



a Prosegur company

CIPHER-CSIRT / RFC2350

CONTROL PAGE

SECURITY CLASSIFICATION	TLP-WHITE
--------------------------------	-----------

Title:	CIPHER-CSIRT / RFC2350
Reference:	CIPHER-CSIRT_RFC2350_EN_V3.0

VERSION CONTROL		
Version	Revision date	Change description
1.0	10/12/2019	Document creation - Certified team
2.0	05/05/2022	Team name changed with all the changes that come with it. In addition, the Constituency
2.1	12/05/2022	Small changes included
3.0	19/12/2025	Full revision of the document including the Constituency

INDEX OF CONTENTS

1	INTRODUCTION	4
	1.1 Abstract.....	4
	1.2 Locations where this document can be found	4
2	CONTACT INFORMATION	5
	2.1 Name of the Team.....	5
	2.2 Address.....	5
	2.3 Time Zone	5
	2.4 Telephone Number	5
	2.5 Electronic Mail Address	5
	2.6 Public Keys and Other Encryption Information	5
	2.7 Team Members.....	6
	2.8 Other Information	6
	2.9 Points of Customer Contact.....	6
3	CHARTER	7
	3.1 Mission Statement	7
	3.2 Constituency	7
	3.3 Authority.....	20
4	POLICIES	21
	4.1 Types of Incidents and Level of Support.....	21
	4.1.1 Incident Classes Supported.....	21
	4.1.2 Level of Support Provided.....	22
	4.1.3 Response Time	22
	4.1.4 Exclusions / Special Handling.....	22
	4.2 Co-operation, Interaction and Disclosure of Information.....	22
	4.3 Communication and Authentication.....	23
5	SERVICES	24
	5.1 Incident Response	24
	5.2 Incident Triage	24
	5.3 Incident Coordination.....	24
	5.4 Incident Resolution	25
	5.5 Post-Incident Activities.....	25
	5.6 Proactive Activities	25
6	DISCLAIMER	26

1 INTRODUCTION

1.1 Abstract

This document describes the CIPHER-CSIRT, the Cipher CSIRT team, according to RFC 2350. The RFC 2350 is an RFC (Request for Comments) which describes the structure, the procedures and the policies of a CSIRT (Computer Security Incident Response Team). The RFC 2350 can be downloaded from <http://www.ietf.org/rfc/rfc2350.txt>.

1.2 Locations where this document can be found

The current version of this document is available from the CIPHER-CSIRT site:

<https://www.cipher.com/why-choose-cipher>

2 CONTACT INFORMATION

2.1 Name of the Team

CIPHER-CSIRT: the Cipher Computer Security Incident Response Team.

2.2 Address

CIPHER - CONSULTORIA EM SEGURANÇA DE INFORMAÇÃO, PORTUGAL, UNIPessoal LDA
Torre de Monsanto, Rua Afonso Praça, 30, 7º Piso
1495-061 Miraflores - Algés - Lisboa
Portugal

2.3 Time Zone

Portugal/WEST (GMT+0 and GMT+1 from April to October).

2.4 Telephone Number

+351 966 389 221

2.5 Electronic Mail Address

irt@cipher.com

2.6 Public Keys and Other Encryption Information

The CIPHER-CSIRT has a PGP key for secure communication.

CIPHER-CSIRT: irt@cipher.com

Fingerprint: 5BC9E9C4F9835585057E7C8B3DD1C76FDFC8914D

2.7 Team Members

(Ordered alphabetically)

Adail Domingues Da Silva De Oliveira - adoliveira@cipher.com

Andreia Nascimento Santos - asantos@cipher.com

Antonio Javier Montes - amontes@cipher.com

Antonio Xavier Ferreira Correia - axcorreia@cipher.com

Bryan Silvestre Matias - bmatias@cipher.com

Daniel António Sousinha - daniel.sousinha@cipher.com

Daniel Martins Mata - daniel.martins-mata@cipher.com

Henrique Pessôa Pessôa Leo - henrique.leo@cipher.com

Miguel De Almeida Martins Libânio - mlibanio@cipher.com

Teresa Leal Ferreira - teresa.leal@cipher.com

Tiago José Rodrigues Costa - Tiago.rodrigues@cipher.com

Yaser Rimawi - yaser.rimawi@prosegur.com

2.8 Other Information

Information regarding activities and structure of the CIPHER-CSIRT, as well as links to various recommended security resources can be found at <https://www.cipher.com/why-choose-cipher>

2.9 Points of Customer Contact

The preferred method for contacting CIPHER-CSIRT is via e-mail at irt@cipher.com. If it is not possible (or not advisable for security reasons) to use e-mail, the CIPHER-CSIRT can be reached by telephone at +351 966 389 221.

