LOGICALIS
Architects of Change

Logicalis EMEA CSIRT

RFC 2350

TLP:CLEAR

[PT]

O Logicalis EMEA CSIRT respeita o Traffic Light Protocol (TLP) no que toca à classificação da informação no âmbito da sua atividade CSIRT, definindo como, quando e com quem a informação pode ser partilhada.

Abaixo, são apresentadas as diferentes classificações da documentação do Logicalis EMEA CSIRT.

[EN]

The Logicalis EMEA CSIRT follows the Traffic Light Protocol (TLP) for the classification of information within the scope of its CSIRT activities, defining how, when and with whom information may be shared.

Below are the different classification levels applied to Logicalis EMEA CSIRT documentation and information.

Classificação / Classification	Descrição / Description
TLP:RED	[PT] Somente para os olhos e ouvidos dos indivíduos destinatários, não sendo possível qualquer partilha. Utilizado quando não é possível atuar sobre a informação sem colocar em risco significativo a privacidade, reputação ou operações das organizações envolvidas. Os destinatários não podem partilhar informações TLP:RED com mais ninguém. [EN] Information is restricted to the named recipients only. It must not be shared or disseminated further under any circumstances. TLP:RED is used when disclosure could cause a significant risk to the privacy, reputation or operations of the organizations or individuals involved. Recipients must not share TLP:RED information with anyone else.
TLP:AMBER	[PT] Divulgação limitada. Os destinatários só podem disseminar a informação para aqueles que necessitam de saber (*need to know basis*) dentro da sua própria organização e com os seus clientes. O TLP:AMBER+STRICT restringe a partilha de informação somente para a própria organização. Utilizado quando é necessário apoio para agir de forma efetiva sobre a informação, mas ainda assim há riscos para a privacidade, reputação ou operações das organizações envolvidas. Os destinatários podem partilhar informações TLP:AMBER com membros da sua própria organização e com os seus clientes, mas somente com aqueles que necessitam de ter acesso à informação (*need to know basis*) para proteger a sua organização e os seus clientes e evitar danos contínuos. Se o Logicalis EMEA CSIRT quiser restringir a partilha somente à Logicalis, deverá ser especificado TLP:AMBER+STRICT. [EN] Limited disclosure. Recipients may share the information strictly on a need-to-know basis within their own organization and with their customers. TLP:AMBER+STRICT restricts information sharing exclusively to the recipient's own organization. TLP:AMBER is used when information requires action or coordination, but where disclosure could still pose risks to privacy, reputation or operations. Recipients may share TLP:AMBER information only with those who need it to protect their organization and their customers and to prevent further harm. If the Logicalis EMEA CSIRT intends to restrict dissemination exclusively to Logicalis, this will be explicitly indicated as TLP:AMBER+STRICT.
TLP:GREEN	[PT] Divulgação limitada. Os destinatários podem divulgar a informação dentro da sua comunidade. O TLP:GREEN é usado quando a informação é útil para consciencialização ou divulgação dentro da sua comunidade de cibersegurança. Contudo, a informação não pode ser partilhada por meio de canais publicamente acessíveis. [EN] Limited disclosure. Recipients may share the information within their community. TLP:GREEN is used when information is useful for awareness or defensive purposes within the cybersecurity community, but must not be shared through publicly accessible channels.
TLP:CLEAR	[PT] Sem limites de divulgação, desde que respeitadas as regras de direitos de autor. [EN] Unlimited disclosure. Information may be shared publicly without restriction, provided that copyright rules are respected.

1. Informação acerca deste documento / About this document

[PT]

Este documento descreve o Serviço de Resposta a Incidentes de Segurança da Informação da Logicalis Portugal, também designado por Logicalis EMEA CSIRT, de acordo com o RFC 2350.

[EN]

This document describes the Information Security Incident Response Service of Logicalis Portugal, also referred to as the Logicalis EMEA CSIRT, in accordance with RFC 2350.

1.1 Data da Última Atualização / Date of Last Update

[PT]

Versão 1.0 publicada em 2026/02/01.

[EN]

Version 1.0 published on 2026/02/01.

1.2 Listas de Distribuição para notificações / Distribution Lists for Notifications

[PT]

Alterações a este documento são comunicadas para a equipa responsável pelo Serviço de Resposta a Incidentes de Segurança da Informação da Logicalis Portugal através do endereço de email soc-csirt@pt.logicalis.com.

[EN]

Changes to this document are communicated to the team responsible for the Information Security Incident Response Service of Logicalis Portugal via the email address soc-csirt@pt.logicalis.com.

1.3 Acesso a este Documento / Access to this Document

[PT]

A versão atualizada desde documento, em português e inglês, está disponível em https://www.pt.logicalis.com/rfc-2350/

[EN]

The current version of this document, in Portuguese and English, is available at:

https://www.pt.logicalis.com/rfc-2350/

1.4 Autenticidade deste Documento / Authenticity of this Document

[PT]

Este documento está assinado com a chave PGP do Logicalis EMEA CSIRT.

