Ernst & Young Paraguay - Auditores y
Asesores de Negocios
Mcal. López 3794 esq. Cruz del Chaco,
Edificio Citicenter - 6° Piso
Asunción, Paraguay

Tel: (595-21) 664-308
Fax: (595-21) 608-985
ey.com

Building a better working world

Asunción, 04 de enero de 2022

Señores
Ministerio de Tecnologías de la Información y Comunicación
Gral. Santos 1170 esq. Concordia - Complejo Santos E2
Asunción, Paraguay

Attn. Gabriela Ratti

Ref: SCC ID# 388.416 - Consultoría para el Servicio de Monitoreo y Elaboración de Boletines y Alertas de Ciberseguridad.

De nuestra consideración:

Por medio de la presente, remitimos en adjunto el Informe Trimestral N° 01, conforme a lo establecido en el contrato N° 56/2021.

Hacemos propicia la ocasión para saludarlo muy atentamente.

Atentamente

Mateo Franco
Ernst & Young
Gerente

Nombre y Cargo del Signatario: Mateo Franco - Gerente
Nombre de la Firma: Ernst & Young- Paraguay Auditores y Consultores
Dirección: Avda. Mariscal López 3794 esq. Cruz del Chaco, P. 6. Asunción, Paraguay

Building a better working world

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

SCC ID# 388.416 - Consultoría para el Servicio de Monitoreo y Elaboración de Boletines y Alertas de Ciberseguridad

Informe Trimestral 01

Ernst & Young Paraguay - Auditores y Asesores de Negocios
Mcal. López 3794 esq. Cruz del Chaco,
Edificio Citicenter - 6° Piso
Asunción, Paraguay

Tel: (595-21) 664-308
Fax: (595-21) 608-985
ey.com

Señores
MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN (MITIC)
General Santos 1170 casi Concordia (Complejo Santos)
Asunción, Paraguay
Atte: Gabriela Ratti - Directora General de Ciberseguridad y Protección de la Información

De mi Consideración:

Tenemos el agrado de dirigirnos a Usted en ocasión de hacer referencia al Servicio "SCC ID# 388.416 - Consultoría para el Servicio de Monitoreo y Elaboración de Boletines y Alertas de Ciberseguridad - contrato Nro. 56/2021"

Sobre el particular, y conforme a lo requerido en el contrato de referencia, remitimos a continuación el siguiente Producto Entregable:

- Informe Trimestral 01 de ejecución del servicio de monitoreo y elaboración de boletines y alertas de ciberseguridad

El desarrollo de nuestro trabajo se basó en el monitoreo activo de las fuentes de información relevantes en cuestiones de ciberseguridad, con el propósito de identificar noticias relevantes de actualizaciones, vulnerabilidades, nuevos vectores de ataques sobre software conocido y utilizado a nivel del territorio de Paraguay, que pudieran ser distribuidas a través de correos electrónicos en forma de boletines, noticias y guías de ciberseguridad.

Hacemos propicia la ocasión para saludarla muy atentamente,

Firma:_____
Nombre: Luis Alberto Ayala Albertini Acosta
En calidad de: Socio - Representante Legal
Dirección: Avda. Mariscal López 3794 esq. Cruz del Chaco

Debidamente autorizado para firmar por y en nombre de Ernst & Young Paraguay Auditores y Asesores de Negocios.

Ernst & Young Paraguay - Auditores y
Asesores de Negocios
Mcal. López 3794 esq. Cruz del Chaco,
Edificio Citicenter - 6° Piso
Asunción, Paraguay

Tel: (595-21) 664-308
Fax: (595-21) 608-985
ey.com

Índice

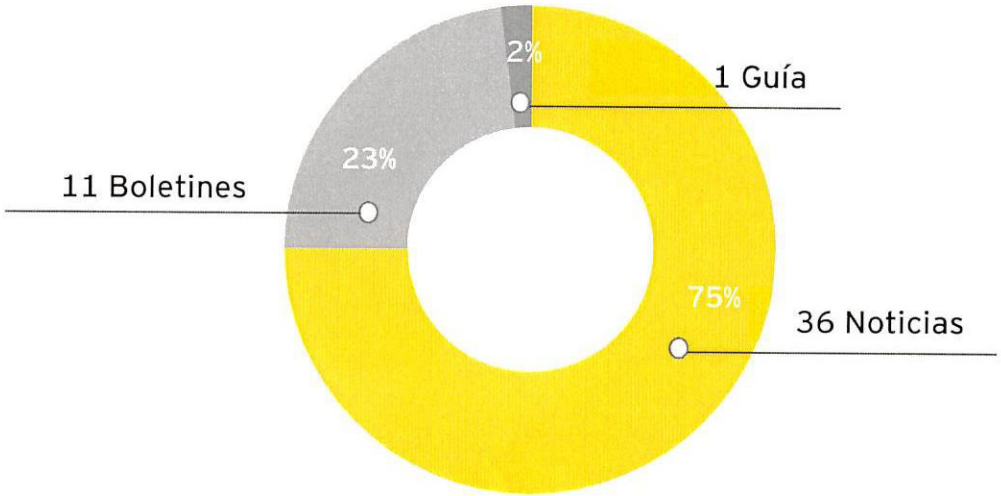
1. Sumario Ejecutivo 3
2. Audiencia 4
3. Noticias de ciberseguridad publicadas 5
4. Boletines de seguridad publicados 9
5. Guías de seguridad elaboradas 11

