DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA EC GTS

Global Trusted Sign

Referência do Documento: DP02_GTS_V16

Classificação do Documento: Público

Data: 6 de julho de 2023

OID do Documento: 1.3.6.1.4.1.50302.1.1.1.2.1.0

Índice

1. Introdução 11
1.1. Contexto geral 11
1.2. Designação e identificação do documento 11
1.2.1. Revisão 12
1.2.2. Datas relevantes 12
1.3. Participantes na infraestrutura de chave pública 13
1.3.1. Entidades de certificação 13
1.3.2. Autoridade de registo 18
1.3.3. Titulares de certificados 19
1.3.4. Partes confiantes 19
1.3.5. Outros participantes 19
1.4. Utilização do certificado 20
1.4.1. Utilização adequada 21
1.4.2. Utilizações proibidas de certificado 22
1.5. Gestão de políticas 22
1.5.1. Entidade responsável pela gestão do documento 22
1.5.2. Entidade de contato 22
1.5.3. Entidade responsável pela determinação da conformidade do documento 23
1.5.4. Procedimento para aprovação do documento 23
1.6. Definições e acrónimos 24
1.6.1. Definições 24
1.6.2. Acrónimos 29
1.6.3. Referências bibliográficas 29
1.6.4. Convenções 30
2. Responsabilidade de publicação e repositório 30
2.1. Repositórios 30
2.2. Publicação da informação 31
2.3. Periodicidade de publicação 31
2.4. Controlos de acesso aos repositórios 31
3. Identificação e autenticação 32
3.1. Atribuição de nomes 32
3.1.1. Tipos de nomes 33
3.1.2. Necessidade de nomes significativos 33
3.1.3. Anonimato ou pseudónimo de titulares 33
3.1.4. Interpretação de formato de nomes 33
3.1.5. Unicidade de nomes 34
3.1.6. Reconhecimento, autenticação e função das marcas registadas 34

3.2. VALIDAÇÃO DE IDENTIDADE NO REGISTO INICIAL 34
3.2.1. Método de prova da posse da chave privada 34
3.2.2. Autenticação de identidade da organização e domínio 34
3.2.2.1. Identidade 35
3.2.2.2. Marcas registradas 36
3.2.2.3. Verificação do pais 36
3.2.2.4. Validação de autorização ou controle de domínio 36
3.2.2.5. Autenticação de um endereço ip 36
3.2.2.6. Validação do domínio wildcard 36
3.2.2.7. Exatidão de fontes de dados 36
3.2.2.8. Registos caa 37
3.2.3. Autenticação de identidade do indivíduo 37
3.2.4. Informação de subscritor/titular não verificada 40
3.2.5. Validação de autoridade 40
3.2.6. Critérios para interoperabilidade ou certificação 40
3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE RENOVAÇÃO DE CHAVE 40
3.3.1. Identificação e autenticação para pedidos de rotina de renovação de chave 40
3.3.2. Identificação e autenticação para renovação de chaves após revogação 40
3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDO DE REVOGAÇÃO 40
4. Requisitos operacionais do ciclo de vida do certificado 40
4.1. PEDIDO DE CERTIFICADO 40
4.1.1. Quem pode submeter um pedido de certificado 41
4.1.2. Processo de registo e responsabilidades 41
4.2. PROCESSAMENTO DO PEDIDO DE CERTIFICADO 41
4.2.1. Desempenho de funções de identificação e autenticação 41
4.2.2. Aprovação ou rejeição de pedidos de certificados 42
4.2.3. Prazo para emissão do certificado 42
4.3. EMISSÃO DE CERTIFICADOS 42
4.3.1. Ações da ec durante a emissão do certificado 42
4.3.2. Notificação ao subscritor/titular pela ec emissora do certificado 43
4.4. ACEITAÇÃO DO CERTIFICADO 43
4.4.1. Conduta que constitui a aceitação do certificado 43
4.4.2. Publicação do certificado pela ec 43
4.4.3. Notificação de emissão de certificados pela ec a outras entidades 43
4.5. UTILIZAÇÃO DO CERTIFICADO E PAR DE CHAVES 44
4.5.1. Utilização do certificado e par de chaves pelo subscritor/titular 44
4.5.2. Utilização do certificado e chave pública por partes confiantes 44
4.6. RENOVAÇÃO DE CERTIFICADO 44

4.6.1. Circunstâncias para a renovação do certificado 44
4.6.2. Quem pode submeter o pedido de renovação do certificado 45
4.6.3. Processamento do pedido de renovação de certificado 45
4.6.4. Notificação de emissão de renovação de certificado ao titular 45
4.6.5. Conduta que constitui a aceitação de renovação do certificado 45
4.6.6. Publicação da renovação do certificado pela ec 45
4.6.7. Notificação da renovação ao certificado a outras entidades 46
4.7. RE-KEY DO CERTIFICADO 46
4.7.1. Circunstâncias para o re-key de certificado 46
4.7.2. Quem pode solicitar a certificação de uma nova chave pública 46
4.7.3. Processamento de pedidos de re-key de certificado 46
4.7.4. Notificação de nova emissão de certificado ao subscritor/titular 46
4.7.5. Conduta que constitui a aceitação do certificado para o qual foi feito o re-key 46
4.7.6. Publicação do certificado pela ec para o qual foi feito re-key 46
4.7.7. Notificação de emissão de certificado pela ec a outras entidades 46
4.8. MODIFICAÇÃO DO CERTIFICADO 46
4.8.1. Circunstâncias para a modificação do certificado 47
4.8.2. Quem pode solicitar a modificação do certificado 47
4.8.3. Processamento de pedidos de modificação do certificado 47
4.8.4. Notificação de nova emissão ao subscritor/titular 47
4.8.5. Conduta que constitui a aceitação de certificado modificado 47
4.8.6. Publicação do certificado modificado pela ec 47
4.8.7. Notificação de emissão de certificado pela ec a outras entidades 47
4.9. REVOGAÇÃO E SUSPENSÃO DO CERTIFICADO 47
4.9.1. Motivos para revogação 47
4.9.1.1. Motivos para a revogação do certificado de um subscritor 47
4.9.1.2. Motivos para a revogação do certificado subordinado da ca 49
4.9.2. Quem pode solicitar a revogação 50
4.9.3. Procedimento para o pedido de revogação 50
4.9.4. Período de carência do pedido de revogação 50
4.9.5. Tempo de processamento do pedido de revogação pela ec 50
4.9.6. Requisito de verificação da revogação pelas partes confiantes 50
4.9.7. Frequência de emissão de crl (caso aplicável) 51
4.9.8. Latência máxima para crl (caso aplicável) 51
4.9.9. Disponibilidade de verificação de estado/revogação online 51
4.9.10. Requisitos de verificação de revogação online 51
4.9.11. Outras formas disponíveis de anunciar a revogação 52
4.9.12. Requisitos especiais relacionados com o comprometimento de chave 52

4.9.13. Motivos para a suspensão 52
4.9.14. Quem pode solicitar a suspensão 52
4.9.15. Procedimento para o pedido de suspensão 52
4.9.16. Limites do período de suspensão 52
4.10. SERVIÇOS DE ESTADO DO CERTIFICADO 52
4.10.1. Caraterísticas operacionais 52
4.10.2. Disponibilidade de serviço 52
4.10.3. Funcionalidades opcionais 52
4.11. FIM DE SUBSCRIÇÃO 53
4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVES 53
4.12.1. Política e práticas de custódia e recuperação de chaves 53
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão 53
5. Controlos de segurança física, gestão e operacionais 53
5.1. CONTROLOS DE SEGURANÇA FÍSICA 53
5.1.1. Localização física e tipo construção 53
5.1.2. Acesso físico 54
5.1.3. Energia e ar condicionado 55
5.1.4. Exposição à água 55
5.1.5. Prevenção e proteção contra incêndio 55
5.1.6. Armazenamento de media 56
5.1.7. Eliminação de resíduos 56
5.1.8. Backups em instalações externas 56
5.2. CONTROLOS PROCEDIMENTAIS 56
5.2.1. Grupos de trabalho 57
5.2.2. Número de pessoas exigidas por grupo 59
5.2.3. Identificação e autenticação por função 59
5.2.4. Segregação de funções 59
5.3. CONTROLOS DE SEGURANÇA PESSOAL 59
5.3.1. Requisitos relativos a qualificações, experiência e credenciação 59
5.3.2. Procedimento de verificação de antecedentes 60
5.3.3. Requisitos e procedimentos de formação 60
5.3.4. Frequência e requisitos para atualização de formação 60
5.3.5. Frequência e sequência da rotação de funções 61
5.3.6. Sanções para ações não autorizadas 61
5.3.7. Requisitos para prestadores de serviços independentes 61
5.3.8. Documentação fornecida ao pessoal 61
5.4. PROCEDIMENTOS DE REGISTO DE AUDITORIA 61
5.4.1. Tipos de eventos registados 61

5.4.2. Frequência de processamento de registos de auditoria 62
5.4.3. Período de retenção de registo de auditoria 62
5.4.4. Proteção de registo de auditoria 62
5.4.5. Procedimentos de cópias de segurança de registos de auditoria 63
5.4.6. Sistema de recolha de registos (interno vs. Externo) 63
5.4.7. Notificação de agentes causadores de eventos 63
5.4.8. Avaliação de vulnerabilidades 63
5.5. ARQUIVO DE REGISTOS 63
5.5.1. Tipos de registos arquivados 63
5.5.2. Período de retenção em arquivo 63
5.5.3. Proteção do arquivo 64
5.5.4. Procedimentos para cópia de segurança do arquivo 64
5.5.5. Requisitos para validação cronológica de registos 64
5.5.6. Sistema de recolha de arquivo (interno vs. Externo) 64
5.5.7. Procedimentos para obter e verificar informação de arquivo 64
5.6. RENOVAÇÃO DE CHAVES 64
5.7. RECUPERAÇÃO EM CASO DE DESASTRE OU COMPROMETIMENTO 64
5.7.1. Procedimentos em caso de incidente ou comprometimento 64
5.7.2. Processos de recuperação caso os recursos informáticos, software e/ou dados, sejam corrompidos 65
5.7.3. Procedimentos em caso de comprometimento de chave privada da entidade 65
5.7.4. Capacidades de continuidade de negócio em caso de desastre 66
5.8. PROCEDIMENTOS EM CASO DE EXTINÇÃO DA ENTIDADE DE CERTIFICAÇÃO OU ENTIDADE DE REGISTO 66
6. Controlos de segurança técnica 66
6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES 66
6.1.1. Geração do par de chaves 67
6.1.1.1. Geração de par de chaves ca 67
6.1.1.2. Geração de par de chaves ra 67
6.1.1.3. Geração de par de chaves utilizador 67
6.1.2. Entrega de chave privada ao subscritor/titular 67
6.1.3. Entrega de chave pública ao emissor do certificado 67
6.1.4. Entrega da chave pública da ec às partes confiantes 67
6.1.5. Tamanhos de chaves 67
6.1.6. Geração dos parâmetros de chave pública e verificação de qualidade 68
6.1.7. Finalidades de utilização da chave (de acordo com o campo key usage x.509 v3) 68
6.2. PROTEÇÃO DE CHAVE PRIVADA E CONTROLOS DE ENGENHARIA DE MÓDULO CRIPTOGRÁFICO 68
6.2.1. Controlos e standards de módulo criptográfico 68
6.2.2. Controlo multi pessoal (n de m) da chave privada 69

6.2.3. Custódia de chave privada 69
6.2.4. Cópia de segurança da chave privada 69
6.2.5. Arquivo de chave privada 69
6.2.6. Transferência da chave privada para/de um módulo criptográfico 69
6.2.7. Armazenamento da chave privada em módulo criptográfico 69
6.2.8. ~~A~~tivação da chave privada 69
6.2.9. ~~D~~esativação da chave privada 70
6.2.10. ~~D~~estruição da chave privada 70
6.2.11. Capacidades do módulo criptográfico 70
6.3. OUTROS ASPETOS DA GESTÃO DO PAR DE CHAVES 70
6.3.1. Arquivo da chave pública 70
6.3.2. Períodos operacionais do certificado e períodos de utilização do par de chaves 70
6.4. DADOS DE ATIVAÇÃO 71
6.4.1. Geração e instalação de dados de ativação 71
6.4.2. Proteção de dados de ativação 71
6.4.3. Outros aspetos dos dados de ativação 71
6.5. CONTROLOS DE SEGURANÇA COMPUTACIONAL 71
6.5.1. Requisitos técnicos específicos de segurança computacional 71
6.5.2. Avaliação/nível de segurança computacional 71
6.6. CONTROLOS TÉCNICOS DO CICLO DE VIDA 72
6.6.1. Controlos de desenvolvimento de sistema 72
6.6.2. Controlos de gestão da segurança 72
6.6.3. Controlos de segurança do ciclo de vida 72
6.7. CONTROLOS DE SEGURANÇA DE REDE 72
6.8. VALIDAÇÃO CRONOLÓGICA 72
7. Perfis de certificado, crl e ocsp 73
7.1. PERFIL DO CERTIFICADO 73
7.1.1. Número(s) de versão 73
7.1.2. Conteúdo e extensões do certificado, aplicabilidade do rfc 5280 73
7.1.2.1. Certificado da root ca 73
7.1.2.2. Certificados da ec subordinada da gts 73
7.1.2.3. Subscritores dos certificados 74
7.1.2.4. Todos os certificados 74
7.1.2.5. Aplicabilidade do rfc 5280 74
7.1.3. Identificadores de objeto de algoritmo 74
7.1.3.1. Subjectpublickeyinfo 74
7.1.3.2. Signature algorithmidentifier 74
7.1.4. Formatos de nome 74

