




smart global

RFC2350

CSIRT SMART GLOBAL SAC

	OTRO	TLP: CLEAR		
		Código:	SG-IRT-OTR-01	
	RFC 2350	Versión:	1.0	
		Aprobado Por:	Jose Tovar	
		Fecha Aprob.:	01 febrero 2024	
		Página	Pág. 2 de 6	

1. Document Information

1.1. Last update date

The version 01 of the document SG-IRT-OTR-01 RFC 2350 Smart Global by SMART GLOBAL S.A.C was published on February 1, 2024.

1.2. Notification distribution list

There is a public distribution list for communications and notifications related to information security events and/or incidents through csirt@smartglobal.pe.

Please direct any questions or comments to the following email address csirt@smartglobal.pe.

1.3. Document identification

Title: SG-IRT-OTR-01 RFC 2350 Smart Global.pdf

Version: 1.0

Document Date: February 1, 2024

Expiration: This document is valid until it is replaced by a later version.

2. Contact Information

2.1. Team name

Smart Global CSIRT

2.2. Address

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

2.3. Time zone

GMT-5. Lima/Perú.

2.4. Phone number

+511 641-8341, ask for CSIRT Smart Global

2.5. Número de fax

Not available.

2.6. Other telecommunications

Not available.


2.7. Email address

Information exchange related to incidents: csirt@smartglobal.pe

2.8. Public keys and other encryption information

PGP is used for functional information exchanges between CSIRT Smart Global and others teams or stakeholders (incidents reports, alerts, etc). CSIRT Smart Global has a public PGP key.

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

	OTRO	TLP: CLEAR		
		Código:	SG-IRT-OTR-01	
	RFC 2350	Versión:	1.0	
		Aprobado Por:	Jose Tovar	
		Fecha Aprob.:	01 febrero 2024	
		Página	Pág. 3 de 6	

2.9. Team members

CSIRT Smart Global team (Operators, Analysts, Incidents Response Specialists).

2.10. Other information

All information about CSIRT Smart Global is available at the following link www.smartglobal.pe

2.11. Customer contact points

The primary contact option of CSIRT Smart Global with our clients is through email messages to the address csirt@smartglobal.pe.

3. Letter

3.1. Misson

To provide monitoring, detection, investigation, resolution, and/or mitigation services for security incidents reported by our clients in coordination with our incident response team. The containment of an incident can be managed either in person or remotely.

3.2. Members

The CSIRT Smart Global services are available to clients who purchase the incident response service. CSIRT of Smart Global S.A.C. is established as a commercial CSIRT of mixed nature.

3.3. Authority

The CSIRT of Smart Global S.A.C operates under the auspices and direction of the General Management. The responsibility of the CSIRT of Smart Global S.A.C is to provide technical support in responding to security incidents to its members. From monitoring and detection to the configuration of security equipment, as long as the security equipment is managed by Smart Global S.A.C. In the scenario where CSIRT Smart Global is limited to providing information security incident response services without directly managing the security equipment, its main function will consist of offering technical advice aimed at containing and mitigating the security incident in question.


4. Policy

Smart Global S.A.C. has defines policies and procedures for the operation of the incident management service, which can be share only with clients who purchase the Service and wish to obtain the information about it. However, in accordance with RFC 2350, the following is described:

4.1. Incident types and support level

Client and/or members of the CSIRT of Smart Global S.A.C. will report all activities associated with information security incidents via email to csirt@smartglobal.pe. The coordinator of CSIRT Smart Global must manage all request that come through email considering the following:

- Validate the service of the applicant for the management of the reported incident.
- For the client who has the service, proceed with the assignment of a security incident response specialist technician for the management of the reported incident.

	OTRO	TLP: CLEAR		
		Código:	SG-IRT-OTR-01	
	RFC 2350	Versión:	1.0	
		Aprobado Por:	Jose Tovar	
		Fecha Aprob.:	01 febrero 2024	
		Página	Pág. 4 de 6	

- For security incident attention requests that come from a client who does not have the service, the coordinator of CSIRT Smart Global Will validate the possibility of support.
- In addition to assigning a security incident response specialist, the specialist will establish the classification of the incident considering the classification of incidents defined by CSIRT Smart Global.

4.2. Cooperation, interaction, and disclosure of information

The CSIRT o Smart Global S.A.C may collaborate with other national and/or international CSIRTs and CERTs. Likewise, with our clients and/or members under the authorization of the coordinator of the CSIRT Smart Global S.A.C. as well as cybersecurity service providers and partners, as necessary for the exchange of information.

