
# INFORME DE EVALUACIÓN

## PLAN DE CIBERSEGURIDAD PARA LA SEP 2021

Plan Especializado

Elaborado por:

**Gerencia de Informática y Tecnología Electoral**

Firma Digital
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por URDAY CHAVEZ Marco Antonio Alberto FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 24.08.2021 17:30:07 -05:00

Firma Digital
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por ROJAS BECERRA Danny David FAU 20291973851 soft
Motivo: Soy el autor del documento
Fecha: 24.08.2021 15:11:21 -05:00

Firma Digital
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por COTRINA CASTAÑEDA Lider Jen FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 25.08.2021 17:09:54 -05:00

**LIMA, AGOSTO 2021**

Firma Digital
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por MONTENEGRO VEGA Roberto Carlos FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 01.09.2021 22:25:58 -05:00

# INDICE

## LISTADO DE ABREVIATURAS

| | |
|---|---|
| Equipo de Respuesta ante Incidentes de Ciberseguridad | CSIRT |
| Firewall de aplicaciones web | WAF |
| Gerencia de Informática y Tecnología Electoral | GITE |
| Jurado Nacional de Elecciones | JNE |
| Oficina Nacional de Procesos Electorales | ONPE |
| Presidencia de Consejo de Ministros | PCM |
| Policía Nacional del Perú | PNP |
| Registro Nacional de Identificación y Estado Civil | RENIEC |
| Sistema de Prevención de Intrusos | IPS |
| Segunda Elección Presidencial 2021<br>2021 | SEP |

# I. RESUMEN EJECUTIVO

La finalidad del presente informe es la ejecución de la tarea “Evaluar el Plan de Ciberseguridad para la SEP 2021”; conforme a la formulación establecida en el POE SEP 2021 V00 con Resolución Jefatural N° 000133-2021-JN del 05JUN2021.

La finalidad de la presente evaluación es verificar si se logró asegurar los sistemas informáticos de la entidad y asegurar la información generada en el marco de la Segunda Elección Presidencial 2021.

Damos cuenta que, durante el proceso electoral, las herramientas detectaron y mitigaron todos los eventos de Ciberseguridad como fueron: infección de malware, correos spam, indisponibilidad de servicio, accesos no autorizados, entre otros utilizando técnicas de análisis de comportamiento, bloqueos de listas negras o inteligencia de amenazas. Y no se registraron incidentes que ocasionaron alguna indisponibilidad o degradación de los servicios que dan soporte a la SEP 2021, permitiendo el normal funcionamiento de todos los sistemas.

# II. EVALUACIÓN DE ACCIONES Y/O ACTIVIDADES OPERATIVAS, TAREAS, PROYECTOS

## 2.1 Descripción de acciones

En el numeral VIII. Acciones del Plan de Ciberseguridad para la SEP 2021, se establece lo siguiente:

| 3. Cód. | 4.Actividad Operativa / Tarea / Acción | Descripción |
|---|---|---|
| 1 | Monitorear las herramientas de Ciberseguridad. | Verificar la mitigación de eventos de Ciberseguridad en las herramientas para evaluar una mejora en las políticas de bloqueo. |
| 2 | Gestionar servicios relacionados a Ciberseguridad. | Gestión del servicio contratado de Ethical Hacking el cual permite detectar vulnerabilidades en los sistemas. |
| 3 | Coordinar reuniones semanales con los integrantes del CSIRT Electoral. | Efectuar reuniones semanales con integrantes de PCM, JNE, RENIEC y sus proveedores para intercambio de información de amenazas que atentan contra los sistemas de las instituciones involucradas en el proceso electoral y su procedimiento de mitigación. |
| 4 | Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral. | Seguimiento a las alertas remitidas por los integrantes de PCM, JNE, RENIEC y sus proveedores, en el grupo de mensajería instantánea, para evaluar su escalamiento y toma de acción en ONPE. |

Tabla N° 1: Lista de actividades del Plan de Ciberseguridad para la SEP 2021

Al respecto, en cumplimiento con las actividades señaladas, en la siguiente tabla se indican las acciones realizadas:

| | FORMATO | Código: | FM11-GPP/PLAN |
|---|---|---|---|
| ONPE | EVALUACIÓN DE PLANES ESPECIALIZADOS Y DE ACCIÓN | Versión: | 01 |
| | | Fecha de aprobación: | 03/01/2017 |
| | | Página: | 1 de 1 |