[EN]

This document is signed with the PGP key of the Logicalis EMEA CSIRT.

1.5 Identificação do Documento / Document Identification

Título / Title	RFC2350 Logicalis EMEA CSIRT
Versão / Version	1.0
Data / Date	15/01/2026
Validade / Expiration	*[PT]* Este documento é válido até ser substituído por uma versão mais recente. *[EN]* This document is valid until replaced by a more recent version.

2. Informação de Contacto / Contact Information

2.1 Nome da Equipa / Team Name

Logicalis EMEA CSIRT

2.2 Endereço Postal / Postal Address

Logicalis EMEA CSIRT

Logicalis Portugal

Lagoas Park, Ed. 5, Torre A, Piso 5

2740-265 Porto Salvo, Portugal

2.3 Zona Horária / Time Zone

Portugal/WEST (GMT+0, GMT+1 em horário de verão / daylight saving time)

2.4 Telefone / Telephone

+351 214 702 135	24x7

2.5 Fax

[PT] Não disponível.

[EN] Not available.

2.6 Outras Telecomunicações / Other Telecommunications

[PT]

Os utilizadores internos da Logicalis e os utilizadores externos registados (clientes e/ou parceiros) poderão utilizar a plataforma de gestão de incidentes de segurança da informação do Logicalis EMEA CSIRT disponível em:

https://lsoc.atlassian.net/servicedesk/customer/portal/103

[EN]

Internal Logicalis users and registered external users (customers and/or partners) may use the Information Security Incident Management platform of the Logicalis EMEA CSIRT available at:

https://lsoc.atlassian.net/servicedesk/customer/portal/103

2.7 Endereços de Correio Eletrónico / Email Addresses

soc-csirt@pt.logicalis.com

2.8 Chaves Públicas e Informação de Cifra / Public Keys and Encryption Information

PGP Key ID	0x948D94903F860D5F
PGP Fingerprint	2589 9D5B 2B36 F5FF E2CC FE2C 948D 9490 3F86 0D5F
PGP Key Type	RSA 4096 bits
PGP Key Expiration	2028-02-02
PGP Public Key URL	https://www.pt.logicalis.com/pgp/logicalis-emea-csirt.asc

2.9 Membros da Equipa / Team Members

[PT]

Coordenação: Artur Martins / Edgar Coutinho

A informação sobre os restantes membros da equipa está disponível por solicitação.

[EN]

Coordination: Artur Martins / Edgar Coutinho

Information regarding other team members is available upon request.

2.10 Outra Informação / Other Information

[PT]

Mais informações relativas ao Logicalis EMEA CSIRT podem ser encontradas em https://pt.logicalis.com/csirt/

[EN]

Further information regarding the Logicalis EMEA CSIRT can be found at:

https://pt.logicalis.com/csirt/

2.11 Meios de Contacto para Utilizadores / User Contact Channels

[PT]

Estão disponíveis os meios de contacto indicados em 2.2, 2.4, 2.6 e 2.7.

[EN]

The contact channels listed in sections 2.2, 2.4, 2.6 and 2.7 are available to users.

3. Guião / Charter

3.1 Missão / Mission

[PT]

O Logicalis EMEA CSIRT é a Equipa de Resposta a Incidentes de Segurança da Informação da Logicalis Portugal. É responsável pela gestão e entrega do SOC interno da Logicalis Portugal e dos serviços proporcionados aos seus clientes e parceiros, aos níveis de Cyber Threat Intelligence (CTI), Security Operations Center (SOC), Resposta a Incidentes Críticos, Análise Forense Digital e Offensive Security.

A missão do Logicalis EMEA CSIRT é a de proteger a informação e reagir a incidentes da Logicalis Portugal e dos seus clientes (Protect & Respond), no contexto da sua constituição, articulando processos e comunicação entre entidades, promovendo uma cultura de segurança e reduzindo o ciber risco.

[EN]

The Logicalis EMEA CSIRT is the Information Security Incident Response Team of Logicalis Portugal. It is responsible for the management and delivery of the internal SOC of Logicalis Portugal and the services provided to its customers and partners, including Cyber Threat Intelligence (CTI), Security Operations Center (SOC), Critical Incident Response, Digital Forensic Analysis and Offensive Security.

The mission of the Logicalis EMEA CSIRT is to protect information and respond to incidents affecting Logicalis Portugal and its customers (Protect & Respond), within the scope of its mandate, coordinating processes and communication between entities, promoting a security culture and reducing cyber risk.

