Menos	**60.00%**
12	Generación de eventos disruptivos	10.5 minutos	2.7 minutos	7.8 Minutos Menos	**74.29%**
13	Generación de siniestros y otros	10.5 minutos	1.4 minutos	9.1 Minutos Menos	**86.54%**
				PROMEDIO (%)	**66.40%**

Fuente: Elaboración propia, con datos del SOC de los JPP.

Los procedimientos de ciberdefensa tienen, en promedio, un porcentaje del 66.40% en disminución del tiempo de reacción con respecto a las actividades de ciberseguridad; esto podría indicar que los cálculos en la fórmula general propuesta en la hipótesis serían positivos.

"Ataque a las páginas Web de los JPP", que se redujo de 75 a 13 minutos; esto evidencia de forma positiva, que efectivamente los procesos de ciberdefensa

aplicados a las equivalentes actividades de ciberseguridad, pueden sumar a sus capacidades de reacción.

En adición, eventos donde el tiempo de reacción es vital, porque no solo involucra la integridad física de los equipos, sino también a las personas encargadas de las operaciones, como el Centro de Operaciones de Seguridad (SOC) y el Centro de Operaciones de Tecnología (TOC), son los eventos referidos a los eventos disruptivos, los mismos que pueden presentarse en diferentes situaciones, pero que en esencia son los movimientos telúricos y los incendios, para los cuales se elaboraron procedimientos a medida de acuerdo a la distribución del recinto, cantidad de personas, tomas eléctricas, zonas de resguardo, salidas de emergencia, entre otros. Como podemos apreciar en el cuadro N° 2, en los procedimientos 12 (generación de eventos disruptivos) y 13 (generación de siniestros y otros) que, si bien es rescatable que estos ejercicios se practicaron con cierta regularidad y obtuvieron resultados aceptables, el entrenamiento realizado sobre la base de los procedimientos de ciberseguridad, le dieron a esta actividad una mejora del 74% y 86% respectivamente, en tiempo de reacción.

El porcentaje promedio de mejora se podría considerar como un aporte significativo de los procedimientos de ciberdefensa sobre las actividades de reacción de ciberseguridad. Este análisis previo se consolidaría con la ejecución de la fórmula descrita en la hipótesis propuesta.

Visualización de Resultados

Luego de evaluar y analizar respecto a los procedimientos de la ciberdefensa con las actividades de ciberseguridad, aplicamos la fórmula a los resultados obtenidos, con el siguiente detalle:

TABLA 3

Cuadro con Procedimientos de ciberdefensa y sus tiempos de reacción durante los JPP.

#	EVENTO O INCIDENTE DE SEGURIDAD INFORMÁTICA	PROCEDIMIENTOS CIBERDEFENSA
1	Ataque por inserción de virus	28 minutos
2	Ataque por inserción de malware de tipo gusano y troyano	32 minutos
3	Ataque por inserción de malware de tipo spyware/rootkit/otros	26.5 minutos
4	Ataque de denegación de servicio simple y distribuida	Inmediato, a reacción de la herramienta (hasta una capacidad "Y + 15 en GB)
5	Ataque a las páginas Web de los JPP	13 Minutos
6	Amenazas mediante redes sociales	36 Minutos
7	Ataques que ocasionan la perdida de conectividad de las redes internas y externas de los JPP	38 minutos
8	Ataque de tipo ransomware	6 Minutos, para el aislamiento del equipo y forense
9	Identificación de amenazas latentes en la red en contra de los JPP	37 Minutos
10	Ataque al funcionamiento del SIEM	8.3 Minutos
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Entre 15 y 20 minutos, varios casos
12	Generación de eventos disruptivos	2.7 minutos
13	Generación de siniestros y otros	1.4 minutos

Fuente: Elaboración propia, con datos del SOC de los JPP.

Al sumar los tiempos de estos procedimientos (en minutos), sobre la base de 12 procedimientos (no se toma en consideración el procedimiento de mitigación ante ataques de denegación de servicio simple y distribuido – DDoS, dado que no devela un tiempo perse, sino que demuestra una mejora en la capacidad de ancho de banda mientras recibe un ataque de denegación de servicio), se obtiene el siguiente resultado:

$$TRA = 28 + 32 + 26.5 + 13 + 36 + 38 + 6 + 37 + 8.3 + 20 + 2.7 + 1.4 = 248.9 \text{ Minutos.}$$

Cuyo promedio es entre 12 (cantidad de procedimientos sumados)

$$\text{Promedio IPC} = 248.9 \div 12 = 20.74 \text{ Minutos.}$$

- TR = ∑ TIEMPO DE ACTIVIDADES DONDE NO SE CONSIDERAN PROCEDIMIENTOS DE CIBERDEFENSA (TANPCD)

Los procedimientos de ciberseguridad respecto al caso de éxito alcanzaron tiempos aceptables de reacción en su ejecución; estas actividades y sus tiempos de reacción son los siguientes:

TABLA 4

Cuadro con las actividades de reacción de ciberseguridad y sus tiempos de reacción durante los JPP.

