ACD-TRC

RFC 2350

Pasión por
la tecnología

CONTROL DATA

CLIENT	TRC
REFERENCE	
KIND OF WORK	Internal memorandum
DATE	02/01/2024

WRITTEN BY	SUPERVISED BY	APPROVED BY
EMILIO RICO		

VERSION REGISTER

EDITION	DATE	WHAT WAS CHANGED	DESCRIPTION
V1	05/01/2024	n.a.	n.a.

ÍNDICE DE CONTENIDO

1. INTRODUCTION.

The objective of this document is to establish and define the policies, responsibilities, procedures and resources necessary for the effective operation of the Computer Security Incident Response Team (CSIRT) of the TRC company.
The document is organized according to the model recommended by IETF RFC 2350, available at:

- https://tools.ietf.org/html/rfc2350.

1.1 Scope.

This document applies to all TRC company personnel, resources and information systems that are involved in the detection, response and mitigation of computer security incidents.

1.2 Recipients.

The recipients of this document are ACD-TRC clients, as well as any other incorporated CSIRT or organization with a legitimate interest in the services provided, and the general public. Consequently, the document can be distributed freely, being subject exclusively to copyright controls.

1.3 Locations where this document may be found.

This document is publicly accessible through the TRC website, specifically in the section corresponding to the ACD-TRC: https://www.grupoTRC.com/csirt

1.4 Authenticating this document.

This document has been signed with the PGP key of the csirt@grupotrc.com account of the ACD-CRT. Both the public key and the signature are available on the ACD-TRC website: https://www.grupoTRC.com/csirt

2. CONTACT INFORMATION.

2.1 Name of the team

- ACD-TRC

2.2 Address

Calle Albasanz 25, 28037 Madrid. España

2.3 Time Zone

Madrid, España (UTC+1)

2.4 Telephone number

The following phone number is enabled as an alternative method:

- +34 912 670 105

2.5 Electronic mail address.

Incident management: **csirt@grupotrc.com**

2.6 Public Keys.

ACD-TRC uses the following email address for communications related to incident response:

- csirt@grupotrc.com
- clave PGP: 399BE493235E667BF458C56047514C227B278F0F

For administrative communications or queries, the address is used:

- sat@grupotrc.com asociada
- clave PGP: 6B23B2435EA762A96B81C515C169CB4A3035100D

These public keys are available at the CSIRT web site.

2.7 Team members.

No public information is provided about the ACD-TRC CSIRT team members

3. MISSION.

3.1 PURPOSE

The ACD-TRC is a private CSIRT that was created by TRC Group Management mandate, with the objective of providing both internal (internal CSIRT) and external services to other organizations and companies, whether public or private (commercial CSIRT). The ACD-TRC's mission is to respond to cybersecurity challenges, making available to the entire TRC Group and its external clients the security services necessary to protect their information systems against security incidents that may affect the integrity, confidentiality or availability of their information and/or harm their operations or reputation.

ACD-TRC intends to provide these services to its clients:

- Improve real-time visibility of your cybersecurity situation.
- Anticipate possible threats and reduce the attack surface.
- Early incident detection and contain them quickly.
- Respond effectively to security incidents and limit the impact.
- Recover activity in the shortest time possible.

3.2 Functions

3.2.1 Incident Response

- Detection and analysis of cybersecurity incidents.
- Coordination and execution of response to cyber incidents.
- Mitigation and recovery of affected systems.
- Post-incident evaluation and lessons learned.

3.2.2 Cyber Threat Intelligence

- Cyber threat intelligence collection and analysis.
- Assessment of exposure to emerging threats.
- Collaboration with external sources to obtain relevant intelligence.
- Implementation of proactive measures based on intelligence.

3.2.3 Cybersecurity Education and Awareness

- Development and delivery of cybersecurity awareness programs.
- Ongoing training for employees on the latest threats and best practices.

3.3 Development Activities

To achieve its mission. ACD-TRC …

- Has highly qualified personnel with experience in information security, with the capacity to provide the services offered, as well as to analyze and respond appropriately to any security incident.
- Has a set of necessary and appropriate procedures and tools for the provision of the services offered and aligned with compliance with legal regulations.
- Performs continuous monitoring, reducing detection times for possible incidents, identifying which threats require immediate intervention, and discriminating false positives.
- Performs proactive and preventive tasks to improve the security of its clients.
- Exchanges technical information about incidents with other CERTs / CSIRTs to improve the joint response to them.
- Periodically executes Quality and Safety audit processes on the services provided, based on the standards and regulations commonly recognized in the sector.