**1. NOMBRE DEL PLAN - AÑO:** Plan de Ciberseguridad SEP 2021

**2. ORGANO RESPONSABLE:** Gerencia de Informática y Tecnología Electoral

| 3. Cód | 4.Actividad Operativa / Tarea / Acción | 5.Unidad Orgánica Responsable | 6. Unidad de Medida | 7. Sustento | 8. FECHA PROGRAMADA | | 9. FECHA EJECUTADA | | 10. METAS FÍSICAS MENSUALES | | | | 11. MEDICIÓN DEL AVANCE DEL PROCESO EVALUADO | | | 12. ANALISIS CUALITATIVO | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | May 2021 | | Jun 2021 | | | | | | | |
| | | | | | Inicio | Fin | Inicio | Fin | Pr | Ej | Pr | Ej | META PROGRAMADA | META EJECUTADA | % AVANC | DESCRIPCIÓN DEL AVANCE / CUMPLIMIENTO | DIFICULTADES PRESENTADAS | MEDIDAS CORRECTIVAS |
| III | PROCESOS DE SOPORTE | | | | | | | | | | | | | | | | | |
| 3.3 | PROCESO: GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN | | | | | | | | | | | | | | | | | |
| ACTIVIDAD: Dar soporte a la institución en temas relacionados a las tecnologías de la institución. | | | | | | | | | | | | | | | | | | |
| 1 | Monitorear las herramientas de Ciberseguridad. | SGIST | Reporte | Reporte | 01/05/21 | 30/06/21 | 01/05/21 | 30/06/21 | 1 | 1 | 1 | 1 | 2 | 2 | 100% | **Mayo 2021**<br>De forma diaria se realizó el monitoreo de las herramientas de Ciberseguridad detectándose 143,347 eventos.<br>**Junio 2021**<br>De forma diaria se realizó el monitoreo de las herramientas de Ciberseguridad detectándose 273,373 eventos. | ninguna | ninguna |
| 2 | Gestionar servicios relacionados a Ciberseguridad. | SGIST | Reporte | Reporte | 01/05/21 | 05/06/21 | 13/05/21 | 08/06/21 | 1 | 1 | 1 | 1 | 2 | 2 | 100% | **Mayo 2021**<br>Con Informe N° 001041-2021/SGIST-GITE (13MAY2021), la Sub Gerencia de Infraestructura y Seguridad Tecnológica aprobó el incremento de un personal adicional, propuesto por la empresa KUNAK CONSULTING SAC, el mismo que se encuentran conforme a lo solicitado en los Términos de Referencia. Adjudicándose Servicio de Ethical Hacking - SEP 2021" al contratista Kunak Consulting S.A.C con la Orden de Servicio N° 0001098 de fecha 25MAY2021.<br>Con Carta N°000100-2021-GAD/ONPE (06MAY2021), se notificó al contratista KUNAK CONSULTING SAC, sobre la Resolución Gerencial N°000201-2021-GAD/ONPE (06MAY2021), que aprobó la ejecución de prestaciones adicionales al Contrato N° 109-2021-ONPE, cuyo objeto es la contratación del Servicio de Ethical Hacking.<br>Con Resolución Gerencial N°000201-2021-GAD/ONPE (06MAY2021), se aprobó la ejecución de prestaciones adicionales al Contrato N° 109-2021-ONPE, cuyo objeto es la contratación del Servicio de Ethical Hacking.<br>**Junio 2021**<br>Con Informe N° 000038-2021-DRB-SGIST-GITE (08JUN2021), se emitió el Informe de Conformidad por el Entregable 1 y 2 del Servicio de Ethical Hacking- SEP2021 | ninguna | ninguna |
| 3 | Coordinar reuniones semanales con los integrantes del CSIRT Electoral. | SGIST | Reporte | Reporte | 01/05/21 | 05/06/21 | 01/05/21 | 5/06/21 | 1 | 1 | 1 | 1 | 2 | 2 | 100% | **Mayo 2021**<br>Se realizaron las siguientes 03 reuniones:<br>Reunión de coordinación general realizada el 13MAY2021, donde se indicaron procedimientos de mitigación de software malicioso.<br>Reunión de coordinación general realizada el 20MAY2021, donde se indicaron los tipos de ataques que provocan una posible denegación de servicio de los sistemas web publicados en Internet.<br>Reunión de coordinación general realizada el 27MAY2021, donde se aclararon los contactos de escalamiento en caso ocurra un incidente de Ciberseguridad.<br>**Junio 2021:**<br>Se realizó la siguiente reunión:<br>Reunión de coordinación general realizada en junio 2021 donde se mostraron los resultados de las mitigaciones realizadas durante el día de elección. | ninguna | ninguna |
| 4 | Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral. | SGIST | Reporte | Reporte | 01/06/21 | 30/06/21 | 01/06/21 | 30/06/21 | 0 | 0 | 1 | 1 | 1 | 1 | 100% | **Mayo 2021**<br>Se detectaron 04 eventos relacionados a ciberataque a gobierno extranjero, campaña de phishing, campaña de malware y Vulnerabilidad en sistemas virtuales.<br>**Junio 2021**<br>Se detectaron 04 eventos relacionados a mensaje falso respecto a elecciones, amenazas de ataque a entidades del gobierno peruano, fuga masiva de información y difusión de noticias maliciosas. | ninguna | ninguna |

Tabla N° 2: Evaluación de las actividades del Plan de Ciberseguridad para la SEP2021

A continuación, se detallan las acciones realizadas por cada actividad:

**Actividad 1: Monitorear las herramientas de Ciberseguridad.**

**Acciones realizadas:**

Durante el mes de mayo y junio se realizó el monitoreo de los eventos detectados y mitigados por las herramientas de Ciberseguridad que protegieron la integridad, confidencialidad y disponibilidad de los sistemas que dieron soporte a las elecciones. A continuación, se muestra en una tabla que consolida los eventos registrados desde el inicio del servicio de monitoreo de las aplicaciones electorales publicadas a Internet:

| Herramienta | Mayo | Junio | Suma de eventos |
|---|---|---|---|
| Sistema de prevención de Intrusos (IPS) | 16.861 | 1.598 | **18.459** |
| Monitoreo Antimalware y antispam Office 365 | 85 | 51 | **136** |
| Firewall Perimetral | 17.226 | 6.729 | **23.955** |
| Anti-Denegación de Servicio | 0 | 0 | **0** |
| Firewall de Aplicaciones Web Cloud | 21.960 | 248,790 | **270.750** |
| Firewall de Aplicaciones Web On premise | 87.185 | 16,182 | **103.367** |
| Antimalware (Antivirus) | 30 | 23 | **53** |
| | | **TOTAL** | **416.720** |

Tabla N° 3: Total de 416.720 eventos detectados y mitigados por las herramientas de Ciberseguridad.

A continuación, se presenta el detalle de la detección y mitigación en cada herramienta de Ciberseguridad:

- Monitoreo del Sistema de prevención de Intrusos (IPS):

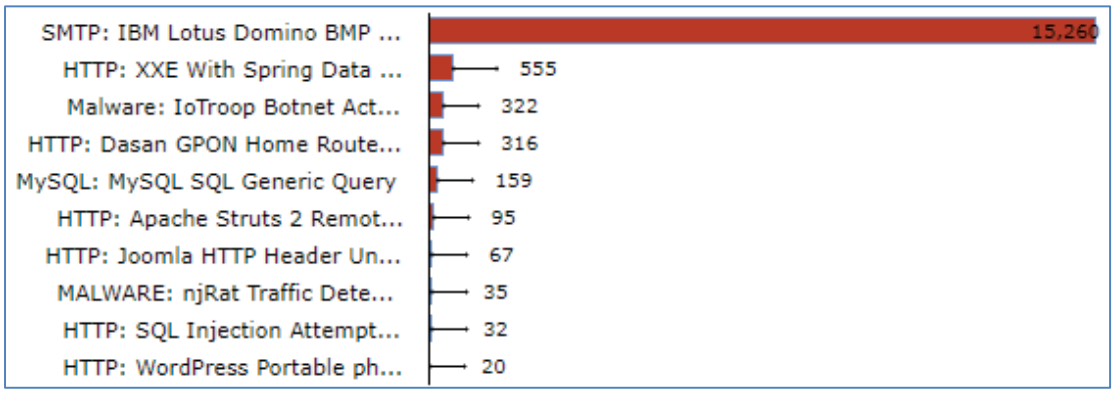



Figura N° 1: Se observa un total de 16.861 eventos detectados y mitigados por la herramienta IPS durante el mes de mayo.