Luis Alberto Ayala Albertini Acosta
Socio

1. Sumario Ejecutivo

Conforme los objetivos y alcances definidos para el presente trabajo, se detalla a continuación un resumen de los documentos elaborados para el periodo reportado:

Firma del Contrato: 29 de septiembre de 2021
Planificación detallada, despliegue de herramientas colaborativas y preparación: 30 septiembre al 23 noviembre
Emisión de Boletines: 24 de noviembre 2021 - 28 de diciembre 2021



- Cantidad de noticias de ciberseguridad publicadas: 36
- Cantidad de boletines de seguridad publicados: 11
- Cantidad de guías de seguridad elaboradas: 1

Luis Alberto Ayala Albertini Acosta
Socio

2. Audiencia

Plataforma	Contactos	Suscriptores
Mail Chimp	1.998	1.962

Luis Alberto Ayala Albertini Acosta
Socio

3. Noticias de ciberseguridad publicadas

Título	Fecha	Enlace
Vulnerabilidad RCE en Microsoft Exchange	25-11-2021	https://www.cert.gov.py/noticias/vulnerabilidades-rce-en-microsoft-exchange
Vulnerabilidad SSRF en VMware vSphere Web Client	26-11-2021	https://cert.gov.py/noticias/vulnerabilidad-ssrf-en-vmware-vsphere-web-client-flexflash
Fallo de seguridad de HTTP Apache afecta a producto Cisco.	26-11-2021	https://cert.gov.py/noticias/fallo-de-seguridad-de-http-apache-afecta-producto-cisco
Vulnerabilidad de elevación de privilegios de Windows Installer	26-11-2021	https://www.cert.gov.py/noticias/vulnerabilidad-de-elevacion-de-privilegios-de-windows-installer
Actualizaciones de Windows generan errores en Kaspersky Endpoint y Windows Defender	29-11-2021	https://cert.gov.py/noticias/actualizaciones-de-windows-generan-errores-en-kaspersky-endpoint-y-windows-defender
Vulnerabilidad de día cero (Zero Day) en dispositivos empresariales de TP-Link de modelo TL-XVR1800L	30-11-2021	https://cert.gov.py/noticias/vulnerabilidad-de-dia-cero-zero-day-en-dispositivos-empresariales-de-tp-link-de-modelo-tl-xvr1800l
Secuestro de correos electrónicos en Microsoft Exchange	30-11-2021	https://cert.gov.py/noticias/secuestro-de-correos-electronicos-en-microsoft-exchange
Múltiples vulnerabilidades detectadas en las plataformas de la aplicación "Zoom"	30-11-2021	https://cert.gov.py/noticias/multiples-vulnerabilidades-detectadas-en-las-plataformas-de-la-aplicacion-zoom
Explotación de vulnerabilidad en Oracle WebLogic para minería de criptomonedas	01-12-2021	https://cert.gov.py/noticias/explotacion-de-vulnerabilidad-en-oracle-weblogic-para-mineria-de-criptomonedas
Vulnerabilidad de desbordamiento de búfer en varios productos de impresoras HP	01-12-2021	https://www.cert.gov.py/noticias/vulnerabilidad-de-desbordamiento-de-bufer-en-varios-productos-de-impresoras-hp
Vulnerabilidad de Inyección DLL en FortiClient y FortiClient EMS	02-12-2021	https://cert.gov.py/noticias/vulnerabilidad-de-inyeccion-dll-en-forticlient-y-forticlient-ems