3 CHARTER

3.1 Mission Statement

The purpose of the CIPHER-CSIRT is to respond to security incidents in its own infrastructure as well as its client's infrastructure, assuring a high degree of availability and the business continuity of affected clients.

3.2 Constituency

The CIPHER-CSIRT constituency is its own infrastructure as well as the infrastructure of its clients. Currently, the following IP addresses are part of our constituency:

18.201.88.141/32	148.69.133.54/32	213.190.49.0/28
34.247.4.201/32	148.69.133.55/32	217.23.199.48/29
34.248.117.39/32	148.69.133.56/32	4.208.16.245/32
34.248.191.171/32	148.69.133.57/32	4.209.228.113/32
34.248.235.169/32	75.2.70.75/32	4.210.105.236/32
34.254.99.141/32	89.114.154.65/32	4.226.19.32/32
52.50.137.244/32	99.83.190.102/32	4.226.19.47/32
52.51.121.116/32	31.221.12.128/26	4.226.23.32/32
54.155.137.224/32	62.38.57.224/27	4.226.25.251/32
54.155.249.211/32	80.17.182.144/28	4.226.28.128/32
54.195.45.72/32	81.0.71.0/26	4.226.33.108/32
54.195.182.247/32	81.93.77.120/29	4.226.37.207/32
99.80.211.186/32	82.141.141.136/29	4.226.50.40/32
108.128.194.197/32	88.118.136.8/29	4.226.50.158/32
41.76.144.0/24	89.44.246.0/24	4.226.53.186/32
41.76.145.0/24	89.204.165.96/27	13.69.131.89/32
197.235.1.0/24	91.199.57.0/24	13.70.194.204/32
197.235.2.0/24	188.119.9.112/28	13.74.36.102/32
197.235.3.0/24	193.85.207.32/29	20.33.18.3/32
148.69.131.126/32	193.126.27.160/27	20.33.18.4/32
148.69.133.50/32	194.224.217.176/28	20.33.18.5/32
148.69.133.51/32	195.29.38.64/27	20.33.18.6/32
148.69.133.52/32	195.65.194.0/27	20.33.18.7/32
148.69.133.53/32		

20.54.61.111/32	104.18.34.21	134.213.245.209
20.54.101.37/32	118.189.76.30	134.213.245.210
20.67.174.86/32	122.169.102.178	134.213.245.211
20.93.60.0/32	123.231.140.40	135.237.1.136
20.107.130.154/32	123.231.140.41	149.72.221.27
20.107.147.189/32	123.231.140.42	15.236.235.169
20.166.37.211/32	123.231.140.43	152.156.125.88
20.166.222.109/32	123.231.140.44	152.156.125.89
20.199.146.86/32	123.231.140.45	152.156.125.90
20.250.160.99/32	123.231.140.46	152.156.125.91
20.250.169.164/32	123.231.140.47	152.156.125.92
20.250.184.12/32	129.126.146.100	152.156.125.93
20.250.199.255/32	129.126.146.82	152.156.125.94
20.250.203.70/32	129.126.146.83	152.156.125.95
40.67.248.173/32	129.126.146.84	162.159.140.147
40.67.251.242/32	129.126.146.85	162.159.200.1
40.67.254.76/32	129.126.146.86	167.114.41.88
40.67.254.77/32	129.126.146.87	170.239.102.80
40.67.254.82/32	129.126.146.88	170.239.102.81
40.127.188.244/32	129.126.146.89	170.239.102.82
51.138.235.175/32	129.126.146.90	170.239.102.83
52.137.25.50/32	129.126.146.91	170.239.102.84
52.155.163.65/32	129.126.146.92	170.239.102.85
65.52.147.251/32	129.126.146.93	170.239.102.86
74.161.75.174/32	129.126.146.94	170.239.102.87
74.161.104.202/32	129.126.146.95	170.239.102.88
74.161.114.62/32	129.126.146.96	170.239.102.89
74.242.193.77/32	129.126.146.97	170.239.102.90
74.242.214.243/32	129.126.146.98	170.239.102.91
135.236.225.254/32	129.126.146.99	170.239.102.92
137.116.234.109/32	13.107.246.10	170.239.102.93
172.161.140.17/32	13.36.10.213	170.239.102.94
172.161.161.30/32	13.89.115.88	170.239.102.95
172.162.241.62/32	132.220.46.58	177.99.224.216
172.205.122.139/32	134.159.162.241	177.99.224.217