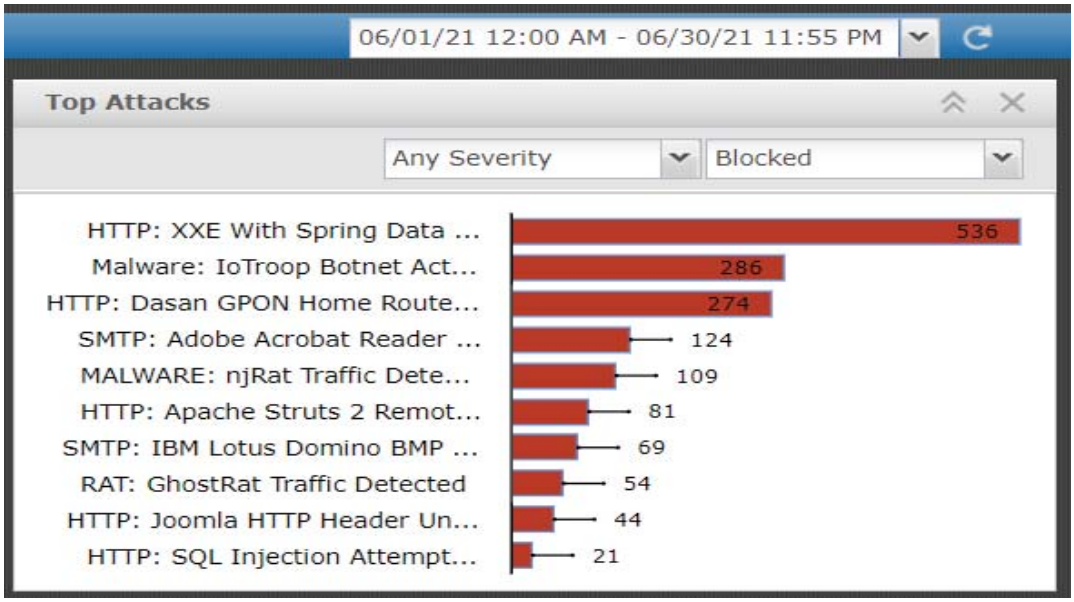



Figura N° 2: Se observa un total de 1.598 eventos detectados y mitigados por la herramienta IPS durante el mes de junio.

- Monitoreo Antimalware y antispam Office 365:

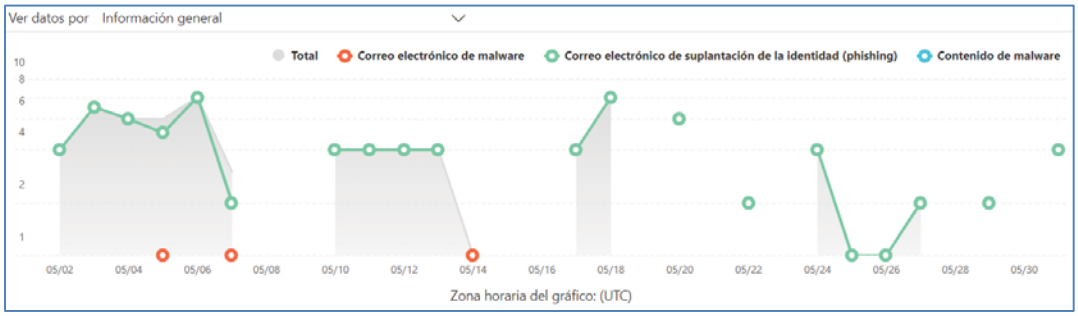



Figura N° 3: Se observa un total de 85 eventos detectados y mitigados por la herramienta antispam y antimalware de Office 365 en el mes de Mayo del presente año.

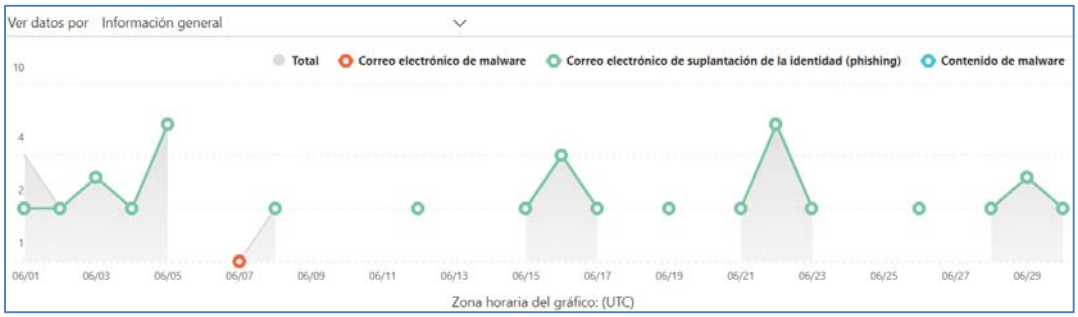
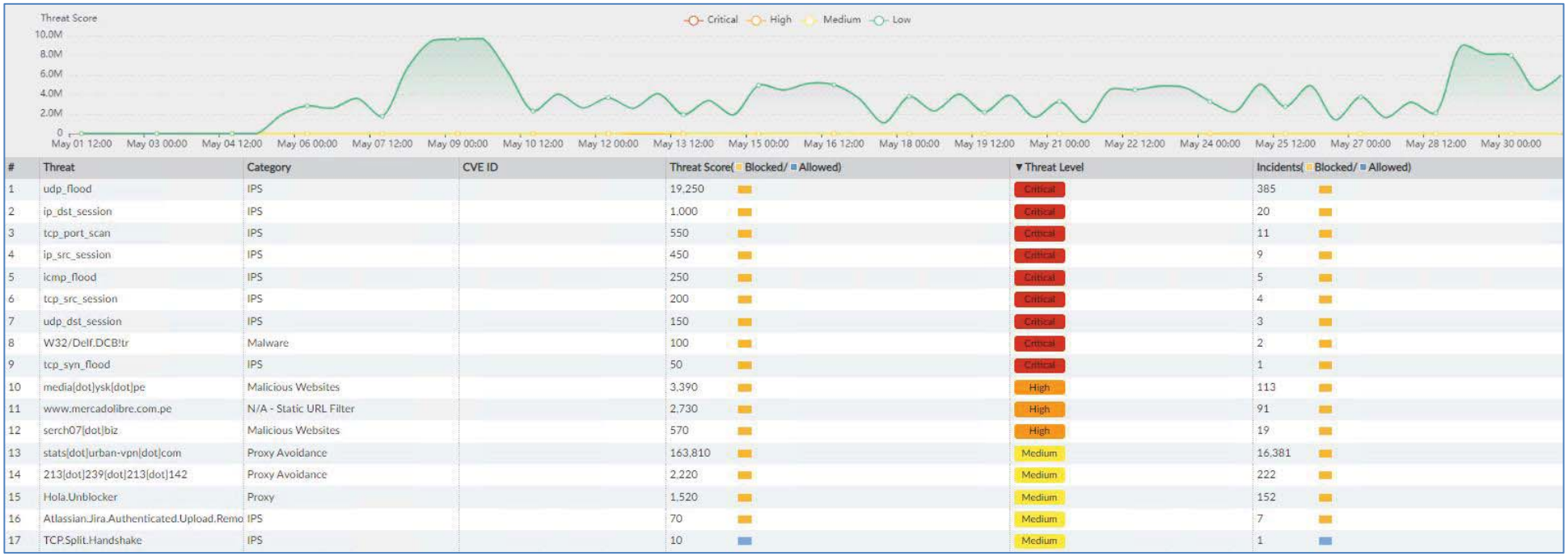


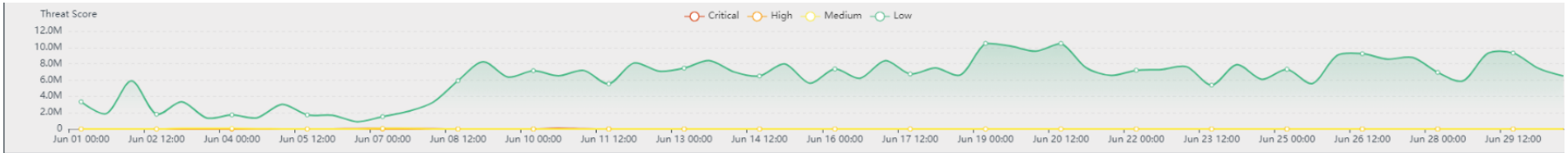

Figura N° 4: Se observa un total de 51 eventos detectados y mitigados por la herramienta antispam y antimalware de Office 365 en el mes de junio del presente año.

