smart global

RFC2350

CSIRT SMART GLOBAL SAC

1. Información del documento

1.1. Fecha de última actualización

La versión 01 del documento SG-IRT-OTR-01 RFC 2350 Smart Global de SMART GLOBAL S.A.C. fue publicada el 01 de febrero del 2024.

1.2. Lista de distribución de notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario especifico dirigirse al correo csirt@smartglobal.pe.

1.3. Identificación del documento

Título: SG-IRT-OTR-01 RFC 2350 Smart Global_es.pdf
Ubicación: **https://www.smartglobal.pe/Cms_Data/Sites/SmartGlobal/Files/csirt/SG-IRT-OTR-01%20RFC%202350%20Smart%20Global_es.pdf**
Versión: 1.0
Fecha del documento: 01 de febrero del 2024
Caducidad: Este documento es válido hasta que sea reemplazado por una versión posterior.

2. Información de contacto

2.1. Nombre del equipo

Smart Global CSIRT

2.2. Dirección

C. Amador Merino Reyna 465, San Isidro 15046, Lima 15001. Lima. Perú.

2.3. Zona horaria

GMT-5. Lima/Perú.

2.4. Número de teléfono

+511 641-8341 o (0800)-71-770.

2.5. Número de fax

No existente.

2.6. Otras telecomunicaciones

No existente.

2.7. Dirección de correo electrónico

Intercambio de información relacionado con incidentes: csirt@smartglobal.pe.

2.8. Claves públicas y otra información de cifrado

PGP se utiliza para intercambios de información funcionales entre el CSIRT de Smart Global S.A.C y otros equipos o interesados (informes de incidentes, alertas, etc.). El CSIRT de Smart Global S.A.C tiene una clave PGP pública.

Fingerprint	9D67 8F12 B0D3 6F12 36CD C64D C016 33A2 15E9 4FF5
URL de la clave PGP pública	https://www.smartglobal.pe/Cms_Data/Sites/SmartGlobal/Files/politicas/PGPCSIRT_SG_pub.txt

2.9. Miembros del equipo

Equipo Smart Global CSIRT (Operadores CyberSOC, Ingenieros de Ciberseguridad y Especialistas en Respuesta a Incidentes).

2.10. Otra información

Toda la información sobre el CSIRT de Smart Global S.A.C se encuentra disponible en el siguiente link https://www.smartglobal.pe/Csirt/QuienesSomos.

2.11. Puntos de contacto con el cliente

La principal opción de contacto del CSIRT de Smart Global S.A.C con nuestros clientes es mediante mensajes de correo electrónico con la dirección de correo csirt@smartglobal.pe y llamada telefónica.

3. Carta

3.1. Misión

Prestar servicios de monitoreo, detección, investigación, solución y/o mitigación de incidentes de seguridad, reportados por nuestros clientes en coordinación con nuestro equipo de respuesta ante incidentes, la contención de un incidente puede ser de manera presencial o remota.

3.2. Miembros

Los servicios de CSIRT de Smart Global S.A.C están disponible para sus clientes que adquieran el servicio de respuesta ante incidentes de seguridad. El CSIRT de Smart Global S.A.C se constituye como un CSIRT comercial de carácter mixto.

3.3. Autoridad

El CSIRT de Smart Global S.A.C opera bajo el auspicio y bajo la dirección de la Gerencia General. La responsabilidad del CSIRT de Smart Global S.A.C es brindar apoyo técnico en la respuesta ante incidentes de seguridad a sus miembros. Desde el monitoreo y detección hasta la configuración de equipos de seguridad, siempre que los equipos de seguridad los administre Smart Global S.A.C. En el escenario en el cual CSIRT se limite a proporcionar servicios de respuesta ante incidentes de seguridad de la información sin gestionar directamente los equipos de seguridad, su función principal consistirá en ofrecer asesoramiento técnico destinado a contener y mitigar el incidente de seguridad en cuestión.