#	EVENTO O INCIDENTE DE SEGURIDAD INFORMÁTICA	ACTIVIDADES CIBERSEGURIDAD
1	Ataque por inserción de virus	51 minutos
2	Ataque por inserción de malware de tipo gusano y troyano	38 minutos
3	Ataque por inserción de malware de tipo spyware/rootkit/otros	38 minutos
4	Ataque de denegación de servicio simple y distribuida	Inmediato, a reacción de la herramienta (hasta una capacidad "Y" en GB)
5	Ataque a las páginas Web de los JPP	75 minutos
6	Amenazas mediante redes sociales	125 minutos
7	Ataques que ocasionan la perdida de conectividad de las redes internas y externas de los JPP	55 minutos
8	Ataque de tipo ransomware	Indeterminado
9	Identificación de amenazas latentes en la red en contra de los JPP	Indeterminado
10	Ataque al funcionamiento del SIEM	Indeterminado
11	Malos manejos de seguridad en los accesos y claves por parte de los usuarios	Entre 40 a 50 minutos, varios casos
12	Generación de eventos disruptivos	10.5 minutos
13	Generación de siniestros y otros	10.5 minutos

Fuente: Elaboración propia, con datos del SOC de los JPP.

Procedemos ahora con la suma de los tiempos de estas actividades de ciberseguridad (en minutos), pero en este caso, a diferencia de los 12 procedimientos usados en ciberdefensa, únicamente usaremos el tiempo de 9 actividades. De igual manera, la actividad que mitiga los ataques de denegación de servicio simple y distribuido DDoS, no devela un tiempo perse, sino un ancho de banda mientras recibe un ataque de denegación de servicio. Asimismo, no se registró una actividad de reacción en ciberseguridad para los ataques de tipo ransomware, ni para la identificación de amenazas latentes en la red contra los JPP.

Adicionalmente, en los eventos de seguridad que no cuenten con actividades de ciberseguridad que ayuden a mitigarlo, se asignará el tiempo de reacción

máximo alcanzado por una actividad de ciberseguridad. Entonces, se efectúa el siguiente cálculo:

TR = 51 + 38 + 38 + 75 + 125 + 55 + 75(*) + 75(*)
+ 75(*) + 50 + 10.5 + 10.5 = 678.0 Minutos.
(*) Tiempo alto de una actividad de ciberseguridad,
usado como reemplazo para actividades que no contaban con
reacción para un determinado evento de seguridad.
Cuyo promedio es entre 12 (cantidad de procedimientos sumados)
Promedio PR = 678.0 ÷ 12 = 56.50 Minutos.

Luego de la toma de métrica y cálculos, reemplazo en la fórmula propuesta en la hipótesis:

Si, IPC ≥ PR => TRA < TR

Entonces:
IPC = 13 Procedimientos de ciberdefensa
PR = 10 Actividades de reacción de ciberseguridad
TRA = 248.9 Minutos
TR = 678 Minutos

Si, 13 ≥ 10 => 248.9 < 678

Luego, como podemos visualizar, se cumple el postulado de la hipótesis, donde a mayor o igual cantidad de inclusión de procedimientos de ciberdefensa versus las actividades de ciberseguridad, se tiene que los tiempos de reacción ante eventos de seguridad, mejoran con respecto a los iniciales.

Esto evidencia que la hipótesis planteada para el trabajo de investigación es correcta.

Fórmula inicial de la hipótesis:
Si, IPC ≥ PR => TRA < TR

Fórmula de la hipótesis con datos de la investigación:
Si, 13 ≥ 10 => 248.9 < 678

4. UNA BREVE DISCUSIÓN

La experiencia de los Juegos Panamericanos y Parapanamericanos de Lima 2019 ofrece importantes lecciones sobre la integración de ciberdefensa y ciberseguridad en el Perú. Una de las principales lecciones es la necesidad de colaboración constante entre el sector público, privado y las Fuerzas Armadas para enfrentar los riesgos del ciberespacio de forma unificada. Si bien el caso demostró la eficacia de esta colaboración, también resaltó la necesidad de desarrollar protocolos más detallados para la cooperación en eventos futuros y la protección de infraestructuras críticas permanentes (Clarke, 2011, p. 75).