- Herramienta Firewall Perimetral:




| # | Threat | Category | CVE ID | Threat Score( Blocked/ Allowed) | ▼Threat Level | Incidents( Blocked/ Allowed) |
|---|---|---|---|---|---|---|
| 1 | udp_flood | IPS | | 19,250 | Critical | 385 |
| 2 | ip_dst_session | IPS | | 1,000 | Critical | 20 |
| 3 | tcp_port_scan | IPS | | 550 | Critical | 11 |
| 4 | ip_src_session | IPS | | 450 | Critical | 9 |
| 5 | icmp_flood | IPS | | 250 | Critical | 5 |
| 6 | tcp_src_session | IPS | | 200 | Critical | 4 |
| 7 | udp_dst_session | IPS | | 150 | Critical | 3 |
| 8 | W32/Delf.DCB!tr | Malware | | 100 | Critical | 2 |
| 9 | tcp_syn_flood | IPS | | 50 | Critical | 1 |
| 10 | media[dot]ysk[dot]pe | Malicious Websites | | 3,390 | High | 113 |
| 11 | www.mercadolibre.com.pe | N/A - Static URL Filter | | 2,730 | High | 91 |
| 12 | serch07[dot]biz | Malicious Websites | | 570 | High | 19 |
| 13 | stats[dot]urban-vpn[dot]com | Proxy Avoidance | | 163,810 | Medium | 16,381 |
| 14 | 213[dot]239[dot]213[dot]142 | Proxy Avoidance | | 2,220 | Medium | 222 |
| 15 | Hola.Unblocker | Proxy | | 1,520 | Medium | 152 |
| 16 | Atlassian.Jira.Authenticated.Upload.Remo | IPS | | 70 | Medium | 7 |
| 17 | TCP.Split.Handshake | IPS | | 10 | Medium | 1 |

Figura N° 5: Se observa un total de 17,226 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de mayo.




| # | Threat | Category | CVE ID | Threat Score( Blocked/ Allowed) | ▼Threat Level | Incidents( Blocked/ Allowed) |
|---|---|---|---|---|---|---|
| 1 | ip_dst_session | IPS | | 218,850 | Critical | 4,377 |
| 2 | udp_dst_session | IPS | | 2,300 | Critical | 46 |
| 3 | ip_src_session | IPS | | 1,150 | Critical | 23 |
| 4 | udp_flood | IPS | | 800 | Critical | 16 |
| 5 | tcp_src_session | IPS | | 700 | Critical | 14 |
| 6 | tcp_dst_session | IPS | | 700 | Critical | 14 |
| 7 | tcp_port_scan | IPS | | 700 | Critical | 14 |
| 8 | tcp_syn_flood | IPS | | 700 | Critical | 14 |
| 9 | HTML/Agent.E3F2!tr | Malware | | 150 | Critical | 3 |
| 10 | HTML/Phishing.BTV!tr | Malware | | 100 | Critical | 2 |
| 11 | icmp_flood | IPS | | 50 | Critical | 1 |
| 12 | Malicious_Behavior.SB | Malware | | 50 | Critical | 1 |
| 13 | media[dot]ysk[dot]pe | Malicious Websites | | 45,420 | High | 1,514 |
| 14 | www.mercadolibre.com.pe | N/A - Static URL Filter | | 10,680 | High | 356 |
| 15 | fajasmyd[dot]com | Phishing | | 4,590 | High | 153 |
| 16 | www[dot]flowsurfv3[dot]net | Malicious Websites | | 3,000 | High | 100 |
| 17 | HTTP.URI.SQL.Injection | IPS | | 2,940 | High | 98 |
| 18 | querilis[dot]com | Malicious Websites | | 2,400 | High | 80 |
| 19 | onmarshtompor[dot]com | Malicious Websites | | 1,470 | High | 49 |
| 20 | serch07[dot]biz | Malicious Websites | | 960 | High | 32 |
| 21 | azoaltou[dot]com | Malicious Websites | | 840 | High | 28 |
| 22 | cesarvallejocollege[dot]com | Phishing | | 780 | High | 26 |
| 23 | enel[dot]zyxmeapp[dot]com | Phishing | | 720 | High | 24 |
| 24 | g8715710740[dot]co | Phishing | | 660 | High | 22 |
| 25 | onemboaran[dot]com | Malicious Websites | | 540 | High | 18 |
| 26 | fkvdha[dot]com | Spam URLs | | 450 | High | 15 |
| 27 | sorryfearknockout[dot]com | Spam URLs | | 450 | High | 15 |
| 28 | goajuzey[dot]com | Malicious Websites | | 360 | High | 12 |
| 29 | thingsrefutation[dot]com | Spam URLs | | 360 | High | 12 |
| 30 | forzubatr[dot]com | Malicious Websites | | 180 | High | 6 |

Figura N° 6: Se observa un total de 6,729 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de junio.