7.1.4.1. Nomes de codificação 74
7.1.4.2. Informações relativas ao assunto - certificados de utilizadores 75
7.1.4.3. Informações relativas ao assunto - certificado da raiz e certificados ca subordinados ... 75
7.1.5. Restrições de nome 75
7.1.6. Identificador de objeto de política de certificado 75
7.1.6.1. Identificadores de política de certificados reservados 75
7.1.6.2. Certificados de ca raiz 75
7.1.6.3. Certificados de ca subordinados 75
7.1.6.4. Certificados de utilizadores 75
7.1.7. Utilização de extensão de restrições de política 75
7.1.8. Sintaxe e semânticas de qualificadores de política 75
7.1.9. Processamento de semânticas para a extensão de políticas de certificado críticas 76
7.2. Perfil CRL 76
7.2.1. Número(s) de versão 76
7.2.2. Crl e extensões da crl 77
7.3. Perfil OCSP 77
7.3.1. Número(s) de versão 77
7.3.2. Extensões ocsp 77
8. Auditoria de conformidade e outras avaliações 77
8.1. Frequência ou circunstâncias da avaliação 77
8.2. Identificação/qualificações do avaliador 77
8.3. Relação do avaliador com a entidade avaliada 78
8.4. Tópicos abrangidos pela avaliação 78
8.5. Ações tomadas como resultado de deficiências 78
8.6. Comunicação de resultados 79
8.7. Auditorias internas 79
9. Outras matérias legais e de negócio 79
9.1. Taxas 79
9.1.1. Taxas de emissão ou renovação de certificado 79
9.1.2. Taxas de acesso a certificado 79
9.1.3. Taxas de acesso a informação de estado ou revogação 80
9.1.4. Taxas para outros serviços 80
9.1.5. Política de reembolso 80
9.2. Responsabilidade financeira 80
9.2.1. Cobertura de seguro 80
9.2.2. Outros recursos 80
9.2.3. Cobertura de seguro ou garantia para utilizadores finais 80
9.3. Confidencialidade de informação de negócio 80

9.3.1. Âmbito de informação confidencial 80
9.3.2. Informação fora do âmbito de informação confidencial 81
9.3.3. Responsabilidade de proteção de informação confidencial 81
9.4. PRIVACIDADE DE INFORMAÇÃO PESSOAL 81
9.4.1. Plano de privacidade 81
9.4.2. Informação privada 81
9.4.3. Informação não considerada privada 82
9.4.4. Responsabilidade pela proteção de informação privada 82
9.4.5. Notificação e consentimento para utilização de informação privada 82
9.4.6. Divulgação resultante de processo judicial ou administrativo 82
9.4.7. Outras circunstâncias de divulgação de informação 82
9.5. DIREITOS DE PROPRIEDADE INTELECTUAL 82
9.6. REPRESENTAÇÕES E GARANTIAS 82
9.6.1. Representações e garantias da ec 82
9.6.2. Representações e garantias da ar 84
9.6.3. Representações e garantias dos subscritores/titulares 84
9.6.4. Representações e garantias das partes confiantes 85
9.6.5. Representações e garantias de outros participantes 85
9.7. RENÚNCIA DE GARANTIAS 85
9.8. LIMITAÇÕES DE RESPONSABILIDADE 85
9.9. INDEMNIZAÇÕES 85
9.10. PRAZO E TERMINAÇÃO 86
9.10.1. Prazo 86
9.10.2. Terminação 86
9.10.3. Efeito da terminação e sobrevivência 86
9.11. NOTIFICAÇÕES INDIVIDUAIS E COMUNICAÇÕES AOS PARTICIPANTES 86
9.12. ALTERAÇÕES 86
9.12.1. Procedimento para alteração 86
9.12.2. Mecanismo de notificação e período 86
9.12.3. Circunstâncias nas quais o oid deve ser alterado 87
9.13. DISPOSIÇÕES DE RESOLUÇÃO DE CONFLITO 87
9.14. LEGISLAÇÃO APLICÁVEL 87
9.15. CONFORMIDADE COM A LEGISLAÇÃO APLICÁVEL 87
9.16. OUTRAS DISPOSIÇÕES 88
9.16.1. Acordo completo 88
9.16.2. Atribuição 88
9.16.3. Severidade 88
9.16.4. Execução (honorários de advogados e renúncia de direitos) 88

9.16.5. Força maior 88
9.17. OUTRAS PROVISÕES 89

1. Introdução

a) Âmbito

O presente documento é a Declaração de Práticas de Certificação e tem como objetivo informar os procedimentos seguidos pela Global Trusted Sign, adiante designada por EC GTS, enquanto prestadora qualificada de serviços de confiança no âmbito do regulamento da UE nº 910/2014, no suporte à sua atividade de emissão de certificados qualificados e avançados da Entidade Certificadora EC GTS.

b) Público-Alvo

O presente documento apresenta-se disponível publicamente e é destinado a todos os participantes que se relacionem com a EC GTS.

c) Estrutura do Documento

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX (Public-Key Infrastructure X.509), do IETF (Internet Engineering Task Force), no documento RFC 3647. No âmbito da presente Declaração de Práticas de Certificação, assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique, recomenda-se o estudo prévio dos referidos tópicos, permitindo assim uma melhor compreensão desta declaração. Os primeiros sete capítulos descrevem os procedimentos e práticas mais importantes no âmbito da certificação digital da PKI GTS. O capítulo oito descreve as auditorias de conformidade. O capítulo nove descreve matérias legais.

1.1. Contexto Geral

As práticas de criação, assinatura e emissão de certificados, assim como de revogação de certificados inválidos, levadas a cabo por uma Entidade de Certificação (EC) são fundamentais para garantir a fiabilidade e confiança de uma infraestrutura de Chaves Públicas (“PKI – Public Key Infrastructure”). A presente Declaração de Práticas de Certificação especifica os requisitos de segurança, políticas e práticas aplicáveis pelo prestador qualificado de serviços de confiança que emita certificados. As políticas e requisitos de segurança encontram-se definidos nos requisitos para a gestão do ciclo de vida dos certificados qualificados em conformidade com as políticas de certificados existentes.

1.2. Designação e Identificação do Documento

O presente documento é a Declaração de Práticas de Certificação da EC GTS cujo OID associado é 1.3.6.1.4.1.50302.1.1.1.2.1.0:

Informação do Documento	
Nome do Documento	Declaração de Práticas de Certificação da EC GTS
Versão do Documento	16.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.1.2.1.0
Data de Emissão	6 de julho de 2023
Validade	6 de julho de 2024
Localização	https://pki.globaltrustedsign.com/index.html

Nota: Atualizações regulares neste documento são realizadas sempre que se justifiquem.

1.2.1. Revisão

N.º da Versão	Elaborado	Aprovado	Motivo
	06-07-2023	06-07-2023	
16	**AdmSeg**	**Grupo de Gestão**	Adição dos endereços no ponto 4.9.7
	Débora Sofia Vieira Rodrigues Assinado com Assinatura Digital Qualificada por: DÉBORA SOFIA VIEIRA RODRIGUES Data: 06-07-2023 10:59:04	Tolentino de Deus Faria Pereira	

1.2.2. Datas Relevantes

ID de versão	Data da versão	Motivo da nova versão
Versão 1	31-07-2017	Declaração de Práticas de Certificação da EC GTS
Versão 2	12-09-2017	Atualização dos conteúdos
Versão 3	29-12-2017	QtimeStamp - ETSI EN 319 421
Versão 4	05-03-2018	Atualização de formatação e conteúdos gerais
Versão 5	08-03-2018	Atualização do ponto 12.3
Versão 6	09-01-2019	Atualização de informação sobre a validade à distância
Versão 7	02-05-2020	Atualização da hierarquia da EC GTS com SUBCA de certificados avançados
Versão 8	24-06-2020	Atualização da hierarquia da EC GTS com SUBCA 03
Versão 9	17-09-2020	Atualização de registos de colaborador do Grupo de Confiança da GTS. Atualização do grupo de confianças
Versão 10	06-05-2021	Atualização de estrutura do documento, de acordo com o RFC 3647
Versão 11	23-06-2021	Atualização geral dos conteúdos
Versão 12	21-07-2021	Correção de OID
Versão 13	20-07-2022	Verificação anual do documento
Versão 14	15-02-2023	Atualização da hierarquia do PKI e revisão do documento
Versão 15	04-07-2023	Verificação anual do documento e atualização dos valores associados aos contactos telefónicos
Versão 16	06-07-2023	Adição dos endereços no ponto 4.9.7

1.3. Participantes na Infraestrutura de Chave Pública

1.3.1. Entidades de Certificação

A ACIN-iCloud Solutions, atua como Entidade de Certificação sendo os seus dados corporativos os seguintes:

Denominação social: ACIN-iCloud Solutions,Lda

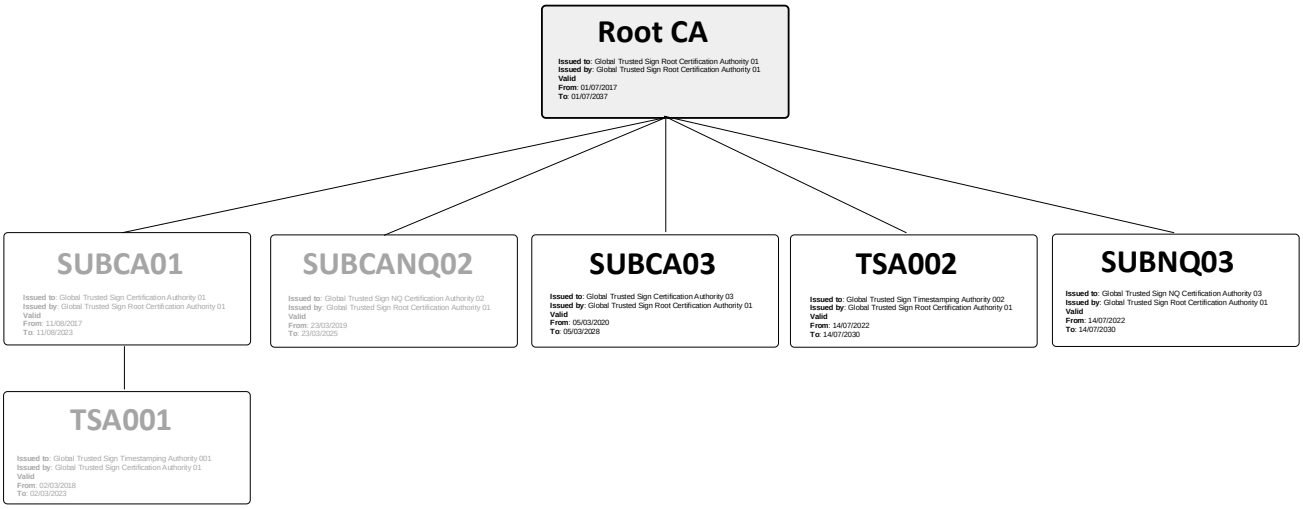
NICP: 511 135 610

Morada: Estrada Regional 104, N.º 42 A, 9350-203 Ribeira Brava

N.º de Telefone: Nacional: 707 451 451[1]/ Internacional +351 291 957 888[2]

Página web: www.acin.pt

A GTS, denominação adotada pela ACIN para o produto de prestador qualificado de serviços de confiança, disponibiliza uma hierarquia de confiança credenciada pelo Gabinete Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), conforme previsto na legislação portuguesa e europeia. É composta por um conjunto de equipamentos, aplicações, recursos humanos e procedimentos indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir assim a adequada gestão do ciclo de vida dos certificados descritos no presente documento. A hierarquia de confiança da GTS é composta pela Entidade Certificadora Raiz da GTS (ROOT CA GTS), as Entidades Certificadoras da GTS (EC GTS01 – SUBCA01 e EC GTS03 – SUBCA03), a Entidade Certificadora Não Qualificada da GTS (EC NQ GTS – SUBCANQ02 e SUBNQ03) e a Entidade Certificadora de Selos Temporais da GTS (EVC GTS – TSA001 e TSA002).



Legenda:

1 – Root CA GTS - Entidade Certificadora Raiz da GTS

[1] Preço máximo a pagar por minuto: 0,09€ (+IVA) para as chamadas originadas nas redes fixas e 0,13€ (+IVA) para as originadas nas redes móveis;

[2] Custo de uma chamada internacional para rede fixa, de acordo com o tarifário em vigor.

2 – SUBCA01 - Entidade Certificadora
3 – TSA001 - Entidade Certificadora de Validação Cronológica da GTS
4 – SUBCANQ02 - Entidade Certificadora Não Qualificada da GTS
5 – SUBCA03– Entidade Certificadora da GTS
6 – TSA002 – Entidade Certificadora de Validação Cronológica da GTS
7 – SUBNQ03 – Entidade Certificadora Não Qualificada da GTS

a) Entidade Certificadora Raiz da GTS (ROOT CA GTS)

A ROOT CA GTS é uma entidade certificadora credenciada pelo Gabinete Nacional de Segurança, de acordo com o Regulamento (UE) N.º 910/2014, estando deste modo habilitada, legalmente, a emitir certificados para Entidades Certificadoras Subordinadas.

O certificado da ROOT CA GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	7d 9f 44 7c b2 77 97 a8 59 57 bf 11 dd 8f 99 f5
Validade	01/07/2017 a 01/07/2037
Marca Digital	70 d1 2e f7 f5 90 18 87 47 88 42 c6 4e 05 ef 2c 0a 63 92 9d
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

b) Entidade Certificadora da GTS (EC GTS)

A Entidade Certificadora da GTS emite:

✓ **Certificados qualificados para autenticação de sítios Web (SSL/TLS)**

Os serviços de autenticação de sítios web fornecem meios que dão aos visitantes de um sítio web a garantia de que existe uma entidade genuína e legítima responsável pelo sítio. Estes serviços contribuem para a criação de relações de confiança na realização de negócios *online*, pois os utilizadores têm confiança na legitimidade desses mesmos sítios web pela garantia de autenticidade, titularidade e confidencialidade da informação transacionada. A prática de emissão de certificados qualificados para autenticação de sítios web da EC GTS está em conformidade com os requisitos do CA/Browser fórum disponíveis em http://www.cabforum.org:

- Organization Validation: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates;
- Extended Validation: Guidelines for the issuance and management of Extended Validation Certificates.