177.99.224.218	181.44.57.84	189.125.227.83
177.99.224.219	181.93.66.10	189.125.227.84
177.99.224.220	185.224.145.68	189.125.227.85
177.99.224.221	185.51.192.61	189.125.227.86
177.99.224.222	186.139.165.7	189.125.227.87
177.99.224.223	186.154.153.100	189.125.227.88
18.203.36.176	186.154.153.101	189.125.227.89
18.223.66.100	186.154.153.102	189.125.227.90
18.230.162.139	186.154.153.103	189.125.227.91
181.13.231.112	186.154.153.96	189.125.227.92
181.13.231.113	186.154.153.97	189.125.227.93
181.13.231.114	186.154.153.98	189.125.227.94
181.13.231.115	186.154.153.99	189.125.227.95
181.13.231.116	186.16.40.133	189.17.176.192
181.13.231.117	186.182.52.115	189.17.176.193
181.13.231.118	186.29.78.94	189.17.176.194
181.13.231.119	189.125.227.64	189.17.176.195
181.13.246.48	189.125.227.65	189.17.176.196
181.13.246.49	189.125.227.66	189.17.176.197
181.13.246.50	189.125.227.67	189.17.176.198
181.13.246.51	189.125.227.68	189.17.176.199
181.13.246.52	189.125.227.69	189.17.176.200
181.13.246.53	189.125.227.70	189.17.176.201
181.13.246.54	189.125.227.71	189.17.176.202
181.13.246.55	189.125.227.72	189.17.176.203
181.164.146.90	189.125.227.73	189.17.176.204
181.212.39.40	189.125.227.74	189.17.176.205
181.212.39.41	189.125.227.75	189.17.176.206
181.212.39.42	189.125.227.76	189.17.176.207
181.212.39.43	189.125.227.77	189.17.30.100
181.212.39.44	189.125.227.78	189.17.30.101
181.212.39.45	189.125.227.79	189.17.30.102
181.212.39.46	189.125.227.80	189.17.30.103
181.212.39.47	189.125.227.81	189.17.30.104
181.29.95.105	189.125.227.82	189.17.30.105

189.17.30.106	189.43.18.110	190.0.151.105
189.17.30.107	189.43.18.111	190.0.151.106
189.17.30.108	189.43.18.96	190.0.151.107
189.17.30.109	189.43.18.97	190.0.151.108
189.17.30.110	189.43.18.98	190.0.151.109
189.17.30.111	189.43.18.99	190.0.151.110
189.17.30.96	189.53.131.240	190.0.151.111
189.17.30.97	189.53.131.241	190.0.151.112
189.17.30.98	189.53.131.242	190.0.151.113
189.17.30.99	189.53.131.243	190.0.151.114
189.2.182.208	189.53.131.244	190.0.151.115
189.2.182.209	189.53.131.245	190.0.151.116
189.2.182.210	189.53.131.246	190.0.151.117
189.2.182.211	189.53.131.247	190.0.151.118
189.2.182.212	189.53.131.248	190.0.151.120
189.2.182.213	189.53.131.249	190.0.151.121
189.2.182.214	189.53.131.250	190.0.151.122
189.2.182.215	189.53.131.251	190.0.151.98
189.2.182.216	189.53.131.252	190.0.151.99
189.2.182.218	189.53.131.253	190.196.58.62
189.2.182.219	189.53.131.254	190.2.31.200
189.2.182.220	189.53.131.255	190.2.31.201
189.2.182.221	189.59.15.240	190.2.31.202
189.2.182.222	189.59.15.241	190.2.31.203
189.2.182.223	189.59.15.242	190.2.31.204
189.43.18.100	189.59.15.243	190.2.31.205
189.43.18.101	189.59.15.244	190.2.31.206
189.43.18.102	189.59.15.245	190.2.31.207
189.43.18.103	189.59.15.246	190.2.47.249
189.43.18.104	189.59.15.247	190.2.47.254
189.43.18.105	190.0.151.100	190.2.47.255
189.43.18.106	190.0.151.101	190.210.24.28
189.43.18.107	190.0.151.102	190.210.24.29
189.43.18.108	190.0.151.103	190.210.24.30
189.43.18.109	190.0.151.104	190.210.24.31