- Firewall de Aplicaciones Web (WAF) Cloud

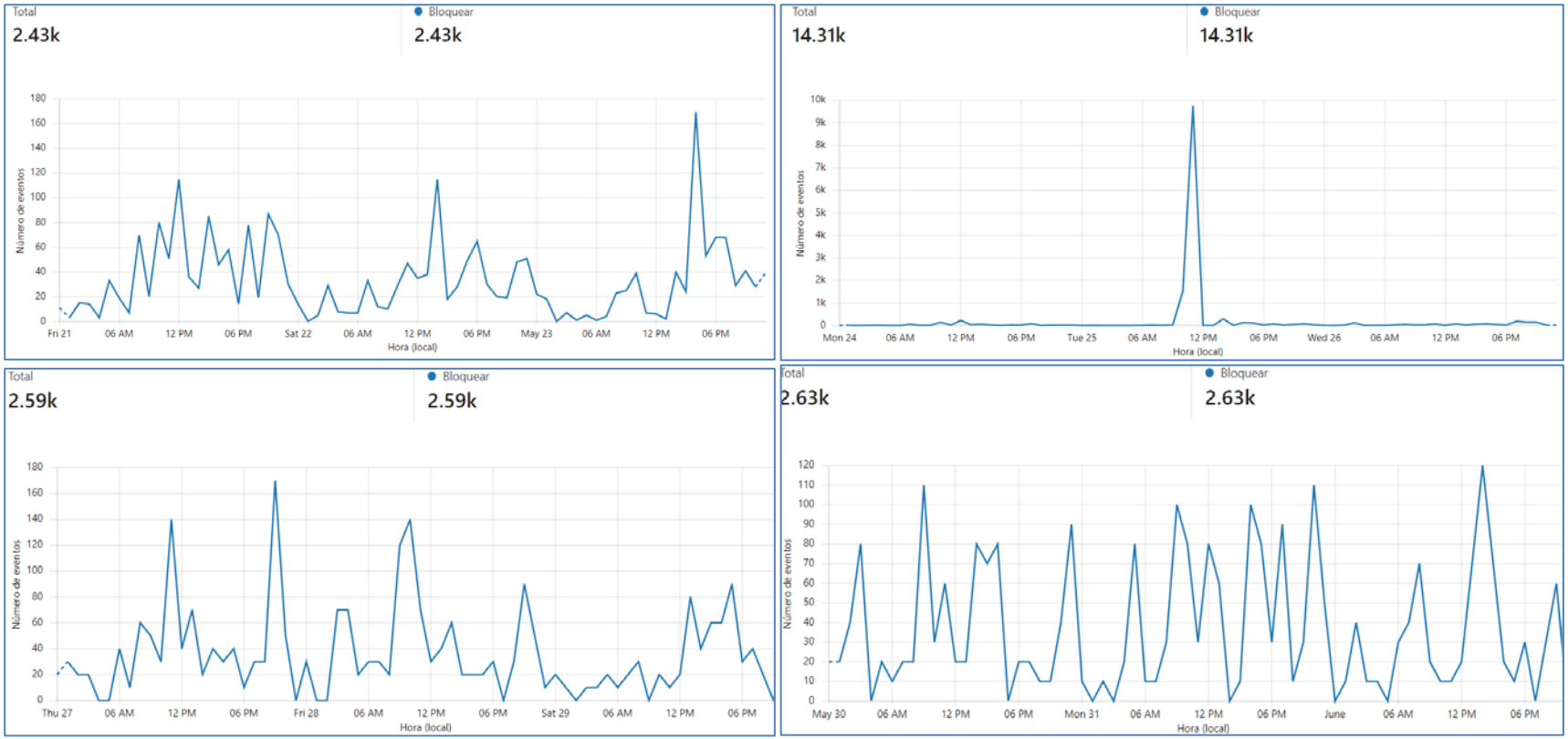



Figura N° 7: Se observa un total de 21.960 eventos detectados y mitigados por la herramienta WAF Cloud durante el mes de mayo.

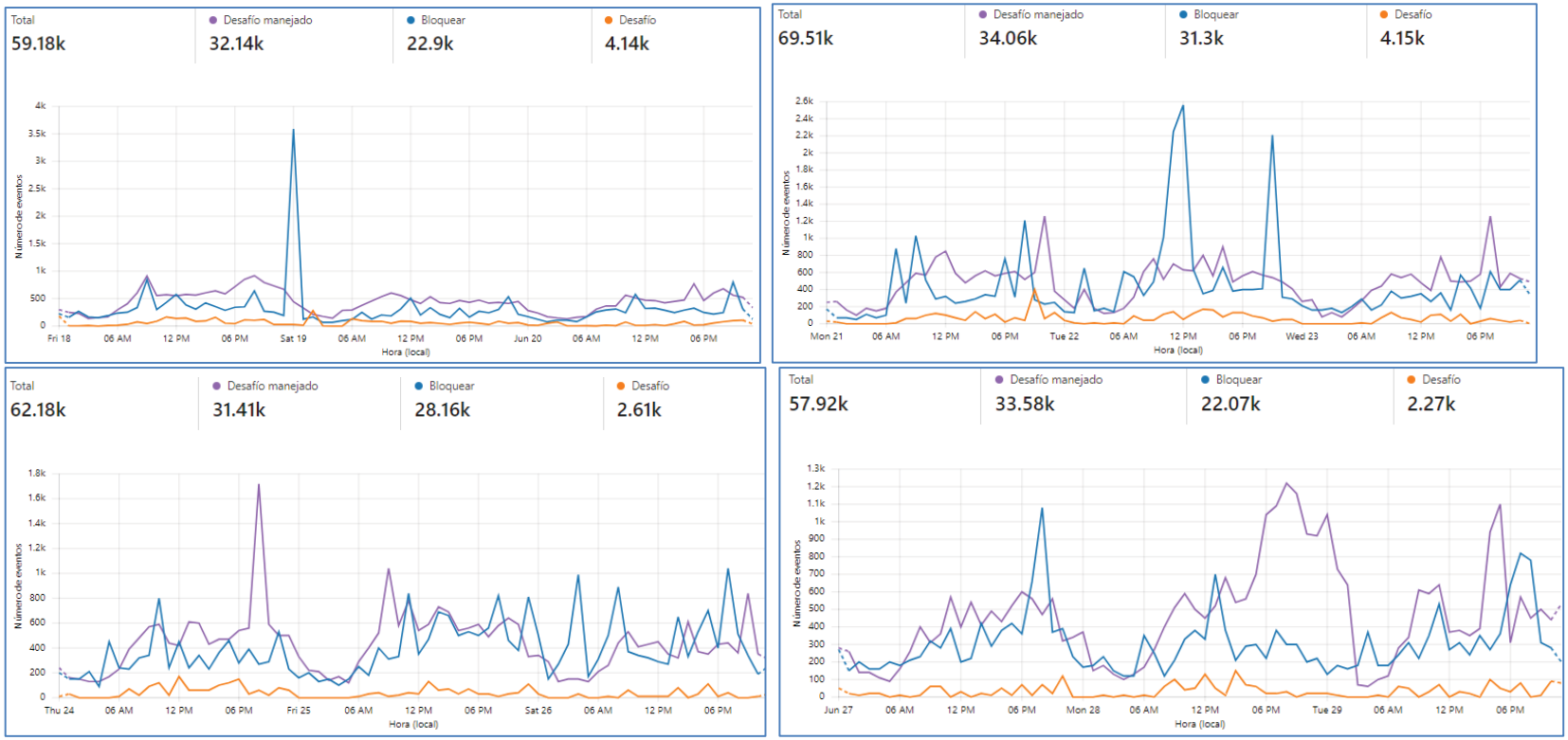



Figura N° 8: Se observa un total de 248,790 eventos detectados y mitigados por la herramienta WAF Cloud durante el mes de junio.