A validação do domínio dos certificados requisitados (dono do domínio, domínio wild-card e CAA Records) conforme definido no CA/B Forum:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.8.4 capítulo 3.2.2.

Em caso de inconsistência entre esta PC e estes Requisitos do CA/B Forum, os requisitos assumem precedência.

✓ **Certificados para assinatura eletrónica qualificada**

Os certificados para assinatura eletrónica qualificada permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo, bem como a integridade do documento.

✓ **Certificados para selos eletrónicos**

Os certificados para selos eletrónicos permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa coletiva, certificando a origem e a integridade do documento.

Os certificados da EC GTS – SUBCA01:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Certification Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	5d f5 55 01 8c 89 45 56 59 8d cf d9 13 3b 87 ab
Validade	11/08/2017 a 11/08/2023
Marca Digital	2b 30 32 d4 9d 12 74 af 30 ab a3 ec 29 a6 a0 25 ae f6 dc bc
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

Os certificados da EC GTS – SUBCA03:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Certification Authority 03, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	1e 0a 5a 4e b2 45 99 3c 5e b9 2f 31 48 db 0c f6
Validade	11/05/2020 a 11/05/2028
Marca Digital	60 2f 17 18 96 72 78 f5 88 4f 33 16 f2 65 9b c1 f3 cc b2 46
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

c) Entidade Certificadora de Selos Temporais da GTS (EVC GTS)

A EVC GTS é uma entidade certificadora de validação cronológica habilitada a emitir selos temporais qualificados. A monitorização do serviço de emissão de selos temporais tem o objetivo de detetar qualquer desvio maior que os requisitos impostos pela norma ETSI EN 319 421. Serão monitorizados todos os offsets entre as máquinas que suportam o serviço de emissão de selos temporais com o objetivo de gerar alarmística relevante que será usada para tomar iniciativas corretivas. A EVC GTS tem a responsabilidade de operar uma ou mais TSU (time-stamping unit) para a criação e assinatura de selos temporais em nome da GTS, cada uma com a sua chave distinta de assinatura, cujo relógio utilizado para emitir selos temporais está sincronizado não só com o próprio relógio atómico da GTS, mas também, para efeitos de redundância, com mais duas fontes acreditadas conforme a norma ETSI EN 319 421.

O certificado da EVC GTS –TSA001:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Timestamping Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	04 bd 81 30 e4 ae 61 40 5a 99 43 db 7a 72 4f 47
Validade	02/03/2018 a 02/03/2023
Marca Digital	21 16 db 77 7e 72 fd 57 61 2a 24 27 8f d2 05 c8 bc fd a3 98
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

O certificado da EVC GTS –TSA002:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Timestamping Authority 002, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	sha256RSA
Nº de Série	21 ee 9d 30 24 e9 0c 7e 62 cf f9 ac 3f f1 0c 08
Validade	14/07/2022 a 14/07/2030
Marca Digital	bf e9 50 86 06 35 80 b8 91 ea 42 e3 c1 e6 70 43 b5 3f 11 e4
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

d) Entidade Certificadora Não Qualificada da GTS (EC NQ GTS)

A ECNQ GTS emite certificados avançados para assinatura não qualificada da Global Trusted Sign, enquanto prestadora de serviços de confiança, que cumprem os requisitos definidos no Regulamento (UE) Nº 910/2014 (no que for aplicável), no ETSI EN 319 401, v2.2.1 e ETSI EN 319 411-1, v.1.2.2.

O certificado da EC NQ GTS 2 – SUBCANQ02:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign NQ Certification Authority 02, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	7e 88 a8 ed 54 02 9f c6 5c 96 00 8e 0a cf bd c1
Validade	23/03/2019 a 23/03/2025
Marca Digital	7e 55 0f f3 8f 70 2e eb 5d 8f f0 e2 02 75 78 3f be 83 57 38
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

O certificado da EC NQ GTS 3 – SUBCANQ03:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign NQ Certification Authority 03, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	sha256RSA
Nº de Série	5b 12 f7 4a cb ca 73 e0 62 cf f2 13 84 35 c5 64
Validade	14/07/2022 a 14/07/2030
Marca Digital	13 c5 be fc 66 be 0f fe 82 97 97 ec 44 5f a9 e4 96 d2 f1 a8
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

1.3.2. Autoridade de Registo

A Autoridade de Registo (AR) é a entidade que aprova os nomes distintos (DN) dos titulares dos certificados e avaliação da veracidade dos documentos e identidade dos titulares dos pedidos. Mediante esta avaliação, aceita ou rejeita a solicitação do mesmo.

Adicionalmente a RA tem autoridade para aprovar a revogação de certificados.

As Autoridades de Registo da Global Trusted Sign estão em conformidade com os requisitos estabelecidos neste documento e estão sujeitas a Auditorias Externas independentes, assim como Auditorias Internas realizadas pela Global Trusted Sign regularmente.

A emissão dos certificados digitais pressupõe a aceitação do Termos e Condições dos certificados:

- FO23_GTS - Termos e Condições dos Certificados para assinaturas qualificadas
- FO24_GTS - Termos e Condições dos Certificados para Selos Eletrónicos
- FO09_GTS - Termos e Condições dos Certificados Autenticação Web
- FO52_GTS - Termos e Condições de certificados de assinatura Avançados
- FO53_GTS - Termos e Condições dos Certificados para Selos Eletrónicos Avançados

a) Autoridade de Registo Interna

No âmbito da Entidade de Certificação Global Trusted Sign, a autoridade de registo é executada pelos serviços internos da mesma, que têm a responsabilidade de validação dos dados necessários, conforme explicitado nas políticas especificas da Global Trusted Sign, para cada um dos serviços disponibilizados.

b) Autoridade de Registo Externa

A Global Trusted Sign, não dispõe de Autoridades de Registo Externas, uma vez que não existe qualquer contrato com terceiras partes para realizar a validação de domínio dos certificados SSL e da identidade dos certificados avançados e qualificados.

1.3.3. Titulares de Certificados

No âmbito da presente declaração de práticas, são subscritores/titulares todos os utilizadores finais a quem tenham sido atribuídos certificados pelo PKI da GTS. São considerados titulares de certificados emitidos pela GTS aqueles cujo nome está inscrito no campo "*Subject*" do certificado e utilizam-no, bem como a respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descritas neste documento, sendo emitidos certificados para as seguintes categorias titulares:

- Pessoa física ou jurídica;
- Pessoa coletiva (organizações);
- Serviços (computadores, firewalls, etc.);
- Os membros dos grupos de trabalho, nomeadamente da Administração de Segurança, agem como subscritores, responsabilizando-se pela correta utilização do certificado, bem como pela proteção e salvaguarda da respetiva chave privada.

1.3.4. Partes Confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave publica, ou seja, confiam que o certificado corresponde na realidade a quem diz pertencer. Neste documento, considera-se uma parte confiante, aquele que confia no teor, validade e aplicabilidade do certificado emitido pelo PKI da GTS.

1.3.5. Outros Participantes

a) Entidade Supervisora

A Entidade Supervisora é a entidade competente para a credenciação e fiscalização das entidades certificadoras prestadoras de serviços de confiança qualificados. No panorama nacional, essa função é desempenhada pelo Gabinete Nacional de Segurança (GNS). A Entidade Supervisora contribui para a confiança nos certificados qualificados, pelas competências que exerce sobre as EC que os emite. No âmbito das suas funções, a Entidade Supervisora exerce os seguintes papéis relativamente às Entidades Certificadoras:

- **Notificação de intenção:** procedimento de aprovação dos serviços de confiança prestados pelos prestadores de serviços qualificados, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, o hardware, software e os procedimentos de acesso e de operação;
- **Organismo de avaliação da conformidade:** enquanto organismo competente para realizar a avaliação da conformidade dos serviços de confiança prestados pelos prestadores de serviços qualificados;
- **Fiscalização:** Inspeções efetuadas para confirmar que tanto os prestadores qualificados de serviços de confiança como os serviços de confiança que prestam cumprem os requisitos estabelecidos pelo Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho.

b) Entidades Externas

A atividade dos prestadores de serviços que suportam a GTS no desempenho das suas funções enquanto prestadora qualificada de serviços de confiança é contratualizada de modo a garantir a atribuição formal das funções e responsabilidades de cada uma das partes, bem como o cumprimento das políticas e práticas instituídas na GTS.

c) Organismo de Avaliação de Conformidade

O Organismo de avaliação da conformidade (*Conformity Assessment Body* – CAB) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

1.4. Utilização do Certificado

Os certificados emitidos pelo PKI da GTS são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança, nomeadamente:

- Autenticação;
- Confidencialidade;
- Integridade;
- Privacidade de Dados;
- Não Repúdio;
- Autenticidade.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, mediante a utilização da estrutura de confiança que a PKI da GTS disponibiliza. As Partes Confiantes podem

verificar a cadeia de confiança de um certificado emitido pela EC GTS, garantindo assim a autenticidade e identidade do titular. Os certificados qualificados emitidos pela EC GTS estão de acordo com esta DPC e são certificados qualificados em conformidade com os requisitos do regulamento (EU) 910/2014.

1.4.1. Utilização Adequada

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela PKI GTS.

a) Certificados qualificados de autenticação de sítios Web

Os certificados qualificados de autenticação de sítios Web emitidos pela EC GTS são utilizados pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos com o objetivo de estabelecer comunicação de dados Web based através de protolocos SSL/TLS. Os certificados qualificados de autenticação de sítios Web têm como objetivo:

- Identificar a entidade coletiva que controla um sítio web: fornece garantia razoável ao utilizador de um navegador Internet que o sítio web que o utilizador está a aceder é controlado por uma entidade coletiva que está identificada no certificado através do nome, sede social, inscrição no Instituto de Registos e Notariado, ou outra informação desambiguadora;

- Permitir comunicações cifradas com um sítio Web: facilita a troca de chaves de cifra de modo a permitir a comunicação de informação cifrada através da Internet, entre o utilizador de um navegador Internet e um sítio web.

- Dificultar os ataques de phishing e outros de fraude de identidade que utilizam certificados;

- Apoiar as empresas que possam ter sido o alvo de um ataque de phishing ou fraude de identidade ao disponibilizar uma ferramenta para a sua identificação perante os utilizadores;

- Apoiar as forças de segurança nas suas investigações de phishing e outros ataques de Comunic1 de identidade, apoiando, quando aplicável, o contacto, investigação, e ações legais contra o Titular.

b) Certificados para assinatura qualificada e selos eletrónicos

Os certificados qualificados de assinatura eletrónica e selos eletrónicos emitidos pela GTS são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de permitir a assinatura probatória de documentos por pessoas singulares e coletivas. Os certificados para assinatura eletrónica qualificada devem ser utilizados para a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita. Esta utilização permite servir de prova da emissão de um documento eletrónico por determinada pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo, bem como a

integridade do documento. No caso dos certificados para selos eletrónicos, a utilização é análoga à dos certificados de assinatura qualificada, no entanto aplicam-se na prova da emissão por determinada pessoa coletiva, certificando a origem e a integridade do documento. O subscritor é responsável pelo conteúdo de todas as transações realizadas através do serviço.

c) Certificados para assinatura e selos eletrónicos avançada

Os certificados digitais avançados oferecem um elevado nível de confiança, todavia não garantem o valor probatório dos certificados qualificados.

Estes certificados podem ser utilizados para:

- Realizar a sua autenticação online de forma segura;
- Assinar emails;
- Assinar documentos sem valor probatório legal.

1.4.2. Utilizações Proibidas de Certificado

Os certificados emitidos na hierarquia de confiança da EC GTS não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente, ressalvada a exceção de poderem ser utilizados em outros contextos quando legalmente previstos na legislação aplicável. Os serviços de certificação prestados pela EC GTS não garantem o cumprimento de requisitos de alta disponibilidade e resiliência, que os qualifique para a sua utilização em serviços ou infraestruturas críticas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra catividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

1.5. Gestão de Políticas

1.5.1. Entidade Responsável pela Gestão do Documento

A gestão desta declaração de práticas de certificação da EC GTS é da responsabilidade do grupo de Confiança da GTS.

1.5.2. Entidade de Contacto

Nome	Grupo de Confiança da GTS
Gestores	Tolentino de Deus Faria Pereira José Luís de Sousa
Morada	ACIN iCloud Solutions, Lda. Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira – Portugal
E-mail geral	info@globaltrustedsign.com

E-mail reportes	report@globaltrustedsign.com
Página de Internet	https://www.globaltrustedsign.com
Telefone	Nacional: 707 451 451[1] Internacional: + 351 291 957 888[2] (Português – Opção 1 / Inglês - Opção 2; GTS - opção 6) [1] Preço máximo a pagar por minuto: 0,09€ (+IVA) para as chamadas originadas nas redes fixas e 0,13€ (+IVA) para as originadas nas redes móveis; [2] Custo de uma chamada internacional para rede fixa, de acordo com o tarifário em vigor.

Sempre que se identifiquem alguns dos motivos para revogação determinados no ponto 4.9.1. devem ser comunicados para os contactos supra ou preferencialmente para o e-mail de reportes.

1.5.3. Entidade Responsável pela Determinação da Conformidade do documento

A Declaração de Práticas de Certificação (DPC) deve ser aplicada internamente, bem como auditada pelo grupo de trabalho Auditor de modo a garantir a sua conformidade. Esta auditoria deve resultar num relatório, que deve ser submetido ao Grupo de Gestão da EC GTS, para aprovação.

1.5.4. Procedimento para Aprovação do documento

A validação desta DPC e todas as correções ou atualizações são executadas pela Administração de Segurança da GTS. Todas as correções ou atualizações são publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definidas. A administração de Segurança da GTS é responsável por determinar quando é que as alterações na DPC levam a uma alteração nos identificadores dos objetos (OID) da DPC. Após validação, a DPC é submetida ao Grupo de Confiança da GTS, que é responsável pela aprovação e autorização das alterações neste tipo de documento.