3.2 Comunidade Servida / Constituency

[PT]

O Logicalis EMEA CSIRT monitoriza, deteta e responde a incidentes de Segurança da Informação de:

- Ativos de informação que constituem a infraestrutura da Logicalis Portugal, nomeadamente:
    - Ativos sob monitorização do Logicalis EMEA SOC,

  - O endereçamento público residente em:
    - 62.28.156.64
    - 62.28.211.46
    - 81.90.48.94 e
  - Os domínios:
    - pt.logicalis.com
    - ao.logicalis.com
    - cilnet.pt
    - cilnet.onmicrosoft.com
    - ptlogicalis.onmicrosoft.com
- Ativos de informação nos domínios de monitorização contratados pelos seus clientes e parceiros ao Logicalis EMEA SOC.

[EN]

The Logicalis EMEA CSIRT monitors, detects and responds to Information Security incidents affecting:

- Information assets that constitute the infrastructure of Logicalis Portugal, namely:
  - Assets under monitoring by the Logicalis EMEA SOC;
  - Public IP address ranges:
    - 62.28.156.64
    - 62.28.211.46
    - 81.90.48.94
  - Domains:
    - pt.logicalis.com
    - ao.logicalis.com
    - cilnet.pt
    - cilnet.onmicrosoft.com
    - ptlogicalis.onmicrosoft.com

- Information assets within monitoring scopes contracted by customers and partners of the Logicalis EMEA SOC.

3.3 Filiação / Affiliation

[PT]

O Logicalis EMEA CSIRT é uma equipa na dependência da Logicalis Portugal, integrada na unidade de Serviços de Segurança, e parte integrante do Logicalis EMEA SOC.

[EN]

The Logicalis EMEA CSIRT operates under Logicalis Portugal, integrated within the Security Services unit, and is an integral part of the Logicalis EMEA SOC.

3.4 Autoridade / Authority

[PT]

O Logicalis EMEA CSIRT atua sob autoridade do CISO e do Conselho de Administração da Logicalis Portugal (para clientes internos) e pelos contratos em vigor (para clientes externos e parceiros).

[EN]

The Logicalis EMEA CSIRT operates under the authority of the CISO and the Board of Directors of Logicalis Portugal (for internal customers) and under the applicable contracts in force (for external customers and partners).

4. Políticas / Policies

4.1 Tipos de Incidente e Nível de Suporte / Incident Types and Level of Support

[PT]

O Logicalis EMEA CSIRT responde a todas as categorias de incidentes de segurança da informação, decorrentes da taxonomia do Centro Nacional de Cibersegurança (CNCS), nomeadamente:

- Código Malicioso
- Disponibilidade
- Recolha de Informação
- Intrusão
- Tentativa de Intrusão
- Segurança da Informação
- Fraude
- Conteúdo Abusivo
- Vulnerabilidade
- Outro

O nível de suporte disponibilizado depende do tipo, severidade e âmbito do ativo afetado, sendo definido contratualmente com cada entidade constituinte.

Após ingeridos em SIEM, os eventos detetados são alvo de uma identificação inteligente pela plataforma de ticketing.

Essa identificação visa a movimentação prioritária ou não, de cada ticket, tendo em consideração os requisitos definidos na fase de Modelo de Governo.

Dessa forma, os eventos confirmados a incidentes são filtrados tendo em consideração:

1 – A taxonomia de classificação do incidente;

2 – A sua criticidade;

3 – Por inerência dos dois pontos anteriores, a sua severidade.

Os incidentes são classificados de S1 a S4, impactando os SLA's de serviço contratados.

[EN]

The Logicalis EMEA CSIRT responds to all categories of Information Security incidents, in accordance with the taxonomy defined by the Portuguese National Cybersecurity Center (CNCS), namely:

- Malware
- Availability
- Information Gathering
- Intrusion
- Attempted Intrusion
- Information Security
- Fraud
- Abusive Content
- Vulnerability
- Other

The level of support provided depends on the type, severity and scope of the affected asset and is defined contractually with each constituent.

Once ingested into the SIEM, detected events are subject to intelligent identification through the ticketing platform.

This identification aims to prioritize or deprioritize each ticket, taking into account the requirements defined during the Governance Model phase.

Confirmed incidents are filtered considering:

1 - Incident classification taxonomy;

2 - Asset criticality;

3 - Resulting incident severity.

Incidents are classified from S1 to S4, impacting the contracted service SLAs.

4.2 Cooperação, Interação e Partilha de Informação / Cooperation, Interaction and Information Sharing

[PT]

A política de privacidade da Logicalis Portugal, e consequentemente do Logicalis EMEA CSIRT, pressupõe que informação sensível só é partilhada com terceiros com a autorização do indivíduo ou entidade que seja proprietário dessa informação.

Aplicam-se as classificações TLP na partilha da informação.