- WAF On premise

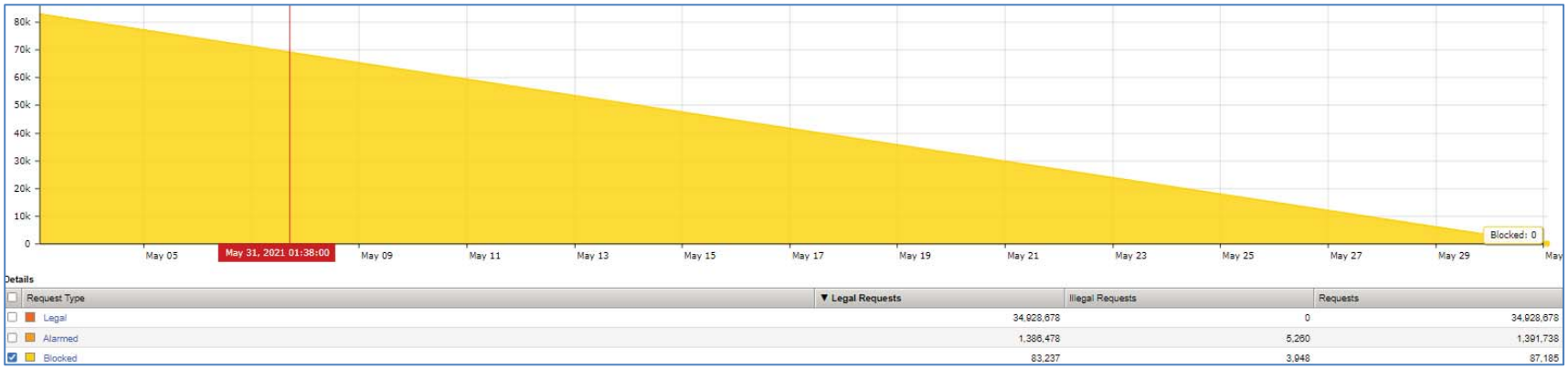



Figura N° 9: Se observa un total de 87.185 eventos detectados y mitigados por la herramienta WAF para aplicaciones on premise durante el mes de mayo.


Figura N° 10: Se observa un total de 16,182 eventos detectados y mitigados por la herramienta WAF para aplicaciones on premise durante el mes de junio.

- Antimalware (Antivirus)

| Acción | Virus | Spyware |
|---|---|---|
| Limpiado/bloqueado | 1 | 0 |
| Eliminado | 20 | 5 |
| En cuarentena | 2 | 2 |
| Sospechoso | 0 | 0 |
| Recientemente infectado | 0 | 0 |
| Aún infectado | 0 | 0 |

Tabla N° 4: Se observa un total de 30 eventos detectados y mitigados por la herramienta antivirus durante el mes de mayo.

| Acción | Virus | Spyware |
|---|---|---|
| Limpiado/bloqueado | 0 | 0 |
| Eliminado | 20 | 3 |
| En cuarentena | 0 | 0 |
| Sospechoso | 0 | 0 |
| Recientemente infectado | 0 | 0 |
| Aún infectado | 0 | 0 |

Tabla N° 5: Se observa un total de 23 eventos detectados y mitigados por la herramienta antivirus durante el mes de junio.

Cabe mencionar que, durante las elecciones, las herramientas detectaron y mitigaron eventos de Ciberseguridad por lo que no se registraron incidentes que causen indisponibilidad o degradación de los servicios que dan soporte a la SEP 2021.

**Actividad 2: Gestionar servicios relacionados a Ciberseguridad.**

**Acciones realizadas:**

Se supervisó la ejecución del servicio Ethical Hacking SEP 2021. Tal como se evidencia en los siguientes informes:

Con Informe N° 000038-2021-DRB-SGIST-GITE (08JUN2021), se emitió el INFORME DE CONFORMIDAD POR EL ENTREGABLE 1 Y 2 DEL SERVICIO DE ETHICAL HACKING – SEP 2021.

Con Informe N° 001041-2021/SGIST-GITE (13MAY2021), la Sub Gerencia de Infraestructura y Seguridad Tecnológica aprobó el incremento de un personal adicional, propuesto por la empresa KUNAK CONSULTING SAC, el mismo que se encuentran conforme a lo solicitado en los Términos de Referencia.

Con orden de servicio N° 0001098 de fecha 25MAY2021, se adjudicó el “Servicio de Ethical Hacking - SEP 2021” al contratista Kunak Consulting S.A.C.

Con Carta N°000100-2021-GAD/ONPE (06MAY2021), se notificó al contratista KUNAK CONSULTING SAC, sobre la Resolución Gerencial N°000201-2021-GAD/ONPE (06MAY2021), que aprobó la ejecución de prestaciones adicionales al Contrato N° 109-2021-ONPE, cuyo objeto es la contratación del Servicio de Ethical Hacking.

Con Resolución Gerencial N°000201-2021-GAD/ONPE (06MAY2021), se aprobó la ejecución de prestaciones adicionales al Contrato N° 109-2021-ONPE, cuyo objeto es la contratación del Servicio de Ethical Hacking.

**Actividad 3: Coordinar reuniones semanales con los integrantes del CSIRT Electoral.**

**Acciones realizadas:**

Con el Informe N° 000017-2020-DRB-SGIST-GITE 03NOV2020 se solicitó a la SGIST su gestión para que la GITE propicie la reactivación del Equipo de Respuesta a Incidentes de Seguridad Digital CSIRT. La gestión de la SGIST se realizó con Informe N° 001428-2020/SGIST-GITE 31DIC2020.

A su vez, la GITE emitió el MEMORANDO N° 003779-2020-GITE/ONPE 31DIC2020 con el que solicita a la Secretaría General hacer de conocimiento al Director de Registros, Estadística y Desarrollo Tecnológico del Jurado Nacional de Elecciones (Ing. Luis Alberto Antonio Ramos Llanos) y a la Gerente de Tecnología de la Información del Registro Nacional de Identificación y Estado Civil (Rosario Roxana Dávila Olórtegui) la reactivación del CSIRT Electoral en el marco de las EG2021.

Finalmente, la Secretaría General emitió los siguientes oficios comunicando a las entidades la reactivación del CSIRT Electoral:

- OFICIO N° 000018-2021/SG 06ENE2021 dirigido al Ministerio de Defensa.
- OFICIO N° 000019-2021/SG 06ENE2021 dirigido al JNE.
- OFICIO N° 000020-2021/SG 06ENE2021 dirigido al RENIEC.