1.6. Definições e Acrónimos

1.6.1. Definições

Definições	
Termo	**Definição**
Assinatura Eletrónica	Dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar
Assinatura Eletrónica Avançada	Assinatura eletrónica que obedeça aos requisitos: a) Esteja associada de modo único ao signatário b) Permita identificar o signatário c) Seja criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo, e d) Esteja ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados
Autenticação	Processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar
Certificado	Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.
Certificado de Assinatura Eletrónica	Atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo
Certificado de Autenticação de Sítio Web	Atestado que torne possível autenticar um sítio web e associe o sítio web à pessoa singular ou coletiva à qual o certificado tenha sido emitido
Certificado de Selo Eletrónico	Atestado eletrónico que associa os dados de validação do selo eletrónico a uma pessoa coletiva e confirma o seu nome
Certificado Qualificado de Assinatura Eletrónica	Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Autenticação de Sítios Web	Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Selo Eletrónico	Certificado de selo eletrónico emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III do Regulamento europeu 910/2014
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves

Definições	
Termo	**Definição**
Credenciação	Ato pelo qual é reconhecido a um prestador de serviços que o solicite e que exerça a atividade de entidade certificadora em conformidade com os requisitos definidos no Regulamento europeu 910/2014.
Criador de um Selo	Pessoa coletiva que cria um selo eletrónico.
Dados de Identificação Pessoal	Conjunto de dados que permita determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa coletiva.
Dados de Validação	Dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico.
Dados para a Criação de um Selo Eletrónico	Conjunto único de dados que seja utilizado pelo criador do selo eletrónico para criar um selo eletrónico.
Dados para a Criação de uma Assinatura Eletrónica	Conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica.
Dispositivo de Criação de Assinaturas Eletrónicas	*Software* ou *hardware* configurados, utilizados para criar assinaturas eletrónicas.
Dispositivo de Criação de Selos Eletrónicos	*Software* ou *hardware* configurados, utilizados para criar selos eletrónicos.
Dispositivo Qualificado de Criação de Assinaturas Eletrónicas	Dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014.
Dispositivo Qualificado de Criação de Selos Eletrónicos	Dispositivo para a criação de selos eletrónicos que satisfaça *mutatis mutandis* os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014.
Documento Eletrónico	Qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual.
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Entidade Certificadora	Entidade ou pessoa singular ou coletiva credenciada como prestador qualificado de serviços de confiança pela entidade supervisora.
Entidade de Registo	Entidade que aprova os Nomes Distintos (DN) das entidades subordinadas e, mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo.
Entidade Supervisora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Função Hash	Operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função.
Hash ou Impressão Digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais.
HSM	Módulo de segurança criptográfico empregue para armazenar chaves e realizar operações criptográficas de modo seguro.

Definições	
Termo	**Definição**
Identificação Eletrónica	O processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva.
Infraestrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico.
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas.
Meio de Identificação Eletrónica	Uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha.
OID	Identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica.
Organismo de Avaliação da Conformidade	Organismo definido que é acreditado nos termos do regulamento 910/2014 como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados.
Organismo Público	Entidade estatal nacional, regional ou local, um organismo de direito público ou uma associação formada por uma ou mais dessas entidades ou por um ou mais organismos de direito público, ou uma entidade privada mandatada por, pelo menos, uma dessas autoridades, organismos ou associações como sendo de interesse público, ao abrigo de tal mandato.
Parte Confiante	As partes confiantes ou destinatários são pessoas singulares ou entidades que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação de um selo temporal ao datum, ou seja, confiam na veracidade do selo temporal.
Política de Certificado	Conjunto de regras que indica a aplicabilidade do certificado a uma comunidade específica e/ou classe de aplicação com requisitos de segurança comuns
Prestador de Serviços de Confiança	Pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança.
Prestador Qualificado de Serviços de Confiança	Prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora.
Produto	*Hardware* ou *software*, ou componentes pertinentes de hardware ou software, que se destinem a ser utilizados para a prestação de serviços de confiança.

Definições	
Termo	**Definição**
Selo Eletrónico	Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos.
Selo Eletrónico Avançado	Selo eletrónico que obedeça aos requisitos: a) Esteja associado de modo único ao seu criador b) Permita identificar o seu criador c) Seja criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico, e d) Esteja ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dados
Selo Eletrónico Qualificado	Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico.
Selo Temporal Qualificado	Selo temporal que satisfaça os requisitos: a) Vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável, b) Basear-se numa fonte horária precisa ligada à Hora Universal Coordenada, e c) Ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente
Selos Temporais	Dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento.
Serviço de Confiança	Serviço eletrónico geralmente prestado mediante remuneração, que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços, ou b) Na criação, verificação e validação de certificados para a autenticação de sítios web, ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços
Serviço de Confiança Qualificado	Serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento europeu 910/2014.
Serviço de Envio Registado Eletrónico	Serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada.

Definições	
Termo	**Definição**
Serviço Qualificado de Envio Registado Eletrónico	Serviço de envio registado eletrónico que satisfaça os requisitos: a) Serem efetuados por um ou mais prestadores qualificados de serviços de confiança b) Garantirem, com um elevado nível de confiança, a identificação do remetente c) Garantir a identificação do destinatário antes da entrega dos dados d) O envio e a receção dos dados serem securizados por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, de modo a tornar impossível a alteração dos dados de forma não detetável e) Qualquer alteração a que devam ser sujeitos para o seu envio ou receção ser claramente indicada ao remetente e ao destinatário dos dados f) A data e a hora do envio e da receção, assim como as eventuais alterações dos dados, serem indicadas por meio de um selo temporal qualificado.
Signatário	Pessoa singular que cria uma assinatura eletrónica.
Sistema de Identificação Eletrónica	Sistema de identificação eletrónica ao abrigo do qual sejam produzidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem pessoas coletivas.
Titular	Ver Signatário.
Utilizador	Pessoa singular ou coletiva que utiliza a identificação eletrónica ou o serviço de confiança.
Validação	Processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico.
Validação Cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos.

1.6.2. Acrónimos

Acrónimos	
C	*Country*
CN	*Common Name*
DN	Nome Distinto *(Distinguished Name)*
DPC	Declaração de Práticas de Certificação
DR	Decreto Regulamentar
EC	Entidade Certificadora
ER	Entidade de Registo
GNS	Gabinete Nacional de Segurança
GTS	*Global Trusted Sign*
HSM	Modulo Criptográfico em Hardware (*Hardware Secure Module*)
LRC	Lista de Revogação de Certificados
O	*Organization*
OU	*Organization Unit*
OID	Identificador de Objeto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	Infraestrutura de Chave Pública *(Public Key Infrastructure)*
SSL/TLS	*Secure Sockets Layer / Transport Layer Security*

1.6.3. Referências Bibliográficas

- ✓ Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;

- ✓ ETSI EN 319 411-1 v.1.2.2: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;

- ✓ ETSI EN 319 411-2 v2.2.2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;

- ✓ ETSI 319 412 v1.4.2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

- ✓ ETSI EN 319 401 v2.2.1: General policy requirements for Trust Service Providers;

- ✓ RFC 5280: Internet X.509 Public key Infrastructure Certificate and Certificate and CRL Profile, 2008;

- ✓ RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003;

- ✓ CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4.

1.6.4. Convenções

Não estipulado.

2. Responsabilidade de Publicação e Repositório

2.1. Repositórios

A EC GTS disponibiliza um repositório, em ambiente web, de informação relativa às práticas adotadas e o estado dos certificados emitidos, nomeadamente:

a) Entidade Certificadora Raiz da GTS (ROOT CA GTS)

- Certificado da ROOT CA GTS;
- Lista de Revogação de Certificados (LRC) da ROOT CA GTS;
- Declaração de Práticas de Certificação (DPC) da ROOT CA GTS;
- Políticas de Certificados (PC) da ROOT CA GTS;
- Outra informação relevante.

b) Entidade Certificadora da GTS (EC GTS)

- Certificado da EC GTS;
- Lista de Revogação de Certificados (LRC) da EC GTS;
- Declaração de Práticas de Certificação (DPC) da EC GTS;
- Políticas de Certificados da EC GTS;

- Outra informação relevante.

c) Entidade Certificadora de Selos Temporais da GTS (EVC GTS)

- Certificado da EVC GTS;
- Declaração de Práticas de Certificação (DPC) da EVC GTS;
- Políticas de Certificados da EVC GTS;
- Outra informação relevante.

d) Entidade Certificadora Não Qualificada da GTS (EC NQ GTS)

- Certificado da EC NQ GTS;
- Lista de Revogação de Certificados (LRC) da NQ EC GTS;
- Declaração de Práticas de Certificação (DPC) da EC GTS;
- Políticas de Certificados da EC NQ GTS;
- Outra informação relevante.

2.2. Publicação da Informação

O repositório das diversas entidades certificadoras pode ser acedido 24x7 em https://pki.globaltrustedsign.com/index.html e em https://pki02.globaltrustedsign.com/index.html.
O repositório será atualizado sempre que haja uma alteração num dos documentos publicados.

2.3. Periodicidade de Publicação

A EC GTS efetua as seguintes publicações, com a seguinte periocidade:

- O certificado da EC GTS é publicado após a sua emissão;
- A LRC é publicada trimestralmente;
- Novas versões ou alterações nas DPC e/ou respetivas Políticas de Certificados (PC), serão publicadas após a sua aprovação pelo Grupo de Gestão.

2.4. Controlos de Acesso aos Repositórios

Foram implementados os seguintes mecanismos de controlo de acesso de segurança:

- Quaisquer alterações à informação publicada no repositório são efetuadas através de processos formais de gestão documental;
- A infraestrutura tecnológica que suporta o repositório e a sua publicação encontra-se em conformidade com as boas práticas de segurança da informação, incluindo os requisitos físicos bem como a gestão por uma equipa com as competências necessárias para a função;

- É garantido que o acesso à informação contida nos repositórios se efetua, apenas e só, em modo de leitura. Para tal, foram implementados mecanismos de segurança de forma a garantir que apenas pessoas autorizadas possam escrever ou modificar a informação contida nos repositórios.

3. Identificação e Autenticação

3.1. Atribuição de Nomes

A EC GTS garante a emissão de certificados contendo um *Distinguished Name* (DN) X.509 a todos os titulares que submetam documentação contendo um nome verificável de acordo com o preconizado no RFC 5280. A atribuição de nomes segue as convenções seguintes:

- Certificados de autenticação de sítios web é atribuído o nome qualificado do domínio e/ou do serviço de confiança, de acordo com a ETSI EN 319 412-4 v1.1.1;
- Certificados de assinatura qualificada para pessoa singular é atribuído o nome real do titular, de acordo com a ETSI EN 319 412-2 v2.2.1;
- Certificados de assinatura qualificada para pessoa singular em associação com uma pessoa coletiva é atribuído o nome do titular e a sua relação com a pessoa coletiva, de acordo com a ETSI EN 319 412-2 v2.2.1;
- Certificados de selos eletrónicos é atribuído o nome da pessoa coletiva, de acordo com a ETSI EN 319 412-3 v1.2.1.

A atribuição dos nomes cumpre os requisitos especificados nas políticas de certificados, estando nestas a identificação em cada uma das políticas:

Identificador da Política	OID
Política de Certificados da Root CA GTS	1.3.6.1.4.1.50302.1.1.2.1.1.0
Política de Certificados SSL EV	1.3.6.1.4.1.50302.1.1.2.2.1.0
Política de Certificados SSL OV	1.3.6.1.4.1.50302.1.1.1.2.1.1
Política de Certificados para Assinatura Qualificada	1.3.6.1.4.1.50302.1.1.1.2.1.2
Política de Certificados para Selos Eletrónicos	1.3.6.1.4.1.50302.1.1.1.2.1.3
Política de Certificados para Assinaturas Avançadas	1.3.6.1.4.1.50302.1.1.2.6.1.0
Política de Certificados para Selos Eletrónicos Avançados	1.3.6.1.4.1.50302.1.1.2.7.1.0
Política de Certificados para Selos Temporais	1.3.6.1.4.1.50302.1.1.2.3.1.0

3.1.1. Tipos de Nomes

A EC GTS garante que, a atribuição dos nomes, cumpre os requisitos especificados nas políticas de certificados para cada tipo de perfil apresentado. Os vários tipos de certificados podem conter os seguintes campos no DN:

Atributo	Código	Regras
Country	C	Código do país do titular do certificado
Organization	O	Este campo corresponde à organização (ou equivalente) à qual o titular do certificado pertence.
Organization Unit	OU	Este campo corresponde informação relativa à unidade organizativa (ou equivalente) a que o titular do certificado pertence.
Common Name	CN	Nome único do titular do certificado. No caso dos servidores de sítios Web, este será designado pelo FQDN (CN = "FQDN".), sendo proibida a sua designação através do endereço IP ou domínios locais. No caso dos certificados de assinatura qualificada, contém o nome do titular ou o seu pseudónimo. No caso dos certificados de selos eletrónicos, contém o nome da pessoa coletiva.
Serial Number	serialNumber	Segue as recomendações do ETSI EN 319 412.

3.1.2. Necessidade de Nomes Significativos

A EC GTS assegura que os nomes utilizados nos certificados por ela emitidos identificam de uma forma significativa e clara os seus titulares, assegurando que o DN usado é apropriado para um dado titular e que a componente ***Common Name*** do DN o representa de forma a ser facilmente identificável pelos interessados. A CA GTS assegura que qualquer campo ***Common Name*** no Subjet DN do certificado, é igual a um dos FQDN ***Subject Alternative Names***, que foi validado, utilizando pelo menos um dos procedimentos da secção 3.2.2.4 das Baseline Requirements CA/B Forum.

3.1.3. Anonimato ou Pseudónimo de Titulares

A EC GTS não permitido o anonimato de titulares no processo de emissão de certificados.