EY

Luis Alberto Ayala Albertini Acosta
Socio

Título	Fecha	Enlace
Difusión de una nueva versión del troyano bancario "Emotet"	03-12-2021	https://cert.gov.py/noticias/difusion-de-una-nueva-version-del-troyano-bancario-emotet
Vulnerabilidad de desbordamiento de buffer del protocolo de transmisión 6pack de Linux	06-12-2021	https://cert.gov.py/noticias/vulnerabilidad-de-desbordamiento-de-buffer-del-protocolo-de-transmision-6pack-de-linux
Múltiples vulnerabilidades en diferentes aplicaciones de Zoho ManageEngine	6-12-2021	https://www.cert.gov.py/noticias/vulnerabilidad-de-ejecucion-remota-de-comandos-en-zoho-manageengine-servicedesk-plus
Vulnerabilidad de acceso a información confidencial en Grafana (Directory traversal)	9-12-2021	https://cert.gov.py/noticias/vulnerabilidad-de-acceso-informacion-confidencial-en-grafana-directory-traversal
Múltiples vulnerabilidades detectadas en productos SonicWall.	10-12-2021	https://www.cert.gov.py/noticias/multiples-vulnerabilidades-detectadas-en-productos-sonicwall
Vulnerabilidad de ejecución remota de comandos en la librería Log4j de Java	10-12-2021	https://www.cert.gov.py/noticias/vulnerabilidad-de-ejecucion-de-comandos-remoto-en-la-libreria-log4j-de-java
Vulnerabilidad de ejecución remota de comandos en el firmware del dispositivo TP Link TL-WR840N v5	13-12-2021	https://www.cert.gov.py/noticias/vulnerabilidad-de-ejecucion-remota-de-comandos-en-el-firmware-del-dispositivo-tp-link-tl-wr840n-v5
Múltiples vulnerabilidades detectadas en Fortinet	14-12-2021	https://www.cert.gov.py/noticias/multiples-vulnerabilidades-detectadas-en-fortinet
Vulnerabilidad de evasión de control de autenticación 2FA para usuarios LDAP en GitLab	14-12-2021	https://cert.gov.py/noticias/vulnerabilidad-de-evasion-de-control-de-autenticacion-2fa-para-usuarios-ldap-en-gitlab
Vulnerabilidad de escalación de privilegios en Laravel	15-12-2021	https://cert.gov.py/noticias/vulnerabilidad-de-escalacion-de-privilegios-en-laravel
Vulnerabilidad de escalamiento de privilegios en Ubuntu	15-12-2021	https://cert.gov.py/noticias/vulnerabilidad-de-escalamiento-de-privilegios-en-ubuntu
Múltiples ataques a enrutadores Mikrotik explotando vulnerabilidades como ejecución remota de comandos y otros.	16-12-2021	https://cert.gov.py/noticias/multiples-ataques-enrutadores-mikrotik-explotando-vulnerabilidades-como-ejecucion-remota-comandos-y-otros

EY

Luis Alberto Ayala Albertini Acosta
Socio

Título	Fecha	Enlace
Acceso a información confidencial de Microsoft Exchange mediante módulo IIS	16-12-2021	https://cert.gov.py/noticias/acceso-informacion-confidencial-de-microsoft-exchange-mediante-modulo-iis
Microsoft publica parches para múltiples vulnerabilidades	17-12-2021	https://www.cert.gov.py/noticias/microsoft-publica-parches-para-multiples-vulnerabilidades
Nuevas vulnerabilidades identificadas que afectan a Log4j	20-12-2021	https://cert.gov.py/noticias/nuevas-vulnerabilidades-identificadas-que-afectan-log4j
Vulnerabilidad de desbordamiento de búfer en Whatsapp y Whatsapp Business para Android	20-12-2021	https://cert.gov.py/noticias/vulnerabilidad-de-desbordamiento-de-bufer-en-whatsapp-y-whatsapp-business-para-android
SAP publica parches para múltiples vulnerabilidades.	20-12-2021	https://cert.gov.py/noticias/sap-publica-parches-para-multiples-vulnerabilidades
Vulnerabilidad Log4j utilizada para instalar malware bancario Dridex en Windows y Linux.	21-12-2021	https://cert.gov.py/noticias/vulnerabilidad-log4j-utilizada-para-instalar-malware-bancario-dridex-en-windows-y-linux
Inyección de código en múltiples productos Netgear.	21-12-2021	https://cert.gov.py/noticias/inyeccion-de-codigo-en-multiples-productos-netgear
Adobe publica parches para múltiples vulnerabilidades de sus productos	22-12-2021	https://cert.gov.py/noticias/adobe-publica-parches-para-multiples-vulnerabilidades-de-sus-productos
Vulnerabilidad SSRF detectada en VMware Workspace ONE UEM console	22-12-2021	https://cert.gov.py/noticias/vulnerabilidad-ssrf-detectada-en-vmware-workspace-one-uem-console
Microsoft publica parches para vulnerabilidades en Active Directory	22-12-2021	https://www.cert.gov.py/noticias/microsoft-publica-parches-para-vulnerabilidades-en-active-directory
Actualización de seguridad para Apache HTTP Server	23-12-2021	https://www.cert.gov.py/noticias/actualizacion-de-seguridad-para-apache-http-server
Apple lanza actualizaciones de seguridad para varios productos	27-12-2021	https://www.cert.gov.py/noticias/apple-publica-parches-para-multiples-vulnerabilidades-de-sus-productos