4. Política

Smart Global S.A.C. tiene definidas políticas y procedimientos para la operación del servicio de CSIRT, los cuales podrán ser compartidos únicamente con los clientes que adquieran el servicio y deseen obtener información al respecto. No obstante, de acuerdo con lo establecido en el RFC 2350, se describe lo siguiente:

4.1. Tipos de incidente y nivel de soporte

Los clientes y/o miembros del CISRT de Smart Global S.A.C reportarán toda actividad asociada a incidentes de seguridad de la información a través del correo electrónico csirt@smartglobal.pe, formulario de reporte de incidente y/o llamada telefónica al CSIRT. El coordinador de Smart Global CSIRT debe gestionar todos los requerimientos que ingresen a través de los medios de comunicación establecidos, de la siguiente manera:

- Validar el servició del solicitante para la gestión de incidente reportado.
- Para el cliente que tenga el servicio se procederá con la asignación de un técnico especialista de respuesta a incidentes de seguridad para la gestión del incidente reportado.
- Para los requerimientos de atención a incidentes de seguridad que procedan de clientes que no cuente con el servicio, el Coordinado del CSIRT de Smart Global S.A.C validará la posibilidad de apoyo.
- Además de asignar un especialista de respuesta a incidentes de seguridad, éste establecerá la clasificación del incidente conforme a los criterios definidos por el CSIRT, y procederá a ejecutar el procedimiento de respuesta ante Incidentes.

4.2. Cooperación, interacción y divulgación de información

El CSIRT de Smart Global S.A.C podrá colaborar con otros CSIRT y CERT nacionales y/o internacionales. Asimismo, con nuestro cliente y/o miembros bajo la autorización del coordinado del CSIRT. La información generada por los servicios se puede compartir con empresas afiliadas a Smart Global S.A.C, así como los proveedores y partners de servicios de ciberseguridad, según sea necesario el intercambio de información.

El intercambio de información se realizará bajo los términos de contrato o términos acordados con nuestros clientes y/o miembros. La información que se podrá intercambiar es la siguiente:

- IoC (Indicadores de compromiso)
- Perfilamiento de ataques y/o amenazas.
- Vulnerabilidades que puedan afectar a nuestros clientes y/o miembros.

Toda información que será compartida deberá de ser aprobado por el coordinador del CSIRT de Smart Global S.A.C.

4.3. Comunicación y autenticación

Los niveles de intercambio de información dependerán de su destinatario, el CSIRT de Smart Global S.A.C, identifica los siguientes niveles de comunicación:

El intercambio de información propia del cliente y/o miembro: Cuando el CSIRT de Smart Global S.A.C, establezca un intercambio de información de indicadores de compromisos (informes y/o reportes) y alertas propias del cliente y/o miembro se aceptará como envió seguro el uso de correos electrónicos sin encriptar.

Intercambio de información consolidados y nuevas amenazas: Cuando el CSIRT de Smart Global S.A.C, realice un intercambio de información de indicadores de compromiso (IoC) o nuevas amenazas detectadas a través de reportes consolidados se considera como envió seguro mediante PGP como mecanismo de autenticación.

Intercambio de información con CSIRT/CERT regionales: Cuando el CSIRT de Smart Global S.A.C, establezca un intercambio de información sobre incidentes y/o indicadores de compromiso sobre escenarios de riesgo actuales, se considera como envió seguro mediante PGP como mecanismo de autenticación.

El cumplimiento de esta política se realizará desde el correo oficial del CSIRT de Smart Global csirt@smartglobal.pe así como con el uso de correos institucionales del personal que forma parte del CSIRT. Se prohíbe el intercambio de información del CSIRT de Smart Global S.A.C, por medios no oficiales como: redes sociales, correos electrónicos personales o dispositivos de almacenamiento externo no autorizados. El CSIRT de Smart Global S.A.C se basa en el estándar de TLP (Traffic Light Protocol) para el intercambio de información confidencial.