Como resultado de las coordinaciones realizadas, el 12ENE2021 se realizó la reunión de reinicio de las actividades del CSIRT Electoral. URL del video https://web.microsoftstream.com/video/a771200f-306b-44e3-861e-b02936c1a60c

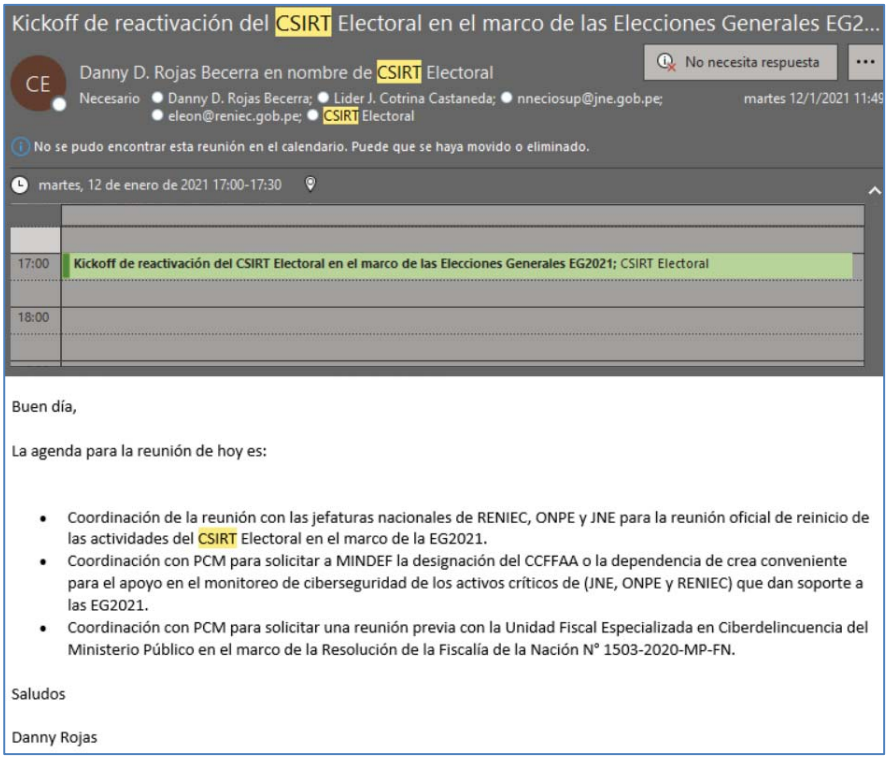



Figura N° 11: Agenda de la reunión de reinicio de actividades del CSIRT Electoral 12ENE2021

Posterior a la reactivación y ejecución del CSIRT Electoral durante las EG 2021, se mantuvo su continuidad operativa para la SEP2021 realizándose las siguientes actividades:

Actividades efectuadas en mayo:

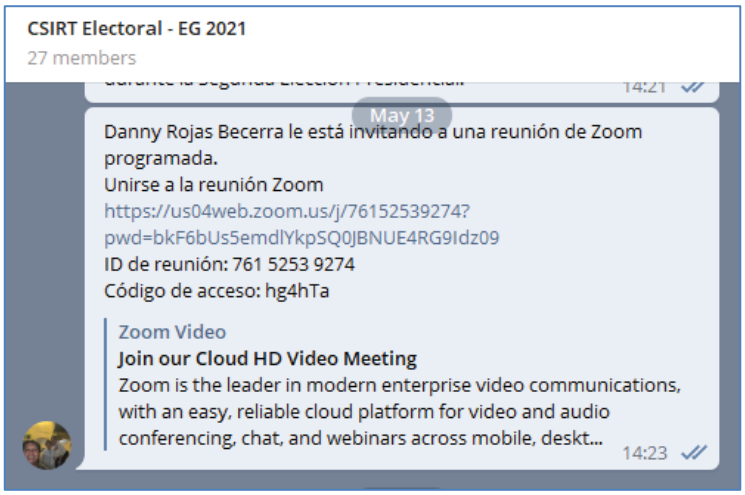



Figura N° 12: Reunión de coordinación general realizada el 13MAY2021, donde se indicaron procedimientos de mitigación de software malicioso.

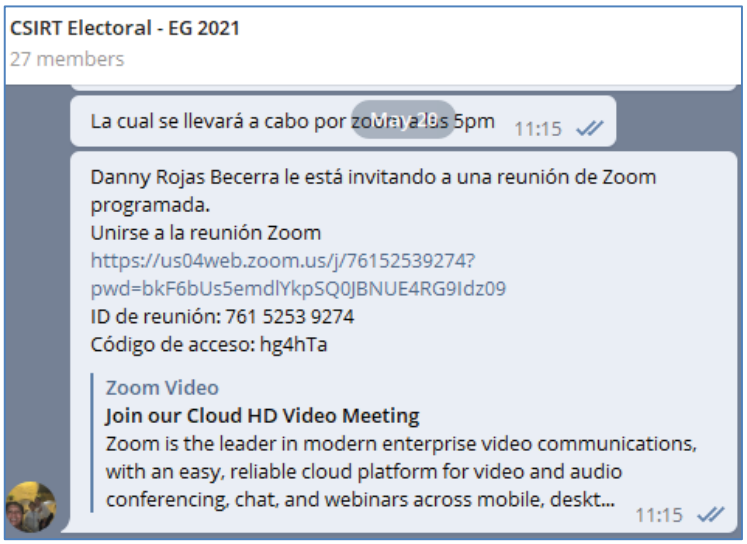



Figura N° 13: Reunión de coordinación general realizada el 20MAY2021, donde se indicaron los tipos de ataques que provocan una posible denegación de servicio de los sistemas web publicados en Internet.


Figura N° 14: Reunión de coordinación general realizada el 27MAY2021, donde se aclararon los contactos de escalamiento en caso ocurra un incidente de Ciberseguridad.

Actividades efectuadas en junio:

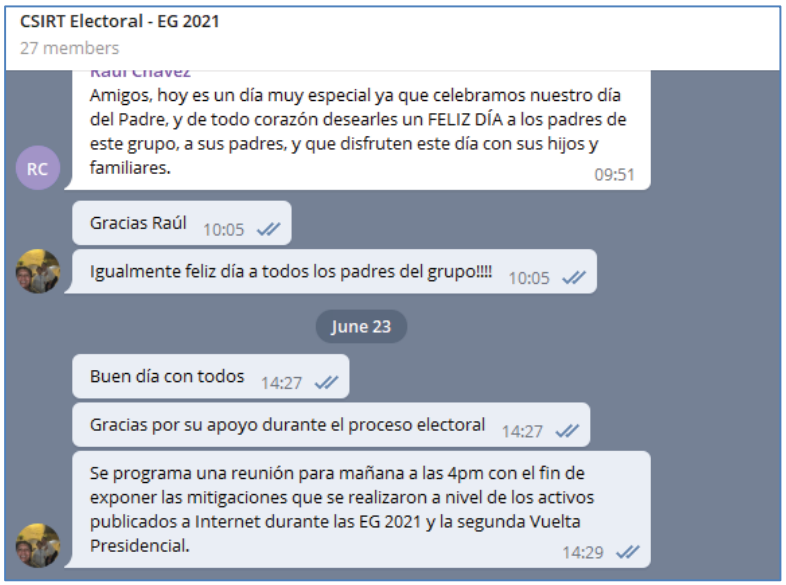



Figura N° 15: Reunión de coordinación general realizada en junio 2021 donde se mostraron los resultados de las mitigaciones realizadas durante el día de elección.

**Actividad 4: Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral.**

**Acciones realizadas:**

Por medio del Telegram oficial se efectuó el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral con el fin de proponer medidas de mitigación y respuesta.