190.210.6.168	190.221.41.144	190.93.136.101
190.210.6.169	190.221.41.145	190.93.136.102
190.210.6.170	190.221.41.146	190.93.136.103
190.210.6.171	190.221.41.147	190.93.136.16
190.210.6.172	190.221.41.148	190.93.136.17
190.210.6.173	190.221.41.149	190.93.136.18
190.210.6.174	190.221.41.150	190.93.136.19
190.210.6.175	190.221.41.151	190.93.136.20
190.216.207.144	190.221.41.152	190.93.136.21
190.216.207.145	190.221.41.153	190.93.136.22
190.216.207.146	190.221.41.154	190.93.136.23
190.216.207.147	190.221.41.155	190.93.136.96
190.216.207.148	190.221.41.156	190.93.136.97
190.216.207.149	190.221.41.157	190.93.136.98
190.216.207.150	190.221.41.158	190.93.136.99
190.216.207.151	190.221.41.159	190.93.138.184
190.216.208.194	190.25.224.100	190.93.138.185
190.216.222.139	190.25.224.101	190.93.138.186
190.217.20.223	190.25.224.102	190.93.138.187
190.220.8.120	190.25.224.103	190.93.138.188
190.220.8.121	190.25.224.96	190.93.138.189
190.220.8.122	190.25.224.97	190.93.138.190
190.220.8.123	190.25.224.98	190.93.138.191
190.220.8.124	190.25.224.99	193.114.143.178
190.220.8.125	190.27.213.112	194.179.36.210
190.220.8.126	190.27.213.113	194.224.37.40
190.220.8.127	190.27.213.114	194.224.37.41
190.221.167.0	190.27.213.115	194.224.37.42
190.221.167.1	190.27.213.116	194.224.37.43
190.221.167.2	190.27.213.117	194.224.37.44
190.221.167.3	190.27.213.118	194.224.37.45
190.221.167.4	190.27.213.119	194.224.37.46
190.221.167.5	190.64.10.98	194.224.37.47
190.221.167.6	190.64.9.29	195.53.155.185
190.221.167.7	190.93.136.100	195.53.155.225

195.53.155.228	200.127.158.200	200.208.2.58
195.53.155.94	200.127.158.201	200.208.2.59
195.53.179.153	200.127.158.202	200.208.2.60
195.53.179.77	200.127.158.203	200.208.2.61
195.76.190.173	200.127.158.204	200.208.2.62
195.76.190.174	200.127.158.205	200.208.2.63
195.76.207.40	200.127.158.206	200.228.42.112
195.76.207.41	200.127.158.207	200.228.42.113
195.76.207.42	200.179.209.176	200.228.42.114
195.76.207.43	200.179.209.177	200.228.42.115
195.76.207.44	200.179.209.178	200.228.42.116
195.76.207.45	200.179.209.179	200.228.42.117
195.76.207.46	200.179.209.180	200.228.42.118
195.76.207.47	200.179.209.181	200.228.42.119
195.77.80.176	200.179.209.182	200.228.42.120
195.77.80.177	200.179.209.183	200.228.42.121
195.77.80.178	200.179.209.184	200.228.42.122
195.77.80.179	200.179.209.185	200.228.42.123
195.77.80.180	200.179.209.186	200.228.42.124
195.77.80.181	200.179.209.187	200.228.42.125
195.77.80.182	200.179.209.188	200.228.42.126
195.77.80.183	200.179.209.189	200.228.42.127
20.126.190.228	200.179.209.190	200.242.94.192
20.190.159.2	200.179.209.191	200.242.94.193
20.190.159.23	200.186.76.98	200.242.94.194
20.190.159.4	200.208.2.48	200.242.94.195
20.190.159.64	200.208.2.49	200.242.94.196
20.190.159.71	200.208.2.50	200.242.94.197
20.190.159.73	200.208.2.51	200.242.94.198
20.190.160.14	200.208.2.52	200.242.94.199
20.190.160.17	200.208.2.53	200.242.94.200
20.190.160.20	200.208.2.54	200.242.94.201
20.190.160.22	200.208.2.55	200.242.94.202
20.246.169.217	200.208.2.56	200.242.94.203
20.51.241.236	200.208.2.57	200.242.94.204

200.242.94.205	200.58.151.111	200.80.131.220
200.242.94.206	200.58.151.112	200.80.131.221
200.242.94.207	200.58.151.113	200.80.131.222
200.27.167.225	200.58.151.114	200.80.131.223
200.27.167.229	200.58.151.115	200.80.157.97
200.27.241.169	200.58.151.116	201.245.162.104
200.27.241.171	200.58.151.117	201.245.162.105
200.27.241.172	200.58.151.118	201.245.162.106
200.58.130.232	200.58.151.119	201.245.162.107
200.58.130.233	200.58.151.120	201.245.162.108
200.58.130.234	200.58.151.121	201.245.162.109
200.58.130.235	200.58.151.122	201.245.162.110
200.58.130.236	200.58.151.123	201.245.162.111
200.58.130.237	200.58.151.124	201.245.162.129
200.58.130.238	200.58.151.125	201.245.195.40
200.58.130.239	200.58.151.126	201.245.195.41
200.58.145.144	200.58.151.127	201.245.195.42
200.58.145.145	200.58.151.96	201.245.195.43
200.58.145.146	200.58.151.97	201.245.195.44
200.58.145.147	200.58.151.98	201.245.195.45
200.58.145.148	200.58.151.99	201.245.195.46
200.58.145.149	200.61.44.113	201.245.195.47
200.58.145.150	200.69.231.20	201.71.137.215
200.58.145.151	200.69.231.21	201.72.97.48
200.58.151.100	200.69.231.22	201.72.97.49
200.58.151.101	200.69.231.23	201.72.97.50
200.58.151.102	200.70.31.154	201.72.97.51
200.58.151.103	200.71.27.164	201.72.97.52
200.58.151.104	200.71.27.165	201.72.97.53
200.58.151.105	200.71.27.167	201.72.97.54
200.58.151.106	200.71.27.168	201.72.97.55
200.58.151.107	200.80.131.216	201.72.97.56
200.58.151.108	200.80.131.217	201.72.97.57
200.58.151.109	200.80.131.218	201.72.97.58
200.58.151.110	200.80.131.219	201.72.97.59

