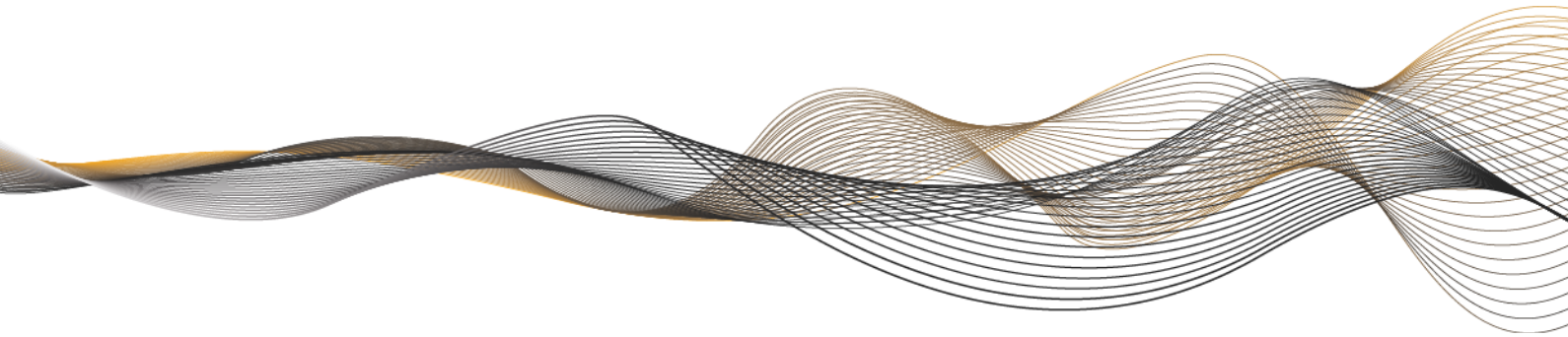
BASE4 SECURITY

ARG - MEX - CL - BRA - COL - PE - ESP - EEUU



CSIRT BASE4

Security - RFC 2350

11 de septiembre de 2023

Índice de contenidos

CSIRT BASE4 Security - RFC 2350

1. INFORMACIÓN DEL DOCUMENTO

1.1. Fecha de la última actualización

12 de septiembre de 2023

1.2. Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de csirt.info@base4sec.com

2. INFORMACIÓN DE CONTACTO

2.1. Nombre del equipo

"CSIRT BASE4 Security", Equipo de Respuesta a Incidentes de Seguridad Informática de BASE4 Security

2.2. Zona Horaria

UTC-3. Buenos Aires/Argentina.

2.3. Otras telecomunicaciones

Ninguna

2.4. Correo electrónico

Informe de incidentes: csirt.incident@base4sec.com

Key ID: 63BF1D73AA1A3F4E

PGP Fingerprint: B15F 136D 36AE 910F 7CC3 9F71 63BF 1D73 AA1A 3F4E

Información de carácter general: csirt.info@base4sec.com

Key ID: E3F559A8F8B6F4F0

PGP Fingerprint: D748 9F01 5217 3A5F 8487 5596 E3F5 59A8 F8B6 F4F0

2.5. Miembros del equipo

Una lista completa de los miembros del equipo no está disponible públicamente. Los miembros del equipo se identificarán ante la parte informante con su nombre completo en una comunicación oficial sobre un incidente.

2.6. Otra información

La información general de los servicios la podrá encontrar publicadas en el siguiente portal : https://www.base4sec.com/cybersoc/

2.7. Puntos de contacto con el cliente

El método preferido para comunicarse con CSIRT BASE4 Security en caso de incidentes por parte de sus clientes es mediante mensajes de correo electrónico con csirt.incident@base4sec.com. El equipo de respuesta a incidentes está disponible en función de los servicios contratados, en los siguientes horarios:

- **Consultas sobre servicios:** Horario comercial (09.00 - 18:00 horas)
- **Incidentes catalogados con peligrosidad baja o media:** Servicio 12x5 (8.00 - 20.00 horas)
- **Incidentes catalogados con peligrosidad alta o crítica:** Servicio de guardia de 24x7x365.

3. CARTA

3.1. Misión

El objetivo principal del CSIRT BASE4 Security es brindar el soporte a las organizaciones de la comunidad atendida o circunscripción de CSIRT BASE4 Security, en el proceso de respuesta a incidentes en todas sus fases. Realizando para ello labores de coordinación, apoyo y capacitación para la preparación; detección y análisis; contención, erradicación y recuperación; y actividades después de ocurrido un incidente. Contribuyendo de manera proactiva a la mejora continua de su ciberseguridad, y aportando los instrumentos necesarios para dar una respuesta rápida y eficiente frente a las ciberamenazas.