EY

Luis Alberto Ayala Albertini Acosta
Socio

Título	Fecha	Enlace
Múltiples vulnerabilidades en productos Netgear	28-12-2021	https://www.cert.gov.py/noticias/multiples-vulnerabilidades-en-productos-netgear

EY

Luis Alberto Ayala Albertini Acosta
Socio

4. Boletines de seguridad publicados

Título	Archivo	Fecha	Enlace	Enviados	Abiertos
Vulnerabilidad RCE en Microsoft Exchange	BOL-CERT-PY-2021-31 Vulnerabilidad_RCE_en_Microsoft_ExchangeV3.docx	25/11/2021	https://cert.gov.py/application/files/5116/3786/2285/BOL-CERT-PY-2021-31_Vulnerabilidades_RCE_en_Microsoft_Exchange.pdf	1962	488
Vulnerabilidad de elevación de privilegios de Windows Installer	BOL-CERT-PY-2021-32 Vulnerabilidad_Microsoft_Windows.docx	26/11/2021	https://cert.gov.py/application/files/2316/3795/4472/BOL-CERT-PY-2021-32_Vulnerabilidad_Microsoft_Windows.pdf	1962	483
Vulnerabilidad de desbordamiento de búfer en varios productos de impresoras HP	BOL-CERT-PY-2021-33 Vulenrabilidad impresoras HP.docx	01/12/2021	https://cert.gov.py/application/files/4416/3838/4984/BOL-CERT-PY-2021-33_Vulnerabilidad_impresoras_HP.pdf	1962	577
Múltiples vulnerabilidades en diferentes aplicaciones de Zoho ManageEngine	BOL-CERT-PY-2021-34 Zoho Manage Engine ServiceDesk Plus.docx	07/12/2021	https://cert.gov.py/application/files/8416/3881/8348/BOL-CERT-PY-2021-34_Zoho_Manage_Engine_ServiceDesk_Plus_1.pdf	1962	459
Múltiples vulnerabilidades detectadas en productos SonicWall.	BOL-CERT-PY-2021-35 Sonic Wall.docx	10/12/2021	https://cert.gov.py/application/files/2616/3914/6015/BOL-CERT-PY-2021-35_Sonic_Wall.pdf	1962	587

EY

Luis Alberto Ayala Albertini Acosta
Socio

Título	Archivo	Fecha	Enlace	Enviados	Abiertos
Vulnerabilidad de ejecución remota de comandos en la librería Log4j de Java	BOL-CERT-PY-2021-36 Java libreria Log4 .docx	10/12/2021	https://cert.gov.py/application/files/5016/3916/5673/BOL-CERT-PY-2021-36_Java_libreria_Log4.pdf	1962	452
Vulnerabilidad de ejecución remota de comandos en el firmware del dispositivo TP Link TL-WR840N v5	BOL-CERT-PY-2021-37 TP-Link.docx	13/12/2021	https://www.cert.gov.py/application/files/2116/3942/4605/BOL-CERT-PY-2021-37_TP-Link.pdf	1962	473
Múltiples vulnerabilidades detectadas en Fortinet	BOL-CERT-PY-2021-38 Multiples vulnerabilidades en Fortinet.docx	14/12/2021	https://cert.gov.py/application/files/9816/3948/9519/BOL-CERT-PY-2021-38_Multiples_vulnerabilidades_en_Fortinet.pdf	1962	568
Microsoft publica parches para múltiples vulnerabilidades	BOL-CERT-PY-2021-39 Multilples vulnerabilidades de Microsoft.docx	17/12/2021	https://cert.gov.py/application/files/5216/3977/3022/BOL-CERT-PY-2021-39_Multilples_vulnerabilidades_de_Microsoft.pdf	1962	536
Microsoft publica parches para vulnerabilidades en Active Directory	BOL-CERT-PY-2021-40 Active Directory.docx	22/12/2021	https://cert.gov.py/application/files/3116/4020/2096/BOL-CERT-PY-2021-40_Active_Directory.pdf	1962	513
Actualización de seguridad para Apache HTTP Server	BOL-CERT-PY-2021 - 41 - Apache HTTP Server	23/12/2021	https://cert.gov.py/application/files/8816/4028/5582/BOL-CERT-PY-2021-41_Apache_HTTP_Server_.pdf	1962	573

EY

Luis Alberto Ayala Albertini Acosta
Socio

5. Guías de seguridad elaboradas

Título	Archivo	Fecha	Enlace
Registros DNS para Servidores de correo	GUIA-Registros-DNS-para-Servidores-de-correo.docx	29/11/2021	Pendiente de Aprobación por la MITIC (17/12/2021)

Luis Alberto Ayala Alberdi