Business IT Computer Security Incident Response Expectations

CSIRT – BUSINESS IT

RFC 2350

expertos@grupobusiness.it
www.GrupoBusiness.it

INDEX

INDEX 2
1. Document information 4
1.1. Last Update Date 4
1.2. Notification distribution list 4
1.3. Locations where this document can be found 4
2. Contact information 4
2.1. Team name 4
2.2. Address 4
2.3. Time zone 4
2.4. Phone number 4
2.5. Email address 4
2.6. Public keys and other encryption information 5
2.7. Team Members 5
2.8. Customer Contact Points 5
3. Letter 5
3.1. Mission 5
3.2. Community served or constituency 6
3.3. Sponsorship and/or affiliation 6
3.4. Authority 6
4. Policies 7
4.1. Incident types and support level 7
4.2. Cooperation, interaction and dissemination of information 7
4.3. Communication and authentication 8
5. Services 8
5.1. Reactive Services 8
5.1.1. Incident Classification 9
5.1.2. Incident Coordination 9
5.1.3. Incident Resolution 9
5.2. Proactive Services 10
5.2.1. Notices and alerts 10
5.2.2. Vulnerability Analysis 10
5.2.3. Security assessment (benchmarks and computer hardening) 10
5.2.4. Training and awareness 11

5.2.5. Sending newsletters, announcements or announcements 11

5.2.6. Information services 11

6. Incident reporting form 11

7. Disclaimers 11

CSIRT – BUSINESS IT

RFC 2350

1. Document Information

1.1. Last Update Date

February 24, 2025.

1.2. Notification distribution list

There is no e-mail distribution channel for notification of changes to this document. Changes are announced by means of notifications at: www.grupobusiness.it/csirt

For any questions or comments, please contact the following email address: csirt-latam@grupobusiness.it

1.3. Locations where this document can be found.

The latest version of this document is published in:

Language	Document URL
SPANISH	https://standprocesos.blob.core.windows.net/csirt/BIT-D-MS-02%20EXPECTATIVAS%20CSIRT%20-%20ESP.pdf
ENGLISH	https://standprocesos.blob.core.windows.net/csirt/BIT-D-MS-02%20EXPECTATIVAS%20CSIRT%20-%20ING.pdf

2. Contact information.

2.1. Team name

"CSIRT – BUSINESS IT": BUSINESS IT Computer Security Incident Response Team.

2.2. Address

Julio Alarcón Ayala S/N between Japan and Pereira, Zaigen Building, 9th Floor. Quito, Ecuador.

2.3. Time zone

UTC-5 Quito/Ecuador.

2.4. Phone number

+593 (02) 6002741, ask by CSIRT-BUSINESS IT

2.5. Email address

Exchange of information related to incidents: csirt-latam@grupobusiness.it .
Other email addresses to contact CSIRT-BUSINESS IT

2.6. Public keys and other encryption information

PGP is used for functional information exchanges between CSIRT-BUSINESS IT and other teams or stakeholders (incident reports, alerts, etc.)

2.7. Team members

The full list of CSIRT-BUSINES IT team members is not publicly available. Team members will identify themselves with the reporting party or customer by their full name in an official communication about an incident.
CSIRT-BUSINESS IT management, liaison and supervision are the responsibility of the Cyber Security Manager and the Incident Responder & Forensic.

2.8. Customer touchpoints

The preferred method of communicating with CSIRT-BUSINESS IT is via email messages to the address csirt-latam@grupobusiness.it .
An email sent to this address will be communicated to the responsible party, or automatically forwarded to the appropriate support person, immediately. If you require urgent assistance, please write "urgent" in the subject line.
If it is not possible (or not advisable for security reasons) to use email
Email: CSIRT-BUSINESS IT can be contacted by phone during regular business hours. Phone messages are checked less frequently than email.
CSIRT-BUSINESS IT's operating hours are generally restricted to normal business hours (Monday to Friday 08:30 to 18:00, excluding holidays).
In the event of a critical incident, the operation could be in a 24x7 format.