A nivel internacional, varios países han adoptado enfoques similares para integrar la ciberdefensa y la ciberseguridad en la protección de sus activos digitales. Países como Estados Unidos y el Reino Unido, han implementado comandos de ciberdefensa que colaboran directamente con agencias de ciberseguridad para proteger infraestructuras críticas. El caso peruano, aunque aún en desarrollo, muestra un progreso significativo hacia esta integración y plantea la posibilidad de ampliar estas capacidades en el futuro, especialmente en sectores vulnerables como energía, telecomunicaciones y banca (Sáinz, 2016, p. 124).

5. CONCLUSIÓN Y RECOMENDACIÓN

Los hallazgos de esta investigación demuestran que las capacidades de ciberdefensa pueden fortalecer significativamente las actividades de ciberseguridad en el Perú. La integración de procedimientos operativos de ciberdefensa en el contexto de los Juegos Panamericanos y Parapanamericanos de Lima 2019, optimizó el tiempo de respuesta frente a incidentes y aumentó la resiliencia del SOC de los juegos ante diversas ciberamenazas. Esta colaboración entre ciberseguridad y ciberdefensa subraya la importancia de una estrategia nacional coordinada, que permita enfrentar de manera efectiva los riesgos y amenazas del ciberespacio.

Se recomienda que el Estado peruano refuerce la colaboración entre entidades públicas y privadas en el campo de la ciberseguridad, promoviendo la participación de actores relevantes en los esfuerzos de ciberdefensa. Es crucial continuar fortaleciendo la capacitación y los recursos tecnológicos de los SOC´s, de modo que los protocolos de ciberdefensa puedan integrarse de manera efectiva en la ciberseguridad. Las lecciones aprendidas del caso de los Juegos Panamericanos, sugieren que una estrategia coordinada y adaptada a las necesidades de la ciberseguridad y ciberdefensa es fundamental para proteger los activos críticos nacionales.

Referencias

Baca, G. (2016). Introducción a las Seguridad Informática. México: Grupo Editorial Patria.

Bello, E. (2020). Ciberseguridad: Tipos de ataques y en qué consisten. Recuperado de: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Cari, P. (2013). Ciberdefensa – Ciberseguridad, Riesgos y Amenazas. Definición del concepto de ciberseguridad.

Clarke, R. & Knake, R. (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.

Clarke, R. (2011). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

Cubeiro, E. (2021). Unidades de ciberinteligencia y ciberguerra al servicio de Estados. Consultado el 7 de enero del 2022. Recuperado de ATALAYAR: https://atal.ayar.com/content/unidades-de-ciberinteligencia-y-ciberguerra-al-servicio-de-estados

DU N° 007-2020, El Peruano. (2020). Decreto de Urgencia N° 007-2020, Gobierno del Perú.

Faesen, L., Torossian, B., Mayhew, E. (2020). Conflicto en el ciberespacio Análisis de las amenazas y el estado del orden internacional en el ciberespacio. Recuperado de: https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/conflict-in-berspace/11

Faliero, R. (2020). "Cybersecurity Defense Strategies". *International Journal of Cyber Defense.*

Garzón, D., Ratkovich, J. C. y Vergara, A. (2017). Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala. Bogotá: Pontifica Universidad Javariana.

Ley N° 30999, El Peruano. (2019). Ley de Ciberdefensa, Gobierno del Perú.

Ministerio de Defensa (2019). Lineamientos para la ciberdefensa en el Perú. Lima: Ministerio de Defensa.

Puime, J. (2009). El ciberespionaje y la ciberseguridad.

Rodríguez, M. (2020). *El reto de la ciberseguridad en América Latina*. Editorial Seguridad Digital.

Rufián, N. (31 de agosto del 2020). La importancia del ciberespacio y de la ciberseguridad en las organizaciones. Segurilatam. Recuperado de: https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/la-importancia-del-ciberespacio-y-de-la-ciberseguridad-en-las-organizaciones_20200831.html

Sáinz, M. (2016). Ciberseguridad: Estrategias y desafíos. Editorial Seguridad Global.

Virilio, P. (1995). Cyber War and the Need for a Cyberdefense Strategy. *Defense and Security Journal.*