201.72.97.60	201.90.134.191	3.130.163.101
201.72.97.61	202.70.141.11	3.131.252.174
201.72.97.62	202.70.141.250	3.20.12.119
201.72.97.63	202.70.141.61	3.65.108.100
201.90.110.144	202.70.141.62	34.107.206.154
201.90.110.145	203.126.170.128	34.202.141.112
201.90.110.146	203.126.170.129	34.241.203.71
201.90.110.147	203.126.170.130	4.147.141.25
201.90.110.148	203.126.170.131	4.175.86.138
201.90.110.149	203.126.170.132	40.118.224.16
201.90.110.150	203.126.170.133	40.126.31.69
201.90.110.151	203.126.170.134	40.126.31.71
201.90.110.152	203.126.170.135	40.126.32.133
201.90.110.153	203.126.170.136	40.126.32.134
201.90.110.154	203.126.170.137	40.126.32.136
201.90.110.155	203.126.170.138	40.126.32.138
201.90.110.156	203.126.170.139	40.126.32.140
201.90.110.157	203.126.170.140	40.126.32.68
201.90.110.158	203.126.170.141	40.126.32.72
201.90.110.159	203.126.170.142	40.126.32.74
201.90.134.176	203.126.170.143	40.126.32.76
201.90.134.177	207.5.68.122	45.11.106.190
201.90.134.178	207.5.69.68	45.43.248.99
201.90.134.179	212.4.112.32	45.43.249.158
201.90.134.180	212.4.112.34	5.7.240.240
201.90.134.181	212.4.112.35	5.7.240.241
201.90.134.182	212.4.112.36	5.7.240.242
201.90.134.183	212.4.112.37	5.7.240.243
201.90.134.184	212.4.112.38	5.7.240.244
201.90.134.185	212.4.112.39	5.7.240.245
201.90.134.186	216.177.216.178	5.7.240.246
201.90.134.187	216.40.47.201	5.7.240.247
201.90.134.188	216.40.47.202	51.105.228.104
201.90.134.189	23.216.149.140	51.105.235.252
201.90.134.190	3.120.73.105	51.124.12.35

52.15.213.185	62.197.44.173	75.2.85.37
52.16.80.176	62.197.44.174	77.226.140.104
52.165.237.15	62.197.44.176	77.226.140.105
52.173.249.137	62.54.192.196	77.226.140.106
52.182.219.10	62.54.193.98	77.226.140.107
52.215.57.184	62.54.201.2	77.226.140.108
52.31.169.225	62.54.235.90	77.226.140.109
52.4.240.2	62.54.236.34	77.226.140.110
52.43.103.218	62.54.98.48	77.226.140.111
54.207.113.4	62.54.98.49	77.226.140.120
54.207.72.64	62.54.98.50	77.226.140.121
54.220.170.182	62.54.98.51	77.226.140.122
54.75.150.36	62.54.98.52	77.226.140.123
54.94.3.205	62.54.98.53	77.226.140.124
58.185.37.192	62.54.98.54	77.226.140.125
58.185.37.193	62.54.98.55	77.226.140.126
58.185.37.194	62.82.137.184	77.226.140.127
58.185.37.195	62.82.137.185	77.228.139.72
58.185.37.196	62.82.137.186	77.228.139.73
58.185.37.197	62.82.137.187	77.228.139.74
58.185.37.198	62.82.137.188	77.228.139.75
58.185.37.199	62.82.137.189	77.228.139.76
58.185.37.200	62.82.137.190	77.228.139.77
58.185.37.201	62.82.137.191	77.228.139.78
58.185.37.202	62.97.122.81	77.228.139.79
58.185.37.203	64.63.136.180	77.228.139.88
58.185.37.204	64.98.148.137	77.228.139.89
58.185.37.205	64.98.148.138	77.228.139.90
58.185.37.206	64.98.148.139	77.228.139.91
58.185.37.207	66.19.24.93	77.228.139.92
62.197.40.211	67.127.41.111	77.228.139.93
62.197.44.161	67.127.41.115	77.228.139.94
62.197.44.165	69.192.139.212	77.228.139.95
62.197.44.170	69.192.139.219	77.229.153.61
62.197.44.172	75.2.6.34	77.229.153.62