[EN]

The privacy policy of Logicalis Portugal, and consequently of the Logicalis EMEA CSIRT, assumes that sensitive information is only shared with third parties with the authorization of the individual or entity that owns the information.

Traffic Light Protocol (TLP) classifications apply to information sharing.

4.3 Comunicação e Autenticação / Communication and Authentication

[PT]

Dos meios de comunicação disponibilizados pelo Logicalis EMEA CSIRT, o telefone e o correio eletrónico não cifrado são considerados suficientes para a transmissão de informação não sensível. Para a transmissão de informação sensível recomenda-se o uso de cifra PGP.

[EN]

Among the communication channels provided by the Logicalis EMEA CSIRT, telephone and unencrypted email are considered sufficient for transmitting non-sensitive information.

For the transmission of sensitive information, the use of PGP encryption is recommended.

5. Serviços / Services

[PT]

O Logicalis EMEA CSIRT disponibiliza os seguintes serviços aos seus constituintes.

[EN]

The Logicalis EMEA CSIRT provides the following services to its constituents.

5.1 Cyber Threat Intelligence

[PT]

Recolha, análise e disseminação de informação sobre ameaças relevantes, com o objetivo de apoiar a deteção precoce, a prevenção e a resposta a incidentes de segurança.

Inclui a monitorização de ameaças, campanhas ativas, indicadores de compromisso (IOC) e indicadores de risco (IoR), bem como o apoio à tomada de decisão.

[EN]

Collection, analysis and dissemination of threat intelligence to support early detection, prevention and response to security incidents.

Includes monitoring of threats, active campaigns, Indicators of Compromise (IOC) and Indicators of Risk (IoR), as well as decision-support activities.

5.2 Monitorização, Deteção e Resposta a Incidentes / Monitoring, Detection and Incident Response

[PT]

Monitorização contínua de ativos de informação, deteção de eventos e incidentes de segurança, análise técnica e resposta inicial, de acordo com os níveis de serviço contratados.

Inclui triagem, classificação, contenção e apoio à erradicação de incidentes.

[EN]

Continuous monitoring of information assets, detection of security events and incidents, technical analysis and initial response, in accordance with contracted service levels.

Includes triage, classification, containment and support for incident eradication.

5.3 Coordenação de Resposta a Incidentes / Incident Response Coordination

[PT]

Coordenação da resposta a incidentes de segurança, atuando como ponto central de contacto entre as partes envolvidas.

Inclui apoio à comunicação, articulação com entidades internas e externas, e acompanhamento do ciclo de vida do incidente até à sua resolução.

[EN]

Coordination of security incident response activities, acting as a central point of contact between involved parties.

Includes communication support, coordination with internal and external entities, and tracking of the incident lifecycle until resolution.

5.4 Análise Forense Digital / Digital Forensics Analysis

[PT]

Realização de análises forenses digitais a sistemas, aplicações e dados, com o objetivo de identificar causas, impactos e evidências associadas a incidentes de segurança.

As atividades são executadas de acordo com boas práticas de cadeia de custódia e metodologias reconhecidas.

[EN]

Execution of digital forensic analysis on systems, applications and data to identify causes, impacts and evidence related to security incidents.

Activities are performed in accordance with chain-of-custody best practices and recognized methodologies.

5.5 Offensive Security

[PT]

Execução de atividades controladas de segurança ofensiva, incluindo testes de intrusão, exercícios de Red Team e Purple Team, com o objetivo de avaliar a postura de segurança e melhorar as capacidades de deteção e resposta.

[EN]

Execution of controlled offensive security activities, including penetration testing, Red Team and Purple Team exercises, aimed at assessing security posture and improving detection and response capabilities.

6. Formulários de Resposta a Incidentes / Incident Response Forms

[PT]

Os utilizadores internos (Logicalis) e os clientes dos serviços de monitorização, deteção e resposta a incidentes, poderão utilizar o formulário referido em 2.6.

Indivíduos ou Entidades sem vínculo ao Logicalis EMEA SOC, deverão utilizar o email soc-csirt@pt.logicalis.com, não existindo neste caso qualquer formulário pré-definido.

[EN]

Internal users (Logicalis) and customers of monitoring, detection and incident response services may use the form referenced in section 2.6.

Individuals or entities without a contractual relationship with the Logicalis EMEA SOC must use the email address soc-csirt@pt.logicalis.com, in which case no predefined form is available.

7. Isenção de Responsabilidades / Disclaimer

[PT]

Embora sejam tomadas todas as precauções na preparação das informações, notificações e alertas, o Logicalis EMEA CSIRT não assume qualquer responsabilidade por erros ou omissões, nem por danos resultantes da utilização da informação disponibilizada.

[EN]

Although all precautions are taken in the preparation of information, notifications and alerts, the Logicalis EMEA CSIRT assumes no responsibility for errors or omissions, nor for damages resulting from the use of the information provided.