3.1.4. Interpretação de Formato de Nomes

As regras utilizadas pela EC GTS para interpretar o formato de nomes suguem o estabelecido no *RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* garantindo assim que todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado são

codificados numa UTF8String, com exceção dos atributos country e serialnumber que são codificados numa *PrintableString*.

3.1.5. Unicidade de Nomes

Na EC GTS, existem controlos que garantem que o DN e o conteúdo da extensão *Key Usage* são únicos, não ambíguos e referentes apenas a uma entidade, garantindo, assim, a rejeição de emissão de certificados emitidos por esta que, tendo o mesmo nome único, identifiquem entidades distintas.

3.1.6. Reconhecimento, Autenticação e Função das Marcas Registadas

Os DN emitidos pela EC GTS são únicos para cada titular e têm em atenção as marcas registadas, não permitindo a utilização deliberada de nomes registados cuja entidade não possa provar ter direito à marca, podendo-se recusar a emitir o certificado com nomes de marcas registadas se concluir que outra identificação seja mais conveniente. Antes da emissão do certificado, no procedimento de autenticação, a entidade/titular terá de apresentar documentos que demonstram o direito à utilização do DN requisitado.

3.2. Validação de Identidade no Registo Inicial

Para que os certificados qualificados das entidades certificadoras possam ser emitidos na hierarquia de confiança da GTS, é obrigatório que a EC GTS verifique o pedido e os parâmetros associados ao mesmo.

3.2.1. Método de Prova da Posse da Chave Privada

Nos casos em que a EC GTS não seja a entidade responsável pela geração do par de chaves criptográficas a atribuir ao utilizador, esta, antes de proceder à sua emissão, assegurará que o utilizador possui a chave privada correspondente à chave pública constante no pedido de certificado.
O método de prova será necessariamente tão mais complexo e preciso consoante a importância do tipo de certificado pedido, encontrando-se documentado na Política de Certificado do certificado em causa.

3.2.2. Autenticação de Identidade da Organização e Domínio

O DN emitidos pela EC GTS têm em atenção as marcas registadas, não permitindo a utilização deliberada de nomes registados cuja entidade não possa provar ter direito à marca, podendo-se recusar a emitir o certificado com nomes de marcas registadas se concluir que outra identificação seja mais conveniente. A EC GTS valida a autenticidade dos dados através de uma das seguintes formas:

a) Utilizando documentos emitidos por entidades governamentais (Registo Comercial, Certidão Permanente etc.);
b) Autenticação do formulário de pedido de certificado que contém os dados da organização, por uma entidade legal com poderes para tal ato (advogado, notário ou solicitador);
c) Uma base de dados de terceiros atualizada periodicamente;
d) Método de Prova de Controlo de Endereço de Email

   Quando é incluído um endereço de email nos atributos ***Distinguished Name*** ou ***Subject Alternative*** Name de um certificado digital, o subscritor deve provar que controla o endereço de email. Para isso, a EC GTS realiza um procedimento de desafio-resposta, que consiste em gerar um token e enviá-lo por email para o endereço de email a ser incluído no certificado. Para comprovar o controlo do endereço de email, o subscritor clica no link que contém o token, que consta no email. A EC recebe a resposta e a prova de controlo de endereço de email é concluída com sucesso;

   Este procedimento também é realizado para confirmar o endereço de email do subscritor incluído no formulário de pedido de certificado (contacto de email do subscritor);
e) Método de Validação de Nome de Domínio / Endereço

   A EC GTS valida o direito de uso ou controlo por parte do requerente do nome de domínio / endereço IP, que será listado nos campos ***Common Name*** e ***Subject Alternative Name*** do certificado, utilizando pelo menos um dos procedimentos da secção 3.2.2.4 das Baseline Requirements CA/B Forum.

3.2.2.1. Identidade

Antes da emissão e disponibilização de um certificado emitido para uma pessoa coletiva ou singular com atributo de associação com uma entidade, é necessário autenticar os dados relativos à constituição e pessoa jurídica da entidade.

Para esses certificados, a identificação da entidade é exigida em todos os casos, para os quais a AR exigirá a documentação pertinente dependendo do tipo de entidade.

A documentação relevante pode ser encontrada no site da Globaltrustedsign, na seção de informações do certificado correspondente.

No caso de entidades fora do território português, a documentação a apresentar será a do Registo Oficial do respetivo país, devidamente apostilado e oficialmente traduzido para português ou inglês, sempre que existam dúvidas relativamente à documentação ou à entidade.

Na emissão de certificados de componentes SSL OV / EV, a existência da entidade é verificada nos registros públicos (https://eportugal.gov.pt), através da consulta aos dados do InformaDB (https://www.informadb.pt/) ou nas bases de dados da autoridade tributária (https://www.portaldasfinancas.gov.pt/).

Para os certificados EV a atividade operacional da entidade é verificada de forma confiável, bem como a qual categoria de entidade ela pertence de acordo com a classificação estabelecida nas políticas definidas pelo CA/Browser Forum en "Guidelines For The Issuance And Management Of Extended Validation Certificates" (Private Organization, Government Entity, Business Entity and Non-Commercial Entity).

Esta verificação é realizada através de uma análise ao regime jurídico aplicável a entidade requerente e através da consulta dos registos da atividade empresarial do mercado ou pela entrega física das escrituras notariais que comprovem toda a informação.

Além disso, é também verificado:

- Que os dados ou documentos fornecidos estejam dentro do prazo de validade.
- Que a existência legal da organização é de pelo menos 1 ano.
- Que não sejam empresas erradicadas em países onde há proibição governamental de fazer negócios ou fazem parte de uma lista relacionada com risco de BCFT.

3.2.2.2. Marcas registradas

Ver ponto 3.1.6.

3.2.2.3. Verificação do pais

Ver ponto 3.2.2.

3.2.2.4. Validação de autorização ou controle de domínio

Para cada **domínio**, é confirmado que o requerente tem controle sobre o referido domínio, mediante uma verificação no registo em https://www.whois.net e/ou https://www.dns.pt

3.2.2.5. Autenticação de um endereço IP

Para cada endereço IP, é confirmado que o requerente tem controle sobre o referido endereço, mediante uma verificação no registo em https://www.ripe.net ou https://whois.arin.net/

3.2.2.6. Validação do domínio Wildcard

A GTS não emite certificados do tipo Wildcard.

3.2.2.7. Exatidão de fontes de dados

A GTS dispõe de uma lista de fontes fidedignas para analisar os dados previamente à emissão dos certificados.

3.2.2.8. Registos CAA

A verificação do Registos CAA é realizada através da ferramenta https://www.entrustdatacard.com/products/categories/ssl-certificates/caa-tool
Para informações adicionais por favor verificar o ponto 4.2.1.

3.2.3. Autenticação de Identidade do Indivíduo

A verificação da identidade dos subscritores e/ou titulares será efetuada pelo grupo de trabalho de Administradores, após a confirmação do pagamento e validação documental, e pode ser realizada das seguintes formas:

- De forma presencial, em português ou em inglês, (Sede da empresa na Ilha Madeira, nas instalações da empresa em: Lisboa, Porto e Ponta Delgada), mediante agendamento, acompanhado do documento de identificação original, estando presentes neste ato dois administradores de registo (alínea a, do n.º 1, do artigo 24º do Reg.910/2014), ou;

- À distância, utilizando meios de identificação eletrónica, por meio de videoconferência, em português ou em inglês, (através de software certificado para o efeito), mediante agendamento, assegurando a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva, com a presença do documento de identificação original, antes da emissão do certificado qualificado, cumprindo com os requisitos estabelecidos no artigo 8.º do regulamento 910/2014 relativamente aos níveis de garantia «substancial» ou «elevado» e o Despacho 154/2017 do GNS, (alínea b, do n.º 1, do artigo 24º do Reg.910/2014), ou

- Com recurso ao certificado autenticação do cartão de cidadão e/ou chave móvel digital, através do portal autenticacao.gov.pt (disponível apenas a cidadãos portugueses, com documentos /certificado digital compatível), ou

- Por meio de um certificado de assinatura eletrónica qualificada ou de um selo eletrónico qualificado emitido nos termos da alínea anterior (alínea c, d, do n.º 1, do artigo 24º do Reg.910/2014), aplicável a renovações.

a) Identificação de Pessoa Singular

Se o titular é uma pessoa singular, a identidade poderá ser verificada através de:

- Nomes próprios e Apelido (de acordo com as práticas para identificação de pessoas);
- Data e local de nascimento;
- Documento de identificação reconhecido que permita distinguir o titular de outros com o mesmo nome;
- Documento com valor probatório equivalente à presença física;

Se o titular é uma pessoa singular em associação com uma pessoa coletiva:

- Nomes próprios e Apelido (de acordo com as práticas para identificação de pessoas);
- Data e local de nascimento;
- Documento de identificação reconhecido que permita distinguir o titular de outros com o mesmo nome;
- Documento com valor probatório equivalente à presença física;
- Nome completo e dados sobre a pessoa coletiva;
- Evidência da associação da pessoa singular com a pessoa coletiva que irá aparecer nos atributos do certificado.

Se o titular é uma pessoa singular do Tipo Profissional:

- Nomes próprios e Apelido (de acordo com as práticas para identificação de pessoas);
- Data e local de nascimento;
- Documento de identificação reconhecido que permita distinguir o titular de outros com o mesmo nome;
- Documento com valor probatório equivalente à presença física;
- Indicação com evidência da Profissão que exerce;
- N.º de Ordem a qual pertence com envio de evidência;
- Organização / Entidade onde exerce a profissão com envio de evidência.

b) Identificação de Pessoa Coletiva

Se o titular é uma pessoa coletiva de representação, a identidade poderá ser verificada através de:

- Nomes próprios e Apelido do requerente (de acordo com as práticas nacionais para identificação de pessoas);
- Data e local de nascimento;
- Documento de identificação reconhecido nacionalmente que permita distinguir o titular de outros com o mesmo nome;
- Documento com valor probatório equivalente à presença física;
- Dados da pessoa coletiva:
  - Nome completo da pessoa coletiva;
  - Morada;
  - Identificação Fiscal (NIPC);
  - Código de Acesso da Certidão Permanente (caso se aplique) ou ata de tomada de posse, acompanhada por estatutos;
- Caso o requerente não seja um representante legal da pessoa coletiva, procuração de poderes de emissão do selo eletrónico.

Se o titular é uma pessoa singular em associação com uma pessoa coletiva do tipo profissional:

- Nomes próprios e Apelido (de acordo com as práticas nacionais para identificação de pessoas);
- Data e local de nascimento;
- Documento de identificação reconhecido nacionalmente que permita distinguir o titular de outros com o mesmo nome;
- Documento com valor probatório equivalente à presença física;
- Nome completo e dados sobre a pessoa coletiva;
- Evidência da associação da pessoa singular com a pessoa coletiva que irá aparecer nos atributos do certificado;
- N.º de Ordem a qual pertence com envio de evidência;
- Função/Cargo que desempenha;
- Área / Departamento da organização à qual pertence.

c) Identificação de Dispositivo ou Sistema

O processo de registo e autenticação será assegurado pelo grupo de trabalho de Administradores de Registo com o objetivo de registar corretamente os utilizadores finais do certificado, usando todos os meios necessários para uma identificação correta e legal do requerente. Entre as operações a realizar para atingir este objetivo contam-se as seguintes:

- Verificar documentos oficialmente reconhecidos pelo Estado em que o subscritor (individual ou organização) está registado:
- O nome completo;
- Os dados de contato, incluindo o endereço de contacto;
- A sua identificação única legal.

A identificação deverá ser autenticada com provas identificativas que devem estar de acordo com as provisões seguintes:

- Ser oficialmente reconhecidas na jurisdição em que o subscritor está registado;
- Indicar o nome completo do subscritor e o seu endereço oficial;
- Ter pelo menos uma prova de identidade que contenha uma fotografia do subscritor;
- Indicar um número de registo único dentro da jurisdição em que tiver sido emitido.

A GTS verificará se cada candidato tem o direito ou privilégio para a obtenção do certificado em questão. Para que os certificados qualificados de autenticação de sítios web com *extended validation* possam ser emitidos na hierarquia de confiança da GTS, é obrigatório que a EC GTS verifique a identidade e o endereço da entidade coletiva requerente, e que o endereço indicado seja o do pacto social, ou onde a sua atividade se realiza.

3.2.4. Informação de Subscritor/Titular Não Verificada

Toda a informação do certificado é verificada.

3.2.5. Validação de Autoridade

Consultar Autenticação de Identidade da Organização e Domínio, secção 3.2.2 e Autenticação de Identidade do Indivíduo, secção 3.2.3.

3.2.6. Critérios para Interoperabilidade ou Certificação

Os certificados emitidos na PKI GTS são emitidos debaixo de uma só hierarquia de confiança.
Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se (mas não se obriga) a que apenas caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') sejam utilizados em entradas do Diretório X.500.

3.3. Identificação e Autenticação para Pedidos de Renovação de Chave

3.3.1. Identificação e Autenticação para Pedidos de Rotina de Renovação de Chave

Muitas infraestruturas de chave pública permitem a atualização automática de certificados para um subscritor antes do fim do período de validade do certificado existente. Esta ação é conhecida como renovação de rotina e é possível no momento em que já existe uma relação de confiança com o subscritor. A renovação é tratada como um novo pedido de emissão pela EC GTS.

3.3.2. Identificação e Autenticação para Renovação de Chaves após Revogação

A renovação é tratada como um novo pedido de emissão pela EC GTS. A GTS requer ao subscritor que use os mesmos detalhes de autenticação usados no pedido original de pedido de certificado.

3.4. Identificação e Autenticação para Pedido de Revogação

O pedido de revogação deve obedecer às condições descritas em pormenor na secção 4.10.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

4.1. Pedido de Certificado

Um pedido de emissão de certificados à EC GTS inicia-se com o preenchimento de um formulário, desenhado para cada tipo de certificado suportado e com a aceitação dos termos e condições

estabelecidos pela EC GTS, devidamente assinados pelo titular de forma manuscrita e que, neste caso, pressupõe o envio dos documentos originais por CTT para a GTS ou de forma digital, com recurso a assinatura qualificada.