The exchange of information will be carried out under the terms of the contracts or terms agreed upon with our clients and/or members. The information that can be exchanged includes:

- IoC (Indicators of compromise)
- Profiling of attacks and/or threats.
- Vulnerabilities that may affect our clients and/or members.

All information to be shared must be approved by the coordinator of CSIRT Smart Global.

4.3. Communication and authentication

The levels of information exchanges will be depend on the recipient. CSIRT Smart Global identifies the following levels of communication:

Information exchange specific to the client and/or client: When CSIRT Smart Global, establishes an exchange of indicators of compromise (reports and/or alerts) specific to the client and/or member, the use of unencrypted emails will be accepted as a secure method of sending.

Exchange of consolidated information and new threats: When CSIRT Smart Global conducts an exchange of information on regional indicators of compromise or new threats detected through consolidated reports, the use of unencrypted email is considered a secure methos of sending.

Exchange of information with regional CSIRTs/CERTs: When CSIRT Smart Global, establishes an exchange of information on incidents and/or indicators of compromise concerning current risk scenarios, it must be done through encrypted emails.


Compliance with this policy will be conducted through the official CSIRT Smart Global email csirt@smartglobal.pe as well as through the use of institutional emails of the staff involved in the process (Operators, Analysts, Coordinators, Heads, Managers, Information Security Consultants). The Exchange of information from CSIRT Smart Global through unofficial means such as social networks, personal emails, or unauthorized external storage devices is prohibited. CSIRT Smart Global relies on the Traffic Light Protocol (TLP) standard for the Exchange of confidential information.

5. Services

5.1. Information security event management.

This aims to identify security incidents through the correlation and análisis of security events.

Monitoring and detection: Monitoring of client security events will be carried out, for which it is necessary for client security teams to send information to Smart Global's SIEM tool, in order to

	OTRO	TLP: CLEAR	
		Código:	SG-IRT-OTR-01
	Versión:	1.0	
	RFC 2350	Aprobado Por:	Jose Tovar
		Fecha Aprob.:	01 febrero 2024
		Página	Pág. 5 de 6

identify possible information security incidents, such as attacks, intrusions, data leaks, or breaches of security policies.

Event analysis: The selection of potential security incidents detected and classified as security incidents to carry out the analysis procedure or to discard it as false alarm. Events detected as incidents or potential incidents will be classified according to the matrix developed by Smart Global S.A.C.

5.2. Information security incident management

The service consists of assistance during an attack or incident. CSIRT Smart Global S.A.C. will be prepared to help and support clients. The CSIRT team is not only capable of collecting and evaluating security incident reports but also analyzing relevant data and conducting a detailed technical analysis of the incident itself. From this analysis, mitigation and incident recovery measures can be recommended and clients can be advised to apply the recommendations.

Information security incident analysis: Analyze and better understand confirmed security incidents. This service includes functions to understand security incidents and their actual and potential repercussions, in order to detect the issues, vulnerabilities, or deficiencies that made the attack or exploitation possible.

Mitigation and recovery: Contain the security incident as much as possible to limit the impact on our clients, reduce losses and recover from the damage, prevent new attacks and further losses by eliminating the vulnerabilities or weak points exploited, and improve overall cybersecurity.

Information security incident coordination: Ensure timely notification and accurate distribution of information, maintain the flow of information and track the situation of client activities or those assigned to participate in the security incident response; and ensure that the response plan is executed by the stakeholders.


Vulnerability discovery and/or investigation: Find, become aware of, or search for new vulnerabilities (previously unknown). The discovery of a new vulnerability is the first necessary step to initiate the vulnerability management cycle. The service includes those functions and activities that CSIRT Smart Global can actively perform through its own research or other services to discover a new vulnerability.

Vulnerability coordination: Exchange information and coordinate activities with our clients and/or members in the process of vulnerability disclosure. Vulnerability management involves notifying, collaborating, and coordinating the information exchange of stakeholders.

6. Communication means for incident reporting

Incident notifications can be made through:

- Incident registration form on the website www.smartglobal.pe
- Email: csirt@smartglobal.pe
- Phone call to the number 0800-71-770 or +51 (01) 641-8341.

	OTRO	TLP: CLEAR	
		Código:	SG-IRT-OTR-01
	Versión:	1.0	
	RFC 2350	Aprobado Por:	Jose Tovar
		Fecha Aprob.:	01 febrero 2024
		Página	Pág. 6 de 6

7. Disclaimer

CSIRT Smart Global will take all precautions in the preparation of information, notifications, and alerts. However, it will not assume responsibility for errors, omissions, or damages resulting from the information contained therein.