3. Letter

3.1. Mission

BUSINESS IT considers digital information as an essential asset that must be protected and monitored in a timely manner due to the rapid evolution of cyber threats to ensure the business continuity of organizations. Cyberattacks often compromise personal and business data, so it is crucial to respond quickly and effectively to security breaches.

In this context, the CSIRT-BUSINESS IT has the mission of supporting the organizations in the community served by BUSINESS IT. This includes coordination to follow the incident response plan in all its phases.

3.2. Community served or constituency

The jurisdiction of CSIRT-BUSINESS IT is comprised of internal and external clients of BUSINESS IT, with whom a service agreement has been signed or formalized that BUSINESS IT provides as a Response to Computer Security Incidents. The incidents handled by CSIRT-BUSINESS IT will be those that affect the networks, systems and applications of internal and external clients of BUSINESS IT in accordance with the services provided by CSIRT, specified in section 5 entitled “Services” of this document.
However, it should be noted that, without prejudice to the foregoing, the services of CSIRT-BUSINESS IT will provide support for systems in BUSINESS IT data processing centers and other locations of BUSINESS IT's internal and external clients that are within the scope of the services provided, such as cloud infrastructure. CSIRT-BUSINESS IT can act, provided that secure remote access to the infrastructure where the incident occurred is provided.

3.3. Sponsorship and/or affiliation

Infrastructure & Managed Business Unit BUSINESS IT Services .
CSIRT-BUSINESS IT seeks to be affiliated with institutions around the world in order to collaborate and share information on computer security incidents.
CSIRT-BUSINESS IT is made up as follows:

- Infrastructure & Managed Business Unit BUSINESS IT Services , run by CSIRT-BUSINESS IT.
- The CSIRT-BUSINESS IT Leader , in charge of BUSINESS IT Incident Responder & Forensic.
- Cybersecurity Analysts and Specialists.

3.4. Authority

CSIRT-BUSINESS IT operates under the auspices and with the authority delegated by the Infrastructure & Managed Business Unit BUSINESS IT Services .
CSIRT-BUSINESS IT CSIRT-BUSINESS IT works in cooperation with the other areas of BUSINESS IT, as well as with internal and external clients. Authoritarian relationships are avoided as far as possible. However, if circumstances warrant it, CSIRT-BUSINESS IT will call upon the Delivery Manager and the Chief Business Officer to exercise their powers, directly or indirectly, as necessary.
Members of the BUSINESS IT community who wish to appeal the actions of CSIRT-BUSINESS IT should contact the Cyber Security Manager. If this resource is not satisfactory, the matter can be referred to the Delivery Manager of the Infrastructure & Managed Business Unit Services of BUSINESS IT.

4. Policies

CSIRT-BUSINESS IT will define its policies and procedures for the operation and management of incidents throughout their life cycle. However, as set out in RFC 2350, the following is described:

4.1. Incident types and support level

CSIRT-BUSINESS IT is authorized to respond to any type of computer security incident that occurs in its community or district and that is part of the services it provides.

CSIRT-BUSINESS IT may act at the request of stakeholders in its served community or constituency or may act if one of its constituents is involved in a computer security incident. Please note that direct support will not be provided to end users; end users are expected to contact their system administrator, network administrator, project manager, IT department head, information security officer or similar position for assistance, CSIRT-BUSINESS IT will support the latter people.

The level of support provided by CSIRT-BUSINESS IT will vary depending on the type and severity of the incident or issue, the type of stakeholder in your served community or constituency, the size of the affected user community, and the resources available to CSIRT-BUSINESS IT to manage the incident at that time, although in all cases a response will be made within one business day.

CSIRT-BUSINESS IT handles different types of incidents classified according to their level of

criticality and prioritization of care based on an impact and urgency matrix,

the level of support from CSIRT-BUSINESS IT It will depend on both factors and the severity determined by the team staff, in accordance with the CSIRT-BUSINESS IT Incident Management Policy.