77.229.153.63	77.231.105.152	85.13.237.2
77.231.105.144	77.231.105.153	85.13.237.3
77.231.105.145	77.231.105.154	93.189.38.67
77.231.105.146	77.231.105.155	99.83.188.20
77.231.105.147	77.231.105.156	
77.231.105.148	77.231.105.157	
77.231.105.149	77.231.105.158	
77.231.105.150	77.231.105.159	
77.231.105.151	77.231.150.18	

Currently, the following domains are part of our constituency:

alarmasgprs1.cl	climax.proseguralarmas.com	mysegurpro.com.br
alarmasgprs2.cl	m	nossobalcao.com
amaseguros.com	commandsecurity.com	pagafacil.com.co
amigosmovistarproseguralarmas.com	compliofficer.com	piecitoscolorados.com
amigosmovistarproseguralarmas.es	connectyoursecurity.com	pitco.lu
amigosprosegur.pt	contesta.es	precinct.com.au
amlcheck.es	corbanpro.com.br	pro.connectyoursecurity.com
as-asoc.cl	costudioprosegur.com	m
atpi.com.ph	crmpa-latam.com	pro.amlcheck.es
avos-tech.com	crmpa-online.com	prosegur-alarmas.cl
azurewebsites.net	cysnet.net	prosegur-brasil.com.br
beaglewatch.co.za	erfcheck.com	prosegur-focal.com.sg
blob.core.windows.net	facilito.com.ec	prosegur-focal.sg
bondalti.com	fundacionprosegur.com	prosegur.cl
bondaltewater.com	genasys.com	prosegur.cn
cashservices.com.au	gif.t2v.cloud	prosegur.co.id
changegroup.at	grabandgobank.com	prosegur.co.uk
changegroup.co.uk	grupoprosegur.cn	prosegur.co.za
changegroup.com	grupoprosegur.com.mx	prosegur.com
changegroup.com.au	grupoproval.net	prosegur.com.ar
changegroup.es	imxclient.com	prosegur.com.au
changegroup.fi	int-prosegur.com	prosegur.com.bo
changegroup.fr	integrasecurity.com.co	prosegur.com.br
changegroup.se	leadalia.com	prosegur.com.co
changegroup.uk	lira.com.sg	prosegur.com.ec
cipher.com	lifthiumenergy.com	prosegur.com.pe
cipherxmdr.io	m1net.com.sg	prosegur.com.ph
cloud.t2v.com	meubalcao.com	prosegur.com.py
clubdeempleadoprosegur.com	midinero.com.uy	prosegur.com.sg
	miprosegur.com	prosegur.com.tr
	myproseguralarm.pe	prosegur.com.uy
	myprosegur.de	prosegur.cr

prosegur.de	prosegurclouditrack.com	qido.com.uy
prosegur.dev	prosegurcostudio.com	qido.pe
prosegur.dk	prosegurcrypto.ar	qido.pt
prosegur.ec	prosegurcrypto.com	qidoalarmas.com
prosegur.es	prosegurcrypto.com.ar	qidoalarms.com
prosegur.eu	prosegurdigitalgold.com	redireccionessueltas.com
prosegur.gt	prosegureuropa.com	redpagos.com.uy
prosegur.hn	prosegurformacaoadistanci a.pt	riskms.es
prosegur.info	proseguritrack.com	securitymanagement.com.s g
prosegur.io	prosegurlatinoamerica.com	securitymanagement.sg
prosegur.lv	proseguronline.com.br	seguridadprosegur.com
prosegur.net	prosegurpay.web.app	segurpro.com
prosegur.ni	prosegurproview.com	segurpro.com.br
prosegur.pt	prosegurquiereverte.es	segurpro.net
prosegur.sv	prosegurresearch.com	segurproseguranca.com.br
prosegur.us	prosegurresearch.es	segursign.com
proseguractiva.cl	prosegursecurityenergy.co m	sendity.com
proseguractiva.com	prosegurservicios.com	sendity.fr
proseguractiva.com.uy	prosegursmartcash.com	sisnet360.com
proseguractiva.es	prosegursmartcash.es	sisprosegur.com
proseguralarmas.com	prosegurvideo.com	solu4b.com
proseguralarmas.com.pt	prosegurvigilancia.com	solunegocios.com
proseguralarmas.es	prosegurvmm.com	solungeocios.com
proseguralarmes.pt	proservicios.pe	solupersonal.cl
proseguralarms.com	prosec.com.sg	soluservicios.cl
proseguralarms.net	prosec.tstudio.tech	tecnoservicebrasil.com
proseguravos.com	qido.cl	tevcoll.com.ec
prosegurcash.com	qido.co	thecashleague.com
prosegurcash.id	qido.com	todosomosprosegur.pt
prosegurchange.co.uk	qido.com.ar	transbank.co
prosegurchange.com	qido.com.co	tsplusplus.com
prosegurchange.dk	qido.com.pe	tstudio.tech
prosegurchile.cl	qido.com.py	tumovistarproseguralarmas .com
prosegurchina.com		
prosegurcloudgps.com		