3.2. Comunidad Atendida/Circunscripción

La circunscripción de CSIRT BASE4 Security son los clientes internos y externos de BASE4 Security, sean estos del sector público o privado con los cuales se hayan suscrito o formalizado algún acuerdo de servicio que BASE4 Security provee como Respuesta a Incidentes de Ciberseguridad. Los incidentes atendidos por CSIRT BASE4 Security serán aquellos que afecten a las redes, sistemas y aplicativos de los clientes

internos y externos de BASE4 Security conforme a los servicios que preste el CSIRT, especificados en la sección 5 denominado "Servicios" del presente documento.

Los servicios de CSIRT BASE4 Security se proporcionan de preferencia de forma remota a través de un acceso seguro a la infraestructura donde se ha producido el incidente, y en caso excepcional de forma presencial en los países donde se cuente con los recursos disponibles y viabilidad técnica y logística.

3.3. Patrocinio y / o Afiliación

CSIRT BASE4 Security está patrocinado por el CyberSOC de BASE4 Security y busca estar afiliado a instituciones alrededor del mundo con la finalidad de colaborar, compartir información y brindar soporte en la respuesta de incidentes de ciberseguridad.

3.4. Autoridad

El CSIRT BASE4 Security ofrece asesoramiento constante a sus clientes en materia de ciberseguridad, llevando a cabo aquellas acciones que requieran sus clientes a nivel operativo y técnico. Teniendo siempre el cliente la potestad principal y última de decisión sobre las acciones a realizar.

4. POLÍTICAS

4.1. Tipos de incidentes y nivel de soporte

El CSIRT BASE4 Security aborda todo tipo de incidentes de ciberseguridad que se presenten en su circunscripción (ver 3.2). El nivel de apoyo brindado por CSIRT BASE4 Security variará según el tipo y la gravedad del incidente o problema, su impacto potencial o evaluado, el tipo de constituyente, el tamaño de la comunidad de usuarios afectada, y recursos disponibles del CSIRT BASE4 Security en el momento. Según el tipo de incidente de seguridad, CSIRT BASE4 Security implementará gradualmente sus servicios que incluyen respuesta a incidentes y análisis forense digital.

4.2. Cooperación, interacción y divulgación de información

El CSIRT BASE4 Security colabora con otros equipos especializados en la mejora de la seguridad, para ello puede compartir la naturaleza de los incidentes detectados en el ejercicio de sus funciones y los métodos de actuación llevados a cabo para su

resolución. No obstante, se considera información confidencial cualquier dato que pueda comprometer los sistemas de información o identificar a nuestros clientes no compartiendo ningún tipo de información relevante a los mismos, salvo consentimiento previo. Y cuando se comparte la forma como se realiza se basa en el protocolo TLP, el cual es aceptado internacionalmente.

4.3. Comunicación y autenticación

El método preferido de comunicación es por correo electrónico.

5. SERVICIOS

5.1. Servicios Reactivos

Estos servicios se activan como consecuencia de incidente, lo que viene a ser el componente central en el trabajo de CSIRT BASE4 Security para el manejo de incidentes de su comunidad atendida o circunscripción:

5.1.1. Clasificación del Incidente

CSIRT BASE4 Security clasifica los incidentes según su nivel de riesgo, asociado a los activos impactados, y la priorización de atención se establece en función de la clasificación de los procesos de negocio impactados. Asimismo, se realiza la investigación para concluir si efectivamente ocurrió un incidente, determinar el alcance de este, y evaluar el incidente en función de la información histórica disponible.

5.1.2. Gestión de incidentes

Este servicio tiene por objetivo manejar un incidente mediante el proceso de respuesta a incidentes que involucra las fases de preparación; identificación; contención, erradicación y recuperación; y actividades post incidente. El CSIRT BASE4 Security proporcionará la asistencia técnica mediante el análisis de equipos comprometidos, recomendaciones para la erradicación y eliminación de la causa del incidente, soporte en la restauración de los equipos y servicios afectados a su estado anterior del incidente y recomendaciones para asegurar los equipos afectados.

También, CSIRT-BASE4 recopilará estadísticas sobre los incidentes que ocurran dentro de su comunidad atendida o circunscripción, o que se vean involucrados de alguna

forma; y según sea necesario, notificará a la comunidad para protegerse contra los ataques conocidos.