While CSIRT-BUSINESS IT understands that there is a wide variation in the level of experience of the BUSINESS IT system administrator and/or the system administrator in your served community or constituency, and although CSIRT-BUSINESS IT will endeavor to present information and assistance at a level appropriate to each individual, CSIRT-BUSINESS IT cannot train system administrators on the fly and cannot perform system maintenance on your behalf. In most cases, CSIRT-BUSINESS IT will provide guidance and recommendations on the information needed to implement appropriate measures.

5. Cooperation, interaction and dissemination of information

CSIRT-BUSINESS IT will cooperate and interact with other organizations in the field of information security, cybersecurity and personal data protection focused on issues related to the response to security incidents, especially with other IRTs (Incident Response Teams), SIRTs (Security Incident Response Teams), CIRCs (Computer Incident Response Centers), CSIRTs (Computer Security Incident Response Teams), CERTs

(Computer Emergency Response Teams), PSIRTs (Product Security Incident Response Teams), NCSCs (National Cyber Security Centers)
or ISACs (Information Sharing and Analysis Centers). This cooperation also includes and often requires the exchange of information about security incidents and vulnerabilities. However, CSIRT-BUSINESS IT will protect the privacy of data subjects in its served community or constituency and will therefore (under normal circumstances) transmit information only in an anonymous form. Unless expressly authorized, the identity or vital information of victims of computer security incidents will not be disclosed.
CSIRT-BUSINESS IT operates within the Ecuadorian legal framework, therefore, CSIRT-BUSINESS IT may be forced to reveal certain information to comply with a legal obligation or an express court order, which would have to be provided in coordination and after analysis with the legal department of BUSINESS IT.
CSIRT-BUSINESS IT handles various types of information, information of a very sensitive nature (restricted, confidential, secret or strictly secret) is only communicated and stored in a secure environment and, if necessary, uses cryptographic mechanisms. All information supplied and provided by CSIRT-BUSINESS IT will be used to help resolve security incidents.
Cooperation, interaction and disclosure of information is carried out in accordance with the CSIRT-BUSINESS IT Information Transfer Policy and Information Classification Policy.
CSIRT-BUSINESS IT It uses the TLP protocol for the exchange of information, as well as secure communication mechanisms through the use of cryptographic controls.

5.1. Communication and authentication

Communication via unencrypted email messages will not be considered secure, however, it is sufficient for the transmission of low-sensitivity data or non-sensitive data. Please note that sensitive data that constitutes information of a highly sensitive nature (restricted, confidential, secret or top secret) must be encrypted before transmission, which includes file transfers.
CSIRT-BUSINESS IT will use end-to-end PGP encrypted email whenever possible. Authentication is provided via PGP signatures using the keys mentioned above.

6. Services

CSIRT-BUSINESS IT will assist its served community or constituency in managing the technical and organisational aspects of incidents. In particular, you will provide assistance or advice regarding the following aspects of incident management in reactive and proactive services:

6.1. Reactive services

These services are activated as a result of an incident, which is the CSIRT-BUSINESS IT's work to manage incidents in its served community or constituency:

6.1.1. Classification of incidents

CSIRT-BUSINESS IT classifies incidents according to their level of criticality and the prioritization of attention is based on an impact and urgency matrix. In addition, an investigation is carried out to conclude whether an incident actually occurred, determine its scope, and evaluate and compare the incident with historical information.

6.1.2. Incident coordination

This service aims to coordinate the response to computer security incidents with other teams at local, regional and global levels, Internet service providers, telecommunications companies and other public and private organizations (law enforcement and legal), as appropriate. Coordination is carried out in close relationship with the affected parties. Part of the objective is to determine the root cause of the incident and which vulnerability was exploited, for which contacts are made with sites that may be involved in the incident.

Also, if applicable, coordination is carried out with the media through the guidelines described in the “Crisis Communication Manual”, which belongs to the Marketing Department of BUSINESS IT.

In addition, where applicable, the preparation of announcements for interested party end users should be managed.

