RFC 2350

Elaborador por	Revisado por	Aprobado por
Responsable del Sistema Integrado de Gestión	Director de Ingeniería	Directorio

1. INFORMACIÓN DEL DOCUMENTO

1.1. Fecha de la última actualización

La versión 1 del documento RFC 2350 de SUPRA SECURITY CENTER (SSC) fue publicada el 01 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 correo contacto@supra.com.pe o por la página web https://supra.com.pe/contacto/

2. INFORMACIÓN DE CONTACTO

2.1. Nombre del equipo:

SUPRA SECURITY CENTER (SSC)

2.2. Zona horaria:

GMT-5

2.3. Otras telecomunicaciones

Ninguna

2.4. Correo electrónico

Informe de incidentes: incidencias@supra.com.pe

PGPKEY Incidencias: BC31 FCD9 2855 34C3 7B29 B72A 8A12 4031 9E2E F4B2

Información de carácter general: contacto@supra.com.pe

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://supra.com.pe/soluciones/supra-security-center/

2.7. Puntos de contacto con el cliente

Página: https://supra.com.pe/contacto/

Correo: incidencias@supra.com.pe

Teléfono: (+511) 6440657

Nuestro horario de respuesta es 24x7x365, todos los días de la semana el Ingeniero de turno está disponible para incidentes y se puede contactar al correo incidencias@supra.com.pe.

3. CARTA

3.1. Misión

SUPRA SECURITY CENTER (SSC) tiene como misión brindar el soporte a las organizaciones de la comunidad atendida, en el proceso de respuesta a incidentes en todas sus fases, prevención, detección y gestión de incidentes. Con el fin de conseguir un ciberespacio más seguro y confiable, preservando la clasificación de información, formando al ingeniero experto de Supra Networks, así como aplicando políticas y procedimientos de seguridad.

3.2. Comunidad Atendida

Los incidentes atendidos por SUPRA SECURITY CENTER (SSC) serán aquellos que afecten a sistemas de los clientes internos y externos, así como cualquier otro sistema en el que se procese información clasificada.

3.3. Patrocinio y / o Afiliación

SUPRA SECURITY CENTER (SSC) está patrocinado por TELECOM BUSINESS SOLUTION S.A.C, de nombre comercial Supra Networks. Supra Security Center (SSC) 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. Está conformado de la siguiente manera:

- Director de Ingeniería
- Jefe de SNOC
- Ingenieros especialistas en gestión de incidentes

3.4. Autoridad

Se opera bajo los auspicios y con la autoridad delegada de Supra Networks y los clientes a los que le brinda el servicio con el objetivo de manejar una gestión de incidente efectiva de los clientes internos y externos.

4. POLÍTICAS

4.1. Tipos de incidentes y nivel de soporte

SUPRA SECURITY CENTER (SSC) está autorizado para atender cualquier tipo de incidentes de ciberseguridad que se produzcan en su comunidad atendida y que forme parte de los servicios que brinde.

Supra Security Center (SSC) maneja diferentes tipos de incidentes y sus criterios de determinación de peligrosidad, el nivel de apoyo dependerá de ambos factores y de la gravedad que determine el personal del SSC.

4.2. Cooperación, interacción y divulgación de información

La información manejada por SUPRA SECURITY CENTER (SSC) es tratada con absoluta confidencialidad, de acuerdo a las políticas y procedimientos para la gestión de incidentes definidos para el SSC, utilizadas para la protección de la información clasificada.

Toda la información suministrada al SSC será utilizada para ayudar a resolver incidentes de ciberseguridad, y sólo se distribuirá a otros equipos y miembros según la necesidad específica y de forma anónima.

En cuanto a la forma como se comparte, 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: incidencias@supra.com.pe.

5. SERVICIOS

5.1 Servicios Reactivos

La respuesta a incidentes proporciona disponibilidad 24*7 para coordinar la recuperación de todo tipo de incidentes relacionados con las TIC y consiste en experiencia, herramientas y otras capacidades para actuar, analizar y comunicarse con las partes interesadas y los medios de comunicación.

5.1.1. Clasificación del Incidente

- Investigación del incidente ocurrido.
- Determinación de la extensión del incidente.
- Evaluación y comparación del incidente con históricos.

5.1.2. Coordinación de incidentes

- Facilitar el contacto con otros sitios que puedan estar involucrados.
- Comunicarse con las partes interesadas y los medios
- Brindar soporte general para la coordinación durante la resolución del incidente

5.1.3. Resolución de incidentes

- Causa inicial del incidente.
- Mitigación y contención del incidente.
- Resolución y erradicación del incidente, en base a la metodología implementada por el equipo.

5.2. Actividades proactivas

Estos servicios tienen como objetivo proveer información oportuna para ayudar a proteger la infraestructura de la comunidad, anticipándose a los ataques cibernéticos. Por tanto, la implementación de estos servicios reducirá el número de incidentes futuros.

- Educación y cultura: proporciona estos servicios mediante capacitaciones sobre buenas prácticas, seguridad de la información, etc.
- Alertas y boletines: se distribuye información de inteligencia en relación con campañas maliciosas detectadas, nuevas amenazas, indicadores de compromiso, etc., así como recomendaciones sobre las acciones a tomar en respuesta a los mismos.
- Análisis de Vulnerabilidades: Corresponde a la evaluación de vulnerabilidades de la infraestructura de red, equipos, software, aplicaciones y otros dispositivos de red con fines de brindar recomendaciones para las correcciones oportunas.
- Monitoreo en tiempo real 24x7x365 (SOC como Servicio)
- Threat Hunting: investigación de amenazas.
- Auditorías: evaluación CMM, evaluación según la norma ISO 27001 de seguridad de la información.
- Pruebas de penetración holística de 360°: Ethical hacking
- Inteligencias de amenazas: monitoreo de la darkweb.

6. FORMULARIOS DE NOTIFICACIÓN DE INCIDENTES

Para reportar incidentes, sírvase remitir un mensaje de correo electrónico a la cuenta incidencias@supra.com.pe

7. DESCARGOS DE RESPONSABILIDAD

SUPRA SECURITY CENTER (SSC) toma todas las precauciones en la preparación de información, notificaciones, alertas e informes, pero no asume ninguna responsabilidad por errores u omisiones, ni por daños resultantes del uso de la información suministrada.