4.1.1. Quem Pode Submeter um Pedido de Certificado

Os pedidos de subscrição de certificados podem ser submetidos pelos seguintes:

- O titular do certificado;
- Um representante do titular do certificado, devidamente autorizado e com poderes para o efeito;
- Uma pessoa coletiva que seja titular do certificado;
- Um representante da GTS.

4.1.2. Processo de Registo e Responsabilidades

Após a receção da documentação, dá-se início a um processo de validação da informação e identidade do titular e quando aplicável entidade requerente. Este processo é executado sempre por 2 Administradores de Registo, com o fim de verificar a autenticidade dos dados fornecidos, dependendo do tipo de certificado solicitado. A GTS não utiliza entidades de registo externas para fornecimento do serviço de registo. No caso dos certificados Web/SSL, o formulário deverá ser acompanhado aquando a sua submissão, de um CSR (Certificate Signing Request) que deve conter informação para os campos do certificado, que devem coincidir com os campos inseridos no formulário.
Nota: O pedido de certificado não implica a sua obtenção se o solicitante não cumprir os requisitos estabelecidos nesta DPC. Os pedidos efetuados aceites ou rejeitados serão arquivados e mantidos por um período mínimo de 7 anos de acordo com o CAB Fórum secção 5.5.2.

4.2. Processamento do Pedido de Certificado

4.2.1. Desempenho de Funções de Identificação e Autenticação

A GTS, assim que rececione o formulário de pedido de emissão de certificado, bem como a informação necessária à emissão do pedido, procederá à validação de toda a informação disponibilizada a fim de verificar a autenticidade dos dados. Nos pedidos de certificados para Autenticação de Website, a GTS efetua ainda verificações do CAA records relevantes no momento de submissão do pedido de certificado e imediatamente antes da emissão do certificado. A EC atua de acordo com os CAA *records*, caso existam. O domínio de identificação da EC GTS nos CAA *records* é globaltrustedsign.com. A CA GTS limita a reutilização da informação de suporte para renovação do certificado, de acordo com ponto "11.14.3- Age of Validated Data" do documento Guidelines for the Issuance and Management of Extended Validation Certificates do CA/ Browser Forum.

4.2.2. Aprovação ou Rejeição de Pedidos de Certificados

Os pedidos de certificados serão aceites, apenas se, todos os dados do pedido forem autênticos. No caso das informações contantes do processo de avaliação o pedido será rejeitado, sendo o responsável pelo mesmo informado.

4.2.3. Prazo para Emissão do Certificado

A GTS tem 60 minutos após validação da identidade e idoneidade do subscritos e boa cobrança para proceder com a emissão e envio do certificado de autenticação web. Para os restantes pedidos, encontra-se definido nos respetivos termos e condições o prazo para emissão de certificado – FO31 – termos e condições gerais.

4.3. Emissão de Certificados

O processo de emissão de certificados é executado pelos Administradores de Registo na EC GTS através de uma cerimónia própria para o efeito. Os certificados são emitidos por interação da EC GTS com um módulo criptográfico em *hardware* (*Hardware Secure Module* - HSM). O certificado emitido inicia a sua vigência no momento da sua emissão. No caso dos certificados para autenticação de sítios web, o certificado emitido inicia a sua vigência no momento da sua emissão.

4.3.1. Ações da EC durante a Emissão do Certificado

O processo de emissão de certificados é sempre levado a cabo por dois Administradores de Registo, por forma a garantir a dupla autenticação. Só desta forma é validada e confirmada a autenticidade dos dados fornecidos.

Os certificados qualificados de e-seal e de assinatura, são emitidos por interação da Entidade Certificadora com um módulo criptográfico em hardware (Hardware Secure Module - HSM), tendo por base o tipo de política de certificado aplicável. O certificado de chave pública é armazenado no HSM. No caso dos certificados para autenticação de sítios web (OV ou EV), o certificado emitido inicia a sua vigência no momento da sua emissão e o subscritor do certificado é notificado via correio eletrónico, sendo-lhe enviado, por este canal, o certificado de chave pública. O envio do certificado requer uma aceitação que é feita de acordo com a secção 4.4. Não serão aceites terminologias não reconhecidas pela ICANN (Internet Corporation for Assigned Names and Numbers), para aceitação de certificados de sítios web.

No caso dos certificados de assinatura qualificada ou selo eletrónico qualificados, a emissão do certificado é efetuada pelo titular do mesmo após verificação da identidade do titular no momento da emissão através de:

- Credenciais de acesso ao Portal da GTS;
- Receção do código OTP para o email configurado no registo do titular.

Os titulares dispõem de 180 dias para emitir qualquer tipo de certificado sob pena de ter que repetir a videoconferência. Os Certificados avançados são emitidos pelos administradores de registo e ficam disponíveis para download na área pessoal do portal GTS, uma vez realizada a autenticação. Para a utilização do certificado será enviado por sms um pin, para o número de telemóvel identificado pelo próprio titular para o efeito aquando a realização da compra do produto. Este certificado pode ser descarregado quantas vezes for necessário.

4.3.2. Notificação ao Subscritor/Titular pela EC Emissora do Certificado

O subscritor do certificado é notificado via correio eletrónico, sendo-lhe enviado, por este canal, o certificado de chave pública.

4.4. Aceitação do Certificado

4.4.1. Conduta que constitui a Aceitação do Certificado

Antes do envio do certificado de chave pública, o subscritor e titular terão de aceitar as condições de utilização do certificado, considerando-se, assim o mesmo como aceite. Perante o certificado emitido, subscritor deve ser uma entidade consciente dos tópicos seguintes:

- O conhecimento das funcionalidades e conteúdo do certificado;
- O conhecimento dos direitos e responsabilidades.

4.4.2. Publicação do Certificado pela EC

A EC GTS não efetua a publicação de certificados emitidos.

4.4.3. Notificação de Emissão de Certificados pela EC a outras Entidades

A EC GTS não notifica outras entidades da emissão dos mesmos.

4.5. Utilização do Certificado e Par de Chaves

4.5.1. Utilização do Certificado e Par de Chaves pelo Subscritor/Titular

Os titulares de certificados utilizam a sua chave privada apenas, e só, para o fim a que estas se destinam (conforme estabelecido no campo do certificado "keyUsage") e sempre com propósitos legais. A utilização do certificado é sempre da responsabilidade do seu titular.

A utilização do certificado apenas é permitida, e caso aplicável para o tipo de certificado em questão:

- A quem estiver designado no campo do certificado *Subject*;
- Depois de aceitar os termos e condições associados ao tipo de certificado;
- Enquanto o certificado se mantiver válido e não estiver na LRC da EC GTS.

4.5.2. Utilização do Certificado e Chave Pública por Partes Confiantes

As partes confiantes devem utilizar um software em conformidade com os standards X.509 e devem confiar no certificado apenas se este não estiver expirado ou revogado. A EC GTS fornece nesta DPC informação sobre os serviços apropriados disponíveis para verificar o estado de validade do certificado, tais como OCSP e CRL.

4.6. Renovação de Certificado

Para realizar a renovação do seu certificado, se as funções e informações, para as quais o certificado inicial foi emitido se mantiverem, apenas terá de solicitar a renovação do seu certificado com os mesmos dados e efetuar pagamento de renovação seguindo as indicações que lhe serão enviadas pela GTS. Este processo obriga a uma nova geração de um par de chaves, e respetivo certificado.

4.6.1. Circunstâncias para a Renovação do Certificado

Se um titular pretender renovar um certificado é desencadeado um procedimento para cada um dos seguintes casos:

Motivo para Renovação	Procedimento de Renovação
O certificado foi revogado	(*i*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com os mesmos campos exceto a chave pública.
O titular pretende prolongar a validade do certificado	(*i*) O antigo certificado é revogado. (*ii*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com os mesmos campos exceto a chave pública.
A informação que deu origem ao certificado sofre alterações	(*i*) O antigo certificado é revogado. (*ii*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com as alterações necessárias incluindo a nova chave pública.

A renovação de certificados utiliza os procedimentos de autenticação e identificação inicial que resultam na geração de novos pares de chaves.

4.6.2. Quem pode Submeter o Pedido de Renovação do Certificado

Podem solicitar a renovação de certificados, os Subscritores/Titulares nas condições estabelecidas no ponto 4.6.1.

4.6.3. Processamento do Pedido de Renovação de Certificado

O processamento do pedido de renovação de certificado, executa-se conforme descrito no ponto 4.6.1.

4.6.4. Notificação de Emissão de Renovação de Certificado ao Titular

A EC GTS notifica o Subscritor, tipicamente por email, em tempo razoável após a emissão do certificado, e pode usar qualquer mecanismo confiável para entregar o certificado ao Subscritor.

4.6.5. Conduta que Constitui a Aceitação de Renovação do Certificado

Os certificados renovados são considerados aceites sete (7) dias após a sua emissão ou notificação da emissão do certificado ao Subscritor, ou quando exista evidência de que o Subscritor utilizou o certificado.

4.6.6. Publicação da Renovação do Certificado pela EC

Não estipulado.

4.6.7. Notificação da Renovação ao Certificado a Outras Entidades

Ver secção 4.4.3.

4.7. Re-Key do Certificado

4.7.1. Circunstâncias para o Re-Key de Certificado

O processo de Re-Key de um certificado não é suportado pela EC GTS.

4.7.2. Quem pode Solicitar a Certificação de uma nova Chave Pública

Não estipulado.

4.7.3. Processamento de Pedidos de Re-Key de Certificado

Não estipulado.

4.7.4. Notificação de Nova Emissão de Certificado ao Subscritor/Titular

Não estipulado.

4.7.5. Conduta que constitui a aceitação do Certificado para o qual foi feito o Re-Key

Não estipulado.

4.7.6. Publicação do Certificado pela EC para o qual foi feito Re-Key

Não estipulado.

4.7.7. Notificação de Emissão de Certificado pela EC a Outras Entidades

Não estipulado.

4.8. Modificação do Certificado

A modificação de certificado é um processo através do qual o certificado é emitido para um Subscritor ou Patrocinador mantendo as mesmas chaves, com alterações apenas na informação do certificado. A modificação de certificados não é suportada pela EC GTS.

4.8.1. Circunstâncias para a Modificação do Certificado

Não estipulado.

4.8.2. Quem Pode Solicitar a Modificação do Certificado

Não estipulado.

4.8.3. Processamento de Pedidos de Modificação do Certificado

Não estipulado.

4.8.4. Notificação de Nova Emissão ao Subscritor/Titular

Não estipulado.

4.8.5. Conduta que Constitui a aceitação de Certificado Modificado

Não estipulado.

4.8.6. Publicação do Certificado Modificado pela EC

Não estipulado.

4.8.7. Notificação de Emissão de Certificado pela EC a Outras Entidades

Não estipulado.

4.9. Revogação e Suspensão do Certificado

A revogação de certificados são mecanismos a utilizar quando, por algum motivo, os certificados deixam de ser fiáveis antes do período de finalização originalmente previsto. Na prática, a revogação de certificados é uma ação através da qual, o certificado deixa de estar válido antes do fim do seu período de validade, perdendo, deste modo, a sua operacionalidade. A suspensão de certificados não é suportada pela EC GTS.

4.9.1. Motivos para Revogação

4.9.1.1. Motivos para a revogação do certificado de um subscritor

a) Um certificado deve ser revogado em 24 horas por uma das seguintes razões:

- O Subscritor solicita por escrito que a EC revogue o Certificado;

- O Subscritor notifica à EC que o pedido de certificado inicial não foi autorizado e não concede a autorização de forma retroativa;
- Comprometimento ou suspeita de comprometimento das chaves privada do titular;
- Comprometimento ou suspeita de comprometimento da senha de acesso ao certificado;
- A EC é informada de um método demonstrado ou comprovado que pode facilmente calcular a Chave Privada do Assinante com base na Chave Pública no Certificado;
- A EC obtém evidências de que a validação da autorização ou controle de domínio para qualquer nome de domínio totalmente qualificado ou endereço IP no certificado não deve ser considerada;
- Comprometimento ou suspeita de comprometimento das chaves privada da ROOT CA GTS;
- Utilização do certificado para atividades abusivas.

b) A EC pode revogar um certificado dentro de 24 horas, todavia deve revogar um certificado no prazo de 5 dias se um ou mais dos seguintes motivos ocorrerem:

- O Certificado não está mais em conformidade com os requisitos da Seção 6.1.5 e da Seção 6.1.6;
- A EC obtém provas de que o Certificado foi mal utilizado;
- Cessação de funções;
- Inexatidões ou alterações nos dados fornecidos;
- A EC é informada de que o Subscritor violou uma ou mais das suas obrigações materiais ao abrigo dos Termos e Condições de Utilização;
- A EC é informada de qualquer circunstância que indique que a utilização de um Nome de Domínio ou endereço IP totalmente qualificado no Certificado já não é legalmente permitida (por exemplo, um tribunal ou árbitro revogou o direito de um Registrador de Nome de Domínio de utilizar o Nome de Domínio, ou um acordo de licença ou de serviços relevante entre o Registrador de Nome de Domínio e o requerente cessou, ou o Registrador de Nome de Domínio não renovou o Nome de Domínio);
- Incumprimento por parte da ROOT CA GTS ou titular das responsabilidades prevista na DPC;
- A EC é informada de que o Certificado não foi emitido em conformidade com estes Requisitos ou com a Política de Certificados ou Declaração de Práticas de Certificação da EC;
- A EC determina ou é informada de que qualquer das informações que aparecem no Certificado é inexata;

- Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- O direito da EC de emitir certificados ao abrigo destes Requisitos expirou ou foi revogado ou terminado, a menos que a EC tenha tomado medidas para continuar a manter o Repositório CRL/OCSP;
- A CA está ciente de que um Assinante violou uma ou mais de suas obrigações materiais sob o Contrato de Assinante ou Termos de Uso;
- A revogação é exigida de acordo com a Política de Certificados e/ou Declaração de Práticas de Certificação da EC;
- Sempre que seja determinado que, por alguma razão, os certificados não foram emitidos de acordo com a Política de Certificados ou Declaração de Práticas de Certificação da GTS;
- A EC é informada de um método demonstrado ou comprovado que põe a Chave Privada do Assinante em risco ou se houver provas claras de que o método específico utilizado para gerar a Chave Privada apresentava falhas;
- Por resolução judicial ou administrativa;
- Sempre que a CA GTS receba notificação ou tenha conhecimento implícito de qualquer circunstância que indique que o endereço de email do certificado deixou de estar legalmente autorizado.