universidadprosegur.com

v-n.com.ar

vn-global.com.ar

vnglobal.com.ar

3.3 Authority

The CIPHER-CSIRT expects to work cooperatively with system administrators and users of the client infrastructures, to the extent possible, to ensure the necessary authority to respond to security incidents.

4 POLICIES

4.1 Types of Incidents and Level of Support

The CIPHER-CSIRT restricts its support and incident handling activities to incidents that fall within its constituency.

Incident classification and reporting follow the RNCSIRT Common Taxonomy¹ (v3.3), aligned with the RSIT WG Reference Security Incident Taxonomy (v1003). Incidents may be classified using a primary classification (main intent/impact) and secondary classifications (e.g., delivery vector or enabling activity) when applicable.

4.1.1 Incident Classes Supported

Within its constituency, CIPHER-CSIRT provides support for incidents that fall under the following RNCSIRT incident classes:

- **Abusive Content:** Spam (unsolicited bulk email), harmful speech/policy violations, sexual/violent prohibited content.
- **Malicious Code:** Infected systems, command-and-control (C2) activity, malware distribution, malware configuration artefacts.
- **Information Gathering:** Scanning, sniffing, social engineering (non-technical means such as lies, tricks, bribes, threats).
- **Intrusion Attempts:** Exploitation of known vulnerabilities, login attempts (e.g., brute-force), new/unknown attack signatures.
- **Intrusions:** Privileged account compromise, unprivileged account compromise, application compromise, system compromise.
- **Availability:** DoS, DDoS, sabotage, misconfiguration, outage (no malice).
- **Information Content Security:** Unauthorized access to information, unauthorized modification of information (e.g., defacement/ransomware encryption), data loss, leak of confidential information.
- **Fraud:** Unauthorized use of resources, copyright infringement, masquerade/impersonation, phishing.
- **Vulnerable:** Weak cryptography, DDoS amplifiers, exposed/unwanted services, information disclosure, vulnerable systems.
- **Other:** Uncategorized, undetermined, test (used when the incident cannot be reliably classified at intake).

¹ https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf

4.1.2 Level of Support Provided

Depending on the type of incident and available information, CIPHER-CSIRT may provide one or more of the following:

- **Intake, triage and classification** according to the RNCSIRT taxonomy (including primary/secondary classifications where relevant).
- **Analysis support** (validation, scoping guidance, and interpretation of indicators/observables provided by the reporter).
- **Coordination and facilitation** with relevant internal parties within the constituency and, where appropriate, external entities (e.g., providers, other CSIRTs) to support containment and mitigation actions.
- **Mitigation and containment guidance** (advisory recommendations to limit impact and reduce recurrence).
- **Information sharing** within applicable information handling rules and agreed disclosure constraints.

Unless otherwise agreed, CIPHER-CSIRT does not provide full remediation, on-site response, or complete forensic investigation; it provides guidance and coordination support as appropriate.

4.1.3 Response Time

Under normal operating conditions, CIPHER-CSIRT will acknowledge and respond to incident reports within 24 hours.

4.1.4 Exclusions / Special Handling

Reports that primarily fall outside CSIRT handling (e.g., certain abusive content categories) may be redirected to the appropriate channels and/or competent authorities, as applicable. Notification to CNCS does not replace any mandatory reporting to judicial or law enforcement authorities when an incident also constitutes a criminal offense.

4.2 Co-operation, Interaction and Disclosure of Information

The CIPHER-CSIRT applies to the information that manages the protection measures corresponding to its nature and classification, taking as a reference, among others, the General European Data Protection Regulation (GDPR) and the European NIS directive.

Likewise, in communications and documentation, the FIRST TLP v1.1 protocol is used internally and externally for the classification and labelling of documents, according to which the following levels of information classification have been established:

- **RED**. Information is not distributable and is restricted to representatives authorized to participate directly in the exchange of information and who have signed the corresponding confidentiality commitments.

- **AMBER**. Information of limited and restricted distribution to authorized personnel, belonging to the service or its beneficiary organizations, who have a legitimate need to know to exercise their functions, and who have signed the corresponding confidentiality commitments.
- **GREEN**. Information of limited distribution and restricted to personnel and institutions within the service's trusted network, with which non-distribution agreements are established, but cannot be freely published or freely accessible.
- **WHITE**. Information that is freely distributed and not restricted but that may be subject to Copyright

Information tagged with identifiers in the TLP will be handled accordingly.