El monitoreo consiste en verificar la disponibilidad e integridad de los servicios publicados hacia internet como son:

- ✓ SEA (Sistema de Escrutinio Automatizado)
- ✓ Web de Resultados
- ✓ Web institucional
- ✓ SIDE (Sistema de Información del Día de Elección)
- ✓ ONPEDUCA
- ✓ CLV (Consulta tu Local de Votación)
- ✓ Elige tu local de votación
- ✓ Consulta miembro de mesa

El monitoreo efectuado por los integrantes del CSIRT Electoral, permite tener una cobertura de observación durante 24 horas, durante los 7 días de la semana, para detectar cualquier incidente que ocurra en los portales web publicados a Internet.

Alertas realizadas en mayo:

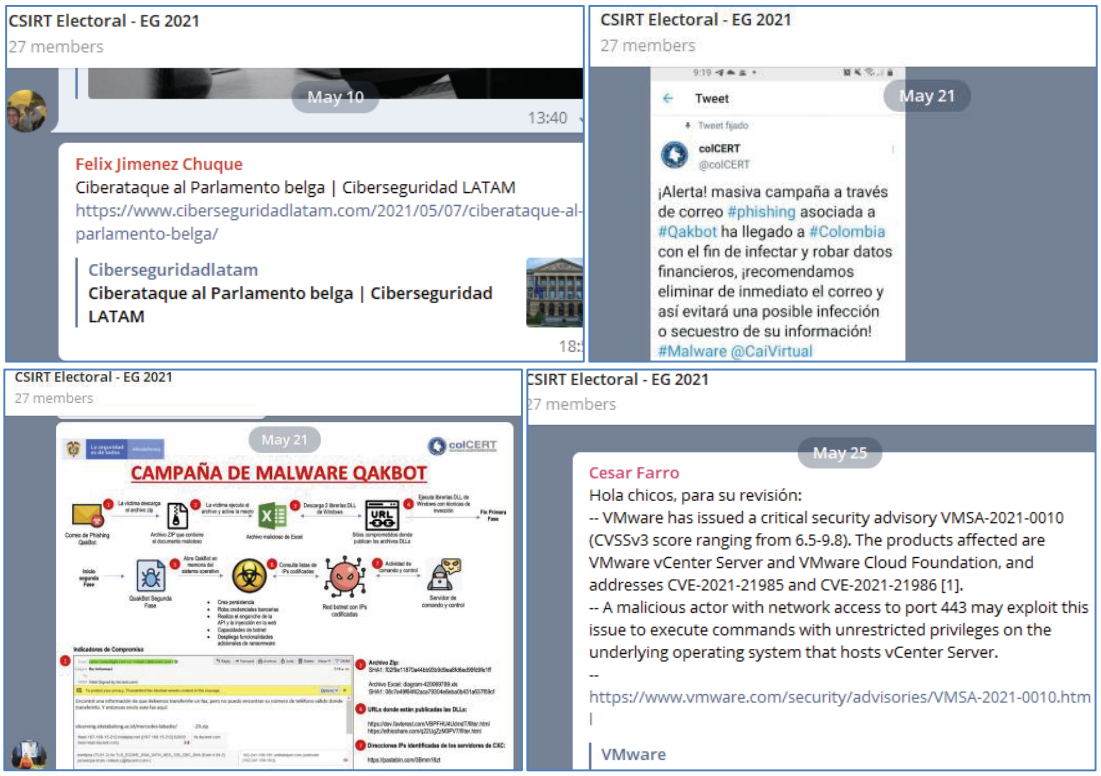



Figura N° 16: Alertas emitidas por los integrantes del CSIRT Electoral en mayo.

Alertas realizadas en junio:


Figura N° 17: Alertas emitidas por los integrantes del CSIRT Electoral en junio.

## 2.2 Reporte del Indicador del Plan de Ciberseguridad para la SEP 2021

Con respecto al objetivo de lo programado:

- Evitar incidentes a los activos informáticos que dan soporte a la SEP2021.

Se aprecia el siguiente resultado en el indicador:

**Indicador 1:** Porcentaje de eventos de Ciberseguridad bloqueados.

$$\left[\frac{X*100\%}{X+Y}\right] = \left[\frac{416{,}720*100\%}{416{,}720+0}\right]$$

**Meta** = 98% **Resultado** = 100%

*X* = Número de eventos de Ciberseguridad bloqueados = 416,720
Y = Número de Incidentes que afectaron los activos de información y servicios informáticos = 0

Corresponde señalar que, durante el día de la Jornada Electoral, todos los eventos de Ciberseguridad fueron bloqueados y no se registraron incidentes que afectaron a los activos de información y servicios informáticos.

# III. BALANCE GENERAL

## 3.1. Logros Obtenidos

- Se ejecutaron el 100% de las tareas programadas en el Plan de Ciberseguridad para la SEP 2021, tal como se muestra a continuación:

| Tareas | Cantidad |
|---|---|
| Programadas | 7 |
| Ejecutadas | 7 |

Tabla N° 6: Tareas

- Durante los meses de mayo y junio se logró bloquear 416.720 eventos adversos los mismos que no registraron incidentes ni afectación a los activos de información y servicios informáticos.

## 3.2. Problemas identificados y medidas correctivas adoptadas

No se presentaron inconvenientes durante la ejecución del Plan de Ciberseguridad.

# IV. EJECUCIÓN DEL PRESUPUESTO

Los recursos ejecutados del Plan de Ciberseguridad para la SEP ascendió a S/ 13.000.00. Dicho cálculo se obtuvo considerando el pago mensual del personal asignado como “Servicio de Locador de servicio de Especialista de Ciberseguridad”:

| # | DESCRIPCIÓN ITEMS – PROGRAMADOS | RETRIBUCIÓN MENSUAL | FECHA DE INICIO DE ACTIVIDADES | PRESUPUESTO PROYECTADO 2DA - VUELTA | | |
|---|---|---|---|---|---|---|
| | | | | TOTAL MAYO | TOTAL JUNIO | TOTAL |
| 1 | ESPECIALISTA DE CIBERSEGURIDAD | 6,500.00 | 1/05/2021 | 6,500.00 | 6,500.00 | 13,000.00 |

Tabla N° 7: Ejecución del presupuesto conforme a lo indicado por SGOI

# V. CONCLUSIONES Y RECOMENDACIONES

**Conclusiones:**

- Todos los eventos detectados por las herramientas de Ciberseguridad fueron mitigados.

- No ocurrieron incidentes de Ciberseguridad en los activos informáticos que dieron soporte a la SEP2021.

- Se mitigó un total de 416.720 eventos de Ciberseguridad tal como se muestran en la Tabla N° 3.

**Recomendaciones:**

Se recomienda continuar con el monitoreo permanente de los eventos de Ciberseguridad con la finalidad de preservar la confidencialidad, disponibilidad e Integridad de la Información de la entidad.