4.9.1.2. Motivos para a revogação do certificado subordinado da CA

A EC Emissora DEVERÁ revogar um Certificado da EC Subordinada num prazo de sete (7) dias se uma ou mais das seguintes situações ocorrer:

- A EC Subordinada solicita a revogação por escrito;
- A EC Subordinada notifica à EC Emissora que o pedido de certificado original não foi autorizado e não concede a autorização com efeitos retroativos;
- A EC Emissora obtém provas de que a Chave Privada da EC Subordinada correspondente à Chave Pública no Certificado sofreu um Compromisso de Chave ou deixou de cumprir os requisitos da Secção 6.1.5 e da Secção 6.1.6;
- A EC Emissora obtém provas de que o Certificado foi mal utilizado;
- A EC Emissora é informada de que o Certificado não foi emitido em conformidade ou que a EC Subordinada não cumpriu com este documento ou com a Política de Certificado ou Declaração de Práticas de Certificação aplicável;
- A EC Emissora determina que qualquer informação no certificado é imprecisa ou enganosa.

4.9.2. Quem pode Solicitar a Revogação

Um pedido de revogação pode ser efetuado de forma legítima por um dos seguintes intervenientes:

- O titular do certificado;
- A Entidade Certificadora ou Entidade Requerente do certificado da entidade subordinada;
- A GTS, no conhecimento de que:
  - Os dados constantes no certificado não correspondem à realidade;
  - O certificado não esteja na posse do seu titular;
- A Entidade Supervisora;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

4.9.3. Procedimento para o Pedido de Revogação

O Pedido de Revogação deve ser efetuado através do serviço disponibilizado para o efeito em https://www.globaltrustedsign.com. A EC GTS irá processar o pedido de revogação nas 24 horas seguintes às da receção do pedido. Nesse intervalo de tempo, será verificada a identidade e autenticidade de quem solicitou a revogação do certificado.

4.9.4. Período de Carência do Pedido de Revogação

O período de carência do pedido de revogação é o tempo disponível para o Subscritor tomar as ações necessárias para pedir a revogação de um certificado sobre o qual tenha suspeita de comprometimento da chave, descoberta de informação imprecisa contida no certificado ou informação desatualizada. Nesta situação, o Subscritor deve pedir a revogação no prazo de 24 horas após a sua deteção.

4.9.5. Tempo de Processamento do Pedido de Revogação pela EC

Após a confirmação da identidade e autenticidade do requerente, a TSP GTS tem 60 minutos, para transitar o estado do certificado para revogado.

4.9.6. Requisito de Verificação da Revogação pelas Partes Confiantes

Antes de confiar na informação listada num certificado, a Parte Confiante deve validar a adequação do certificado para a finalidade pretendida e garantir que o certificado é válido. Para verificar o estado do certificado, as Partes Confiantes necessitam consultar as respostas OCSP ou CRL identificadas em cada certificado.

4.9.7. Frequência de Emissão de CRL (caso aplicável)

Os estados dos certificados emitidos pela EC GTS podem ser verificados através da consulta da sua CRL. A CRL é atualizada de 6 em 6 horas, sendo emitida a cada 24 horas ou sempre que haja uma revogação dos certificados emitidos, neste caso é emitida uma nova CRL imediatamente. A disponibilização nos repositórios é feita num período não superior a 30 minutos, sendo o seu download feito em menos de 10 segundos. De modo a garantir a sua disponibilidade, a CRL é disseminada nos seguintes repositórios:

- https://pki.globaltrustedsign.com/download/crl/subca/gts_subca_crl.crl
- https://pk2.globaltrustedsign.com/download/crl/subca/gts_subca_crl.crl
- https://pki.globaltrustedsign.com/download/crl/subca/gts_subca_03_crl.crl
- https://pki02.globaltrustedsign.com/download/crl/subca/gts_subca_03_crl.crl
- https://pki.globaltrustedsign.com/download/crl/subca_nq/gts_subcanq02_crl.crl
- https://pki02.globaltrustedsign.com/download/crl/subca_nq/gts_subcanq02_crl.crl
- https://pki.globaltrustedsign.com/download/crl/subca_nq/gts_subnq03.crl
- https://pki02.globaltrustedsign.com/download/crl/subca_nq/gts_subnq03.crl

4.9.8. Latência Máxima para CRL (caso aplicável)

A GTS dispõe recursos suficientes para garantir as condições normais de operação, nomeadamente um tempo de resposta, para a CRL e OCSP, menor ou igual a 10 segundos.

4.9.9. Disponibilidade de Verificação de Estado/Revogação Online

A Global Trusted Sign Root CA dispõe de serviços de validação OCSP do estado dos certificados de forma online. Esse serviço poderá ser acedido em http://ocsp.globaltrustedsign.com

4.9.10. Requisitos de Verificação de Revogação Online

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das LRC ou num servidor de verificação do estado online (via OCSP).
As LRC podem ser acedidas em https://pki.globaltrustedsign.com/index.html, garantindo a sua disponibilidade 24 horas por dia, 7 dias por semana, exceto na ocorrência de alguma paragem de manutenção programada e devidamente comunicada às partes envolvidas.
O fim da subscrição de um certificado ocorre quando o prazo de validade é expirado ou o certificado é revogado, conforme RFC 3647. O serviço atualiza respostas OCSP com uma periodicidade de 10m conforme definido no campo ***nextupdate***.

4.9.11. Outras Formas Disponíveis de Anunciar a Revogação

Não estipulado.

4.9.12. Requisitos Especiais Relacionados com o Comprometimento de Chave

Para além dos motivos referidos na secção 4.9.1 desta Declaração de Práticas de Certificação, as partes podem usar o email report@globaltrustedsign.com para demonstrar o comprometimento da chave privada dos certificados subscritos.

4.9.13. Motivos para a Suspensão

A GTS não suporta a suspensão de certificados.

4.9.14. Quem pode solicitar a Suspensão

Não estipulado.

4.9.15. Procedimento para o pedido de Suspensão

Não estipulado.

4.9.16. Limites do período de Suspensão

Não estipulado.

4.10. Serviços de Estado do Certificado

4.10.1. Caraterísticas Operacionais

O estado de certificados emitidos está disponível publicamente utilizando CRL e o serviço OCSP.

4.10.2. Disponibilidade de Serviço

O serviço de estado de certificado está disponível 24 horas por dia, 7 dias por semana. Se um certificado for revogado, este não se mantém na CRL após a sua data de expiração.

4.10.3. Funcionalidades Opcionais

Não estipulado.

4.11. Fim de Subscrição

O fim da subscrição de um certificado ocorre quando o prazo de validade é expirado ou o certificado é revogado, conforme RFC 3647.

4.12. Custódia e Recuperação de Chaves

4.12.1. Política e Práticas de Custódia e Recuperação de Chaves

A EC GTS efetua a retenção da sua chave privada e das chaves privadas de todos os seus clientes através de um HSM guardado em ambiente seguro.

- São arquivadas internamente em ambientes seguros e por longos períodos de tempo;
- São geradas e armazenadas em HSM não sendo possível a transferência das mesmas para outros meios ou dispositivos;
- As chaves privadas da EC GTS têm pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original e são alvo de cópias de segurança;
- São armazenadas de forma cifrada em HSM.

4.12.2. Política e Práticas de Encapsulamento e Recuperação de Chave de Sessão

Consultar ponto 4.12.1.

5. Controlos de Segurança Física, Gestão e Operacionais

5.1. Controlos de Segurança Física

5.1.1. Localização Física e Tipo Construção

A EC GTS foi desenhada de forma a proporcionar um ambiente seguro capaz de proteger os sistemas que suportam a atividade da Entidade Certificadora. As operações da GTS são realizadas numa sala numa zona de alta segurança, do edifício da GTS, acessível apenas às pessoas que dele necessitem para desempenho das suas funções de confiança. A GTS garante ainda que as suas zonas de alta segurança possuem todo o conjunto de características previstas, bem como os mecanismos necessários por forma a garantir as condições de segurança, no que concerne a:

- Localização física e tipo de construção, com paredes em alvenaria, betão ou tijolo;
- Teto e pavimento com construção similar à das paredes;
- Inexistência de janelas;
- Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança acionável eletronicamente, caraterísticas corta – fogo e funcionalidade antipânico;
- Acesso físico ao local;

- Energia e ar condicionado;
- Exposição à água / inundações;
- Prevenção e proteção face a incidentes/desastres tais como incêndios, inundações e semelhantes;
- Eliminação de resíduos;
- Salvaguarda dos suportes de informação.

5.1.2. Acesso Físico

De forma a oferecer confidencialidade, integridade e disponibilidade da informação à infraestrutura tecnológica, a GTS encontra-se hierarquizada em seis níveis de segurança:

- Nível 1;
- Nível 2;
- Nível 3;
- Nível 4;
- Nível 5;
- Nível 6.

O Nível 1 de segurança é identificado por grande parte da área da infraestrutura. O primeiro perímetro de segurança encontrado trata-se da zona de receção ao edifício, onde o pessoal afeto à organização é alvo de um sistema biométrico e os visitantes são alvo de registo apropriado por parte dos colaboradores da receção. Esta zona conta ainda com a munição de câmaras CCTV, com a capacidade de monitorizar todos os pontos de acesso ao edifício. A área de segurança seguinte é denominada pelo Nível 2. Este nível situa-se num piso do edifício para o efeito e representa o corredor entre o nível 01, a sala de sistemas (Nível 3) e a sala do TSP (Nível 4), sendo que, para aceder a esta área é necessária uma autenticação positiva na passagem de um controlo de acesso por parte dos grupos de confiança do TSP. No caso dos visitantes (auditores e manutenção) será fornecido um cartão de acesso para autenticação nos controlos de acessos. Estes cartões só validam acessos mediante a autenticação prévia de membros que exerçam funções orgânicas na estrutura do TSP.A área representada pelo Nível 3 de segurança, engloba a zona de antecâmara e a sala de sistemas. A funcionalidade principal da zona de antecâmara serve para impossibilitar a passagem direta do Nível 2 de segurança para o Nível 4. O acesso a estas zonas destina-se apenas para pessoal autorizado, enquanto os visitantes (auditores e manutenção), podem aceder apenas quando acompanhados pelos Grupos de Confiança do TSP. A entrada ou saída efetuada neste nível é apenas permitida após uma identificação positiva nos controlos de acesso, sendo que essas identificações são baseadas no fator biométrico. O sistema de controlo de acesso é gerido através de um software que controla todos os pontos de acesso à infraestrutura. O acesso para o Nível 4 de Segurança é realizado a partir de um dispositivo de controlos de acesso. O acesso só é permitido após a identificação positiva de dois

colaboradores de grupos de confiança diferentes. São utilizados dois mecanismos de identificação em simultâneo, biometria e código PIN. O Nível 5 de segurança, é materializado pelo Cofre de Segurança localizado no interior do Nível 4, onde estão os *smartcards* dos Administradores/Operadores do TSP para acesso aos sistemas de gestão do ciclo de vida dos certificados. Os acessos aos mesmos são apenas autorizados aos membros do grupo de confiança com funções estabelecidas na orgânica do TSP e com acesso aos serviços prestados pela TSP. É de referir ainda que o Cofre de Segurança, esta homologado segundo a norma EN 1143-1. O último nível de segurança, o Nível 6, é definida pelos compartimentos individualizados dentro do Cofre de Segurança (Nível 5), onde se encontram os dispositivos para acesso às funcionalidades do sistema do TSP. Cada compartimento identifica um individuo autorizado e com funções estabelecidas na orgânica do TSP, ao qual apenas o próprio poderá ter acesso.

5.1.3. Energia e Ar Condicionado

O ambiente seguro da GTS possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de:

- Alimentação de energia contínua ininterrupta com a potência suficiente para manter autonomamente a rede elétrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações elétricas que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia, e geradores de eletricidade a diesel);
- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente. Um sensor de temperatura ativa um alerta GSM, sempre que a temperatura atinge valores anormais. Este alerta GSM consiste em telefonemas com uma mensagem previamente gravada, para os elementos da equipa de manutenção.

5.1.4. Exposição à Água

As zonas de alta segurança têm instalados os mecanismos devidos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da GTS.

5.1.5. Prevenção e Proteção Contra Incêndio

O ambiente seguro da GTS tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Estão instalados nos vários níveis físicos de segurança, sistemas de deteção e alarme de incêndio;
- Estão disponíveis equipamentos fixos e móveis de extinção de incêndios, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;
- Existem procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6. Armazenamento de Media

Os suportes de informação sensível são armazenados de forma segura, em cofres e de acordo com o tipo de suporte e classificação da informação. O acesso a estas zonas é restrito a pessoas devidamente autorizadas.

5.1.7. Eliminação de Resíduos

No final do seu ciclo de vida, documentos e materiais em papel que contenham informações críticas deverão ser eliminados através de métodos eficazes que não permitam a reconstrução dos mesmos. Outros equipamentos de armazenamento (discos rígidos e afins) devem ser devidamente limpos, de modo a não seja possível recuperar alguma informação através de formatações seguras, ou destruição física dos equipamentos. No caso de periféricos criptográficos, estes devem ser destruídos segundo as instruções e recomendações dos respetivos fabricantes.