When reporting a sensitive incident, please indicate so appropriately, using the appropriate TLP label in the subject line, and please consider using encryption as specified in section 2.6

The CIPHER-CSIRT will handle all information that is provided as confidential. However, statistical data can be generated from some of this information as long as full confidentiality and anonymization can be ensured.

All confidentiality and privacy customer rights are safeguarded by a non-disclosure agreement, which is part of the standard incident handling service contract.

4.3 Communication and Authentication

In view of the types of information that the CIPHER-CSIRT will likely be dealing with, telephones and unencrypted e-mail will be sufficiently secure for low-sensitivity data. Any sensitive data should be encrypted with PGP.

5 SERVICES

5.1 Incident Response

CIPHER-CSIRT provides incident response support only for incidents affecting its constituency. Activities are performed in accordance with recognized CSIRT best practices and relevant guidance from organizations such as CERT/CC, ENISA, Trusted Introducer and FIRST.

The service typically includes intake and validation of reports, incident classification, coordination support, and mitigation guidance. Unless otherwise agreed, CIPHER-CSIRT provides advisory and coordination services and does not perform full remediation, on-site response, or comprehensive digital forensics.

Where applicable, CIPHER-CSIRT leverages its security monitoring and response capabilities, including the CIPHER xMDR platform, to support incident intake, correlation, enrichment and investigation workflows. Automation is used to accelerate initial assessment; final incident handling decisions remain under human responsibility.

5.2 Incident Triage

CIPHER-CSIRT performs an initial triage to validate the report and determine priority/severity based on available information, including (where applicable): incident type/classification, impact, scope/extent, urgency, confidence level, and potential for ongoing harm.

For incidents originating from monitored environments, triage is supported by automated workflows (e.g., alert correlation, enrichment and scoring). The assigned priority/severity is reviewed and, if necessary, adjusted by an analyst based on the evidence available and the operational context.

Each reported incident is recorded and assigned a unique incident identifier, and relevant information is documented to support tracking, coordination and reporting.

5.3 Incident Coordination

CIPHER-CSIRT coordinates the handling of incidents by facilitating communication and actions among relevant parties within the constituency and, when appropriate, external entities (e.g., service providers, vendors, other CSIRTs).

During analysis, CIPHER-CSIRT may identify likely causes, contributing factors and attack paths based on available evidence. Coordination activities are supported by case management and traceability features (e.g., timelines, artefact tracking and documented actions) to ensure continuity throughout the incident lifecycle.

When an incident is outside CIPHER-CSIRT's scope or authority, the report may be referred/forwarded to the appropriate responsible entity, and CIPHER-CSIRT may support coordination as appropriate.

5.4 Incident Resolution

CIPHER-CSIRT supports incident resolution by guiding containment, eradication and recovery, and for improving security posture to reduce recurrence. Where legal or disciplinary action is contemplated, CIPHER-CSIRT may guide preservation of relevant evidence and recommended documentation practices.

An incident may be considered resolved when one or more of the following conditions apply (as appropriate to the case):

- Affected services/systems have returned to an agreed normal operational state;
- Containment/mitigation actions have been implemented, and risk is reduced to an acceptable level;
- Responsibility has been formally transferred to another competent entity;
- The constituency confirms closure or accepts residual risk.

Non-confidential and/or sanitised data may be retained for statistical purposes, service improvement, and, where relevant, for information sharing with involved CSIRTs under applicable information handling rules.

5.5 Post-Incident Activities

After incident closure, CIPHER-CSIRT may support post-incident activities to strengthen prevention and readiness, such as:

- Post-incident review/lessons learned, including validation of what happened, what worked well, and what should be improved.
- Recommendations for corrective and preventive actions, including hardening measures, detection improvements, and process adjustments.
- Control and monitoring enhancements, where applicable (e.g., detection logic improvements, alert tuning guidance, indicator sharing).
- Reporting and metrics, using non-confidential or sanitised information for service quality, trend analysis, and (where applicable) structured information sharing with relevant CSIRTs.

Post-incident activities may be executed as part of normal CSIRT support or as additional services, depending on scope, complexity and agreement with the constituency.

5.6 Proactive Activities

The CIPHER-CSIRT provides consulting services. Detailed descriptions of these services are available at: <https://www.cipher.com>

6 DISCLAIMER

While every precaution will be taken in the preparation of information, notifications and alerts, CIPHER-CSIRT assumes no responsibility for errors or omissions, or for damage resulting from the use of information contained within.

Furthermore, several contractual obligations are included in the standard service contract, which only cover the parties involved.