Tenga en cuenta que CSIRT-BASE4 tiene por función la coordinación de respuesta a incidentes con información en parte provista por la comunidad atendida o circunscripción, sin coacción. En ese sentido, es probable que no siempre sea posible llegar a una resolución exitosa de todos los incidentes, ya que la resolución real depende de las correctas acciones que realice y ejecute la parte interesada.

5.1.3. Análisis Forense Digital

El CSIRT BASE4 Security proporciona el servicio de análisis forense con fines de investigación durante y post incidente para buscar evidencia que permita identificar las acciones realizadas por el actor malicioso, así como la validación de las hipótesis de la investigación según sea el caso y objetivos establecidos por el cliente. Para esta actividad el equipo del CSIRT BASE4 Security se apoyará en toda información y registro de evidencia disponible y que sea viable para el desarrollo de las investigaciones y la corroboración de las hipótesis o su descarte.

5.2. Servicios proactivos

Estos servicios tienen por finalidad proveer información oportuna para ayudar a protegerla infraestructura y sistemas de la comunidad atendida o circunscripción, anticipándose a los ataques cibernéticos. Por lo tanto, el éxito o implementación oportuna de los servicios reducirá el número de incidentes futuros. El CSIRT BASE4 Security coordina y mantiene los siguientes servicios en la medida de lo posible en función de sus recursos:

5.2.1. Consulting

El CSIRT BASE4 Security puede aportar con el conocimiento y experiencia técnica y de gestión del equipo para diversas actividades de consultoría para la mejora de las capacidades de detección y respuesta a incidentes de ciberseguridad. Entre estas la revisión documental y elaboración de Playbooks y otros instrumentos técnicos documentales que permitan aplicar y operativizar las mejoras prácticas en este ámbito.

5.2.2. Threat Hunting

La búsqueda proactiva de comportamientos anómalos que puedan ser indicadores de la presencia de un actor de amenaza que ha logrado evadir los controles de seguridad implementados es un enfoque proactivo que el CSIRT BASE4 Security realiza bajo un enfoque metodológico y sistemático, considerando el entorno y sector de comunidad atendida o circunscripción.

5.2.3. Emulación de Adversario

El CSIRT BASE4 Security puede diseñar y ejecutar ejercicios técnicos para poner a prueba las capacidades técnicas y los procesos de los equipos de ciberseguridad, para identificar oportunidades de mejora en los diferentes aspectos como visibilidad, detección, alerta y respuesta.

6. FORMULARIOS DE NOTIFICACIÓN DE INCIDENTES

Utilice la siguiente plantilla y envíela por correo electrónico a la dirección correspondiente. Por favor, proporcione tantos detalles como sea posible, adjuntando cualquier archivo relevante si es necesario (registros, mensajes de correo electrónico, capturas de pantalla, etc..):

```
================================================== ================
REPORTE DE INCIDENTE
¿Ha informado de este incidente a otras personas u organizaciones?:
- Tipo de incidente detectado (Phishing, Malware, DDoS,  Uso/acceso no
autorizado...):
Utilice la Taxonomía de Incidente de Referencia desarrollada por la
Reference Security Incident Taxonomy Task Force cuando sea posible, ver
https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/b
lob/master/working_copy/humanv1.md
- ¿Cuándo se detectó este incidente? (fechahora y zona horaria):
- Detalles del incidente (breve descripción del incidente):
Complete la siguiente información sobre el sistema afectado y host del
atacante (si se conoce).
--- Sistema afectado (duplicar si es necesario) ---
Nombre de host:
Dominio:
Dirección IP:
Puerto:
Sistema operativo:
```

```
Propósito principal del sistema afectado (estación de trabajo,
web/DNS/FTP/Aplicación/Servidor de base de datos, Enrutador, Firewall...):
--- Fin del sistema afectado —

--- Host atacante (duplicar si es necesario) ---
Nombre de host:
Dominio:
Dirección IP:
Puerto:
Protocolo:
--- Fin del host atacante ---
==================================================
```

7. DESCARGOS DE RESPONSABILIDAD

Si bien se tomarán todas las precauciones en la preparación de la información, notificaciones y alertas, CSIRT BASE4 Security no asume ninguna responsabilidad por errores u omisiones, ni por daños resultantes del uso de la información proporcionada durante la ejecución de sus servicios.

Control Documental

Versión: **01** Vigencia: **13/09/2023**	Revisión: **14/09/2023**
Informe generado por: **Carlos Aguilar**	Informe revisado por: **Mauricio Cruz**
Confidencialidad: **TLP:CLEAR**	

BASE4
SECURITY

www.base4sec.com