- Applies the best practices commonly recognized in the sector.

All managed security services offered by the SACD-TRC to clients and/or their information systems have the medium ENS level (National Security Scheme)..

4. Constituency.

All services provided by ACD-TRC are aimed at all departments, units and services of the companies belonging to the TRC Group, as well as external companies and/or organizations, whether public or private, that subscribe to them.

4.1 Authority

The ACD-TRC is located within the Cybersecurity Directorate of the TRC Group. The ACD-TRC operates, within the TRC Group, under the authority of the Head of Corporate Information Security and the Cybersecurity Directorate.

5. Policies.

5.1 Types of Incidents and Level of Support.

ACD-TRC is authorized to address all types of computer security incidents that occur at its constituency.

The typology of the managed security incidents corresponds to what is established by the National Cryptological Center of Spain, CCN-CERT, taking as reference the Security Guide CCN-STIC 817 “Cyberincident Management” within the scope of the National Security Scheme (ENS), available at the URL:

- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

The level of support provided in each case will depend on what is contractually established with each ACD-TRC client..

Resources will be allocated according to the following priorities:

- Threats to the physical safety of human beings.
- Root or system-level attacks on any Management Information System or any part of the backbone network infrastructure.
- Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.
- Compromise of restricted confidential service accounts or software installations, in particular those used for MIS applications containing confidential data, or those used for system administration.
- Denial of service attacks on any of the above three items. Any of the above at other sites, originating from the constituency of Grupo Banco Sabadell CERT.
- Large-scale attacks of any kind.
- Threats, harassment, and other criminal offenses involving individual user accounts.
- Compromise of individual user accounts on multi-user systems.
- Compromise of desktop systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations.
- Denial of service on individual user accounts..

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. In most cases, ACD-TRC will provide pointers to the information needed to implement appropriate measures.

ACD-TRC is committed to keeping the constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited..

5.2 Co-operation, Interaction and Disclosure of Information.

The ACD-TRC interacts in its daily operations with other CSIRTs, legal authorities, sources of information and intelligence, client organizations, suppliers, manufacturers, etc. But especially with the three (3) national CERTs.:

- CCN-CERT (**https://ccn-cert.cni.es**), to which relevant information security incidents and systems that affect public organizations and companies are reported.
- INCIBE-CERT (**https://incibe-cert.es**), to which relevant information security incidents and systems that affect citizens, organizations and companies in the private sector are reported.
- ESPDEF-CERT (**https://emad.defensa.gob.es/unidades/mcce/**), to which relevant security incidents that could affect the field of national defense are reported.

Additionally, for those cases in which the incident has put at risk or caused the leak of personal data protected by the European General Data Protection Regulation (RGPD) and the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD) that regulates the processing of personal data in Spain, the necessary procedures will be carried out with the Spanish Data Protection Agency, AEPD. (**https://www.aepd.es/es**),

Furthermore, it is considered essential to establish formal cooperative relations with other CSIRTs. At the time of writing this document, it is being initiated the process to become part of the CSIRT.es community (**https://csirt.es/**) at the national level, and with the Trusted Introducer community (**https://www.trusted-introducer.org**) at the European level.

To facilitate the cooperation, distribution and exchange of information with clients, organizations or other CSIRTs, the FIRST TLP protocol (**https://www.first.org/tlp**) will be used to label the information..

The ACD-TRC undertakes not to share information with other parties without prior agreement and authorization from the owner of the same, except in cases where there is a higher legal or regulatory obligation that requires sharing such information..

As additional measures, in addition to the above, the ACD-TRC undertakes to:

- Apply at all times appropriate technical and legal measures to protect information.
- Anonymize the shared information as much as possible and within it select only relevant data for the resolution of incidents.
- Protect the privacy of personal information and always within the assumptions included in the European and Spanish regulations for the protection of personal data.
- Stop the distribution of information at the moment the owner of the information notifies the denial of permission to do so (except in cases where there is a higher legal or regulatory obligation that requires sharing said information).