5. Servicios

5.1. Gestión de eventos de seguridad de la información.

El cual tiene como objetivo identificar los incidentes de seguridad a partir de la correlación y análisis de eventos de seguridad.

Monitoreo y detección: Se realizará el monitoreo de los eventos de seguridad de los clientes, para lo cual es necesario que los equipos de seguridad de los clientes envíen información a la herramienta SIEM de Smart Global S.A.C, a fin de identificar posibles incidentes de seguridad de la información, como ataques, intrusiones, filtración de datos o infracciones en las políticas de seguridad.

Análisis de eventos: La selección de posibles incidentes de seguridad detectados y clasificados como incidentes de seguridad para realizar el procedimiento de análisis o para descartarlo como falsa alarma. Los eventos detectados como incidentes o posibles incidentes serán clasificados según la matriz desarrollada por Smart Global S.A.C.

5.2. Gestión de Incidentes de seguridad de la información

El servicio consiste en ayudar durante un ataque o incidente. El CSIRT de Smart Global S.A.C estará preparado para ayudar y apoyar a los clientes, el equipo de Smart Global CSIRT no solo tiene la capacidad de recopilar y evaluar informes de incidentes de seguridad, sino también de analizar los datos relevantes y realizar un análisis técnico detallado del propio incidente. A partir de este análisis se pueden recomendar medidas de mitigación y recuperación de incidentes, y asesorar a los clientes a aplicar las recomendaciones.

Análisis de incidentes de seguridad de la información: Analizar y comprender mejor los incidentes de seguridad confirmados. Este servicio consiste en funciones para comprender los incidentes de seguridad y sus repercusiones reales y potenciales, a fin de detectar los problemas o vulnerabilidades o deficiencias que hicieron posible el éxito del ataque o la explotación.

Mitigación y recuperación: contener el incidente de seguridad en la medida de lo posible para limitar el impacto a nuestros clientes, reducir las pérdidas y recuperarse de los daños, evitar nuevos ataques y nuevas perdidas mediante la eliminación de las vulnerabilidades o puntos débiles explotados y mejorar la ciberseguridad en general.

Coordinación de incidentes de seguridad de la información: Garantizar la notificación oportuna y la distribución de información, exacta, mantener el flujo de información y

rastrear la situación de las actividades de los clientes o a las que se les encomiende participar en la respuesta al incidente de seguridad; y asegurar que el plan de respuesta se ejecute por las partes interesadas.

Descubrimiento y/o investigación de vulnerabilidades: Encontrar, conocer o buscar nuevas vulnerabilidades (previamente desconocidas). El descubrimiento de una nueva vulnerabilidad es el primer paso necesario para iniciar el ciclo de la gestión de vulnerabilidades. El servició incluye aquellas funciones y actividades que el CSIRT de Smart Global S.A.C pueda realizar activamente a través de su propia investigación u otros servicios para descubrir una nueva vulnerabilidad.

Coordinación de vulnerabilidades: Intercambiar información y coordinar las actividades con nuestros clientes y/o miembros en el proceso de divulgación de vulnerabilidades. La gestión de las vulnerabilidades implica notificar, colaborar y coordinar el intercambio de información de las partes interesadas.

6. Medio de comunicación para reporte de incidentes

La notificación de incidentes puede realizarse mediante:

- Formulario de registro de incidentes en el sitio web www.smartglobal.pe
- Correo electrónico: csirt@smartglobal.pe
- Llamada telefónica al numero 0800-71-770 o +51 (01) 641-8341.
- Cualquier otro medio que se establezca en el alcance del servicio.

7. Descargos de responsabilidad

El CSIRT de Smart Global S.A.C tomará todas las precauciones en la preparación de información, notificaciones y alertas. No obstante, no asumirá responsabilidad por errores, omisiones o daños resultantes de la información contenida en el mismo.