6.1.3. Incident Resolution

This service aims to manage an incident through the incident response process that involves the phases of preparation; detection and analysis; containment, eradication and recovery; and activities after an incident has occurred.

CSIRT-BUSINESS IT will provide technical assistance by analyzing compromised systems, making recommendations for eradicating and eliminating the cause of the incident, and securing the affected systems.

CSIRT-BUSINESS IT will also collect statistics on incidents that occur within its served community or constituency, or in which it is otherwise involved, and will notify the community as necessary to protect against known attacks.

Please note that CSIRT-BUSINESS IT is tasked with coordinating incident response with information partly provided by the community served or constituency, without coercion. In that sense, it is likely that a successful resolution of all incidents will not always be possible, since the actual resolution depends on the correct actions taken and executed by the interested party.

6.2. Proactive services

These services are intended to provide timely information to help protect the network infrastructure of the community served or constituency in anticipation of cyber-attacks. Therefore, successful or timely implementation of the services will reduce the number of future incidents.

CSIRT-BUSINESS IT coordinates and maintains the following services to the extent possible within its resources:

6.2.1. Notices and alerts

This service aims to proactively alert and warn about cyber attacks or interruptions, security vulnerabilities, intrusion alerts, malware , viruses
computer scientists, anomalous behaviors and provide recommendations to address the problem to the interested party in their served community or constituency. This is done through:

- Correlation of events,
- Monitoring,
- Advanced analytics and automated investigations and responses,
- Use of artificial intelligence,
- Respond smarter and faster

6.2.2. Vulnerability analysis

Vulnerability scanning is the process of identifying systems on the network that have known or identified vulnerabilities, such as flaws, security breaches, exploits , insecure access entry points, and system configuration errors.

It corresponds to the evaluation of vulnerabilities of the network infrastructure, equipment,
software, applications, and other network devices for the purpose of providing recommendations for timely remediation.

7. Security assessment (benchmarks and computer hardening)

" Hardening " or computer hardening is a series of techniques, tools and best practices to reduce vulnerabilities in technological systems, whose objective is to reduce security risks by eliminating possible attack vectors and the
materialization of the attack surface on some system.

The service corresponds to the assessment of configurations that allows the security status of information systems and the effectiveness of controls to be analyzed and monitored. The service is provided through access to a set of cybersecurity resources and tools to implement critical security controls, which includes a priority set of good practices in cybersecurity, as well as defensive actions that can help prevent the most dangerous and high-impact cyberattacks; and in this sense, support compliance with

a series of multiple information security and cybersecurity frameworks. The security assessment corresponds to configuration baselines and best practices for configuring a system securely. Each of the guidance recommendations refers to one or more international good practice controls that were developed to help organizations improve their cyber defense capabilities.

7.1.1. Training and awareness

CSIRT-BUSINESS IT members will give seminars, talks and courses periodically or upon request according to available resources, on topics related to computer security; these seminars, talks and courses will be open to clients, administrators of the systems managed by BUSINESS IT or may also be a public event according to timely communication.

8. Sending newsletters, announcements or announcements

This service aims to provide information on the threat landscape, published vulnerabilities, ongoing attacks, indicators of compromise, new tools, attack techniques or attack artifacts, security and protection measures, among others, to send general alerts and the recommended course of action, which are necessary to protect the systems and networks of your served community or constituency.

8.1.1. Information services

These services include:

- List of departmental security, administrative and technical contacts. These lists will be made available through commonly available channels.
- Mailing lists to inform security contacts about new information relevant to their computing environments. These lists will be available only to customers and the administrators of the systems operated by BUSINESS IT.
- Pre-compiled and ready-to-install versions will be provided whenever possible .

9. Incident reporting form

To report incidents, please send an email to csirt-latam@grupobusiness.it . As of the date of this document, forms for reporting incidents to CSIRT-BUSINESS IT have not yet been developed.

10. Disclaimers

While CSIRT-BUSINESS IT will take every precaution in preparing information, notifications and alerts, CSIRT-BUSINESS IT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained therein.