5.3 Communication and Authentication

Considering the type of information that the TRC Group CSIRT is likely to process, the phones will be considered sufficiently secure for use, even if they are not encrypted. Unencrypted email will not be considered particularly secure but will be sufficient for the transmission of low-sensitivity data. If highly sensitive data needs to be sent via email, PGP will be used. Network file transfers will be considered similar to email for these purposes: sensitive data must be encrypted for transmission.

When it is necessary to establish a certain degree of trust, and always before revealing confidential information, the identity of the other party will be verified. Within the community and with known neighboring sites, references from known and trusted people will be enough to identify someone. Otherwise, appropriate methods such as a search for FIRST members, use of WHOIS and other Internet registration information, etc., along with telephone calls or emails, will be used to ensure that the other party is not a imposter Incoming emails whose data must be trusted are verified personally with the sender or using digital signatures (in particular, PGP is supported).

6. Services.

6.1 Incident response.

ACD-TRC will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

6.1.1 Incident Triage.

Incident triage activities include:

- Report assessment - Interpretation of incoming incident reports, their prioritization and relation to ongoing incidents and trends.
- Verification - Support in determining whether an incident has really occurred and its scope.

6.1.2 Incident Coordination

Incident coordination activities include:

- Information categorization - Categorization of incident related information (logfiles, contact information, etc.) with respect to the information disclosure policy.
- Coordination - Notification of involved parties on a need-to-know basis, as per the information disclosure policy.

6.1.3 Incident Resolution

Incident resolution activities include:

- Technical Assistance - This may include analysis of compromised systems.
- Eradication - Elimination of the cause of a security incident and its effects.
- Recovery - Support in restoring affected systems and services to their status before the security incident.

In addition, ACD-TRC will collect statistics concerning incidents that occur within or involve the community and will notify the community as necessary to assist it in protecting against known attacks.

6.2 Proactive activities.

ACD-TRC will take part in proactive services with the objective to reduce the number of actual incidents by providing proper and suitable information concerning potential incidents to the constituency. Grupo Banco Sabadell CERT will perform proactive activities to improve performance and capabilities, such as:

- Information services.
- Training and simulation activities.
- Forensics and malware analysis.
- Cyber Intelligence coordination and contextualization.
- Threat hunting.

7. Reporting incidents.

When a client detects a security event or incident, they will report it to the ACD-TRC through this email account: **csirt@grupotrc.com**.

Confidentiality measures will be those established with each client at the beginning of the service provision and must include the maximum information available, according to the following indications:

NOTIFY	DESCRIPTION
Subject	General description of the incident.
Descriptión	Detailed description of what happened.
Incident's date and time	Indicate as precisely as possible when the incident occurred
Detection's date and time	Indicate as precisely as possible when the incident was detected
Taxonomy classification of the incident	Possible classification of the incident based on the described taxonomy. This classification is determined in the ACD-TRC Security Incident Management Procedure and will be delivered to each client through the way stipulated with each of them at the beginning of the service provision.
Incident Impact Categorization	Estimated impact on the entity, depending on the level of impact of the incident. This categorization is determined in the ACD-TRC Security Incident Management Procedure, and will be delivered to each client through the way stipulated with each of them at the beginning of the service provision.
Affected resources	Indicate technical information on the number and type of assets affected for the incident, including all possible information including the following: ▪ Number of computers, servers or devices affected ▪ Device name and IP ▪ Team function ▪ Time zone ▪ Hardware ▪ Operating system ▪ Affected software ▪ Affected files ▪ Security settings ▪ Protocol/port
Origin of the incident	Indicate the cause of the incident if known, for example, opening of a suspicious file, connection of a USB device, access to a malicious website, etc.
Attachments	Include attached documents that can provide information that helps to know the cause of the problem or its resolution (screenshots, information log files, emails, etc.).

Madrid, a 5 de enero de 2024

Fdo: ALFREDO ESTIRADO BRONCHALO
CONSEJERO DELEGADO GRUPO TRC

Grupo TRC.
c/ Albasanz 25. 28037. Madrid
www.grupotrc.com
CONTACTO:
Mail: grupotrc@grupotrc.com
Tlf: 91 267 00 00