5.1.8. Backups em Instalações Externas

Todas as cópias de segurança são guardadas em ambiente seguro em instalações externas.

5.2. Controlos Procedimentais

A atividade de emissão de certificados digitais da GTS, enquanto entidade certificadora de certificados qualificados, exige o cumprimento de um conjunto de normas europeias. Estas mesmas normas definem um conjunto de grupos de trabalho, com competências, atividades e regras distintas, que deve ser garantido pela GTS. Nas funções de confiança está incluído todo o pessoal com acesso aos sistemas de certificação das EC e que na prática podem materialmente afetar:

- Manipulação de informações de subscritor e validação de informação de emissão de Certificado;
- Funções do ciclo de vida dos certificados;
- Configuração e manutenção dos sistemas de certificação;

No âmbito da sua estrutura organizativa são consideradas funções de confiança as descritas a seguir, estando divididas e diferenciadas pela natureza da sua atividade, quer se trate do software para

certificação digital. A cada uma delas são cometidas as seguintes responsabilidades consoante o âmbito.

5.2.1. Grupos de Trabalho

a) Grupo de Trabalho da Administração de Sistemas (AdmSist)

Responsáveis pela instalação, configuração e manutenção dos sistemas, no entanto, com acesso controlado às configurações relacionadas com a segurança. Este grupo tem como responsabilidades, nomeadamente:

- Gestão do ambiente de produção;
- Instalação, configuração e manutenção dos sistemas e rede tendo acesso controlado às configurações relacionadas com os componentes aplicacionais;
- Gestão do desempenho dos sistemas que suportam a atividade da GTS, de modo a garantir que a infraestrutura esteja sempre disponível e operacional, previsão das necessidades futuras que decorrem da atividade da GTS e os seus custos;
- Gestão dos incidentes e avarias de *hardware* e *software;*
- Reposição do sistema através das cópias de segurança, quando necessário;
- Execução e manutenção de documentação (procedimentos) pertinentes à execução das suas funções;
- Guarda dos artefactos sob a sua custódia.

b) Grupo de Trabalho da Administração de Segurança (AdmSeg)

Responsáveis globais sobre segurança dos sistemas, nomeadamente, pela gestão e implementação das regras e práticas de segurança no âmbito dos serviços prestados pela GTS. Este grupo tem como responsabilidades, nomeadamente:

- Definição da documentação associada às práticas de segurança da informação da GTS;
- Definição dos procedimentos relacionados com a gestão das chaves criptográficas;
- Garantia de que toda a documentação associada à GTS se encontra atualizada, adaptada à realidade e armazenada de forma segura de acordo com a sua classificação;
- Gestão da implementação das práticas e políticas de segurança, incluindo o controlo de acessos lógico e físico;
- Gestão dos riscos associados aos serviços prestados pela GTS;
- Monitorização dos eventos de segurança e gestão da alarmística associada a estes;
- Participação e resposta aos incidentes de segurança;
- Guarda dos artefactos sob a sua custódia.

c) Grupo de Trabalho de Operação de Sistemas (OpSist)

Responsáveis pela operação de rotina dos sistemas de confiança, estando autorizados a realizar as cópias de segurança e sua recuperação. Este grupo tem como responsabilidades, nomeadamente:

- Operação diária dos sistemas;
- Realização de operações de rotina;
- Realização de cópias de segurança;
- Guarda dos artefactos sob a sua custódia.

d) Grupo de Trabalho de Administração de Registo (AdmReg)

Responsáveis pela aprovação da emissão, suspensão e revogação de certificados digitais (certificados de assinatura qualificada, selos eletrónicos, certificados para autenticação de sítios Web, e selos temporais). Este grupo tem como responsabilidades, nomeadamente:

- Emissão e revogação dos certificados;
- Submissão dos *Certificate Signing Request* (CSR) para a execução dos processos de registo;
- Elaboração da videoconferência para validação da identidade dos titulares;
- Criação ou atualização das entidades requerentes de serviços de certificação;
- Validação da documentação a ser entregue pelo titular para emissão/revogação de certificados;
- Validação da identidade dos titulares por videoconferência;
- Notificação dos titulares quando necessário;
- Guarda dos artefactos sob a sua custódia.

e) Grupo de Trabalho de Auditoria (Auditor)

Responsáveis pela análise interna da conformidade com as normas nacionais e europeias aplicáveis à atividade da GTS enquanto prestadora de serviços qualificados, estando autorizados a ver e monitorizar os arquivos de atividade dos sistemas de confiança. Este grupo tem como responsabilidades, nomeadamente:

- Registo e monitorização de todas as operações sensíveis do sistema;
- Registo de todos os procedimentos passíveis de auditoria;
- Verificação periódica da conformidade com os processos, políticas e procedimentos em vigor no âmbito da atividade de prestadora de serviços qualificados;
- Guarda dos artefactos sob a sua custódia;
- Apresentação de sugestões de melhoria.

f) Grupo de Trabalho de Gestão (Gestão)

Responsáveis por assegurar os meios técnicos, financeiros e humanos para o correto funcionamento da GTS enquanto prestadora de serviços qualificados. Este grupo tem como responsabilidades, nomeadamente:

- Nomeação dos membros dos restantes Grupos de Trabalho;
- Revisão e aprovação das Políticas e Declaração de Práticas da GTS;
- Guarda dos artefactos sob a sua custódia.

5.2.2. Número de pessoas exigidas por grupo

Cada grupo tem 2 pessoas de modo a garantir a redundância dos recursos.

5.2.3. Identificação e Autenticação por Função

Consultar ponto 5.2.1.

5.2.4. Segregação de funções

A composição dos grupos de trabalho deve respeitar os princípios de privilégio mínimo e segregação de funções. Deste modo, a tabela a seguir apresenta as incompatibilidades entre os diferentes grupos existentes na GTS, de modo a evitar quaisquer conflitos de interesse.

Grupo de Trabalho	Incompatível com				
	(a)	(b)	(c)	(d)	(e)
(a) Administração de Segurança		X	X	X	X
(b) Administração de Sistemas	X				X
(c) Administração de Registo	X				X
(d) Operação de Sistemas	X				X
(e) Auditoria	X	X	X	X	

5.3. Controlos de Segurança Pessoal

5.3.1. Requisitos Relativos a Qualificações, Experiência e Credenciação

Todos os membros que integrem um dos grupos de trabalho da GTS devem cumprir os seguintes requisitos:

- Apresentar provas da suficiente qualificação e experiência para o desempenho da respetiva função;
- Garantir confidencialidade relativamente a informação sensível da GTS ou dados de identificação dos titulares;

- Garantir que não desempenham funções que possam causar conflito com as suas responsabilidades nas atividades da GTS;
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função;
- Ter recebido a documentação necessária para o desempenho da respetiva função;
- Ter sido nomeado formalmente para a função a desempenhar.

5.3.2. Procedimento de Verificação de Antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer um dos Grupos de Trabalho e inclui a verificação da identidade e do registo criminal, bem como das referências indicadas no *curriculum vitae*.

5.3.3. Requisitos e procedimentos de Formação

Os membros dos Grupos de Trabalho devem estar sujeitos a um plano de formação e treino específico, que englobe os seguintes tópicos:

- Aspetos legais relativos à prestação de serviços de certificação;
- Certificação digital e Infraestruturas de Chave Pública;
- Conceitos gerais sobre segurança da informação;
- Formação específica para o Grupo de Trabalho em causa;
- Funcionamento do software e/ou hardware usado na GTS;
- Política de Certificados e Declaração de Práticas de Certificação;
- Sensibilização em critérios de avaliação de certificados SSL de acordo com o EV Guidelines CA/Forum Browser;
- Procedimentos para a continuidade da atividade;
- Recuperação face a desastres.

5.3.4. Frequência e Requisitos para Atualização de Formação

Sempre que ocorra qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos existentes, deverá desencadear-se um processo de formação adequado para todos os Grupos de Trabalho. Devem ainda ser realizadas sessões formativas aos elementos das Entidades Certificadoras sempre que ocorram alterações às Políticas de Certificação ou na Declaração de Práticas de Certificação da GTS. Tais factos devem ser tidos em linha de conta de modo a garantir o nível pretendido de conhecimentos para a execução satisfatória das responsabilidades que compete aos diferentes Grupos de Trabalho.

5.3.5. Frequência e Sequência da Rotação de Funções

Não estipulado.

5.3.6. Sanções para Ações Não Autorizadas

Todas as ações não autorizadas e que desrespeitem a Declaração de Práticas de Certificação da GTS e as Políticas de Certificados deverão ser alvo de medidas disciplinares adequadas, quer tenham sido realizadas de forma deliberada ou sejam ocasionadas por negligência. Poderão ainda, de acordo com a gravidade da infração cometida, ser aplicadas sanções previstas na lei.

5.3.7. Requisitos para Prestadores de Serviços Independentes

O acesso à Zona de Alta Segurança por consultores ou prestadores de serviços independentes exige a supervisão contínua pelos membros dos grupos de trabalho, sendo a sua identidade confirmada através da verificação de documentação emitida por fontes confiáveis. Adicionalmente devem realizar o seu registo no livro de presenças existente para o efeito.

5.3.8. Documentação Fornecida ao Pessoal

Deverá ser disponibilizada aos membros dos Grupos de Trabalho a informação e documentação necessária relativamente às Políticas de Certificados, à Declaração de Práticas de Certificação da GTS, à documentação com a descrição das responsabilidades, obrigações e tarefas dependendo da função e ainda documentação técnica acerca do software e hardware utilizado na Entidade Certificadora da GTS.

5.4. Procedimentos de Registo de Auditoria

5.4.1. Tipos de Eventos Registados

Deverão ser registados todo o tipo de eventos significativos, capazes de ser auditáveis, em especial os seguintes:

- Cópias de segurança, restauro ou arquivamento de dados;
- Dispositivos físicos de segurança de entrada/saída dos vários níveis de segurança.
- Manutenções ao sistema;
- Modificações ou atualizações relativamente a software e hardware;
- Mudança de pessoal;
- Ligar e desligar aplicações ou sistemas que intervenham na atividade de certificação;
- Operações realizadas por membros dos Grupos de Trabalho;

- Tentativas, com ou sem sucesso, de acesso a recursos sensíveis da Entidade Certificadora da GTS;
- Tentativas, com ou sem sucesso, de alteração dos parâmetros de segurança;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar contas do sistema;
- Tentativas, com ou sem sucesso, de início e fim de sessão;
- Tentativas, com ou sem sucesso, de operações relativas a pedido, emissão, renovação, modificação, suspensão e revogação de chaves e certificados;
- Tentativas, com ou sem sucesso, de gerar, emitir ou atualizar LCR;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar informação dos titulares dos certificados;
- Tentativas, com ou sem sucesso, de acesso às Zonas de Alta Segurança da EC GTS.

O registo dos eventos, efetuado quer por meios automáticos ou manuais, deverá conter, no mínimo, informações tais como a data e hora do evento, a categoria e descrição do mesmo, o número de série do evento, bem como a identificação do agente que o terá originado.

5.4.2. Frequência de Processamento de Registos de Auditoria

A auditoria dos registos deverá ser realizada de forma regular, em especial na ocorrência de eventos que possam ser considerados suspeitos ou que possam comprometer, de alguma forma, a atividade em questão. Todos esses eventos deverão ficar registados num relatório sumário, passível de ser analisado, bem como as decisões e ações tomadas em resposta a estes.

5.4.3. Período de Retenção de Registo de Auditoria

Os registos de auditoria deverão ser mantidos nos sistemas por um período de, pelo menos, 1 mês após o seu processamento. Após esse período, deverão ser arquivados tal como definido na seção 5.5 do presente documento.

5.4.4. Proteção de Registo de Auditoria

Os registos de auditoria devem encontrar-se protegidos contra as tentativas de acessos, alteração, manipulação ou destruição não-autorizadas. Por norma, os registos eletrónicos devem estar protegidos com recurso a técnicas criptográficas de modo a que ninguém, à exceção das próprias aplicações de visualização de registos, com o controlo de acessos adequado, possa aceder aos mesmos. Os registos manuais devem ser armazenados em locais que cumpram os requisitos definidos para o efeito, dentro de instalações seguras da EC GTS. Este tipo de registos de auditoria é considerado informação sensível.

5.4.5. Procedimentos de Cópias de Segurança de Registos de Auditoria

Devem ser realizadas cópias de segurança dos registos de auditoria de forma regular.

5.4.6. Sistema de Recolha de Registos (Interno vs. Externo)

Os registos são recolhidos e tratados centralmente.

5.4.7. Notificação de Agentes Causadores de Eventos

Os eventos passíveis de serem auditáveis são registados nos sistemas internos da GTS, sendo estes armazenados de forma segura. Não está contemplada qualquer notificação ao agente causador do evento.

5.4.8. Avaliação de vulnerabilidades

Ainda que não ocorram alterações significativas no ambiente global da EC GTS, deverão ainda assim ser efetuadas avaliações de vulnerabilidades, tendo em vista minimizar ou eliminar potenciais tentativas de quebras de segurança no sistema. O resultado das avaliações deve ser reportado aos responsáveis pela matéria, para que estes as possam rever e aprovar, caso se justifique, um plano de implementação e correção das vulnerabilidades detetadas.

5.5. Arquivo de Registos

5.5.1. Tipos de Registos Arquivados

A EC GTS irá arquivar, no mínimo, os seguintes tipos de dados:

- Os registos de auditoria especificados no presente documento;
- As cópias de segurança dos sistemas que compõem a infraestrutura da EC;
- Documentação relativa ao ciclo de vida dos certificados;
- Chaves para efeitos de confidencialidade (quando aplicável);
- Contratos estabelecidos entre a EC e outras entidades.

5.5.2. Período de Retenção em Arquivo

O tempo de retenção dos dados sujeitos a arquivo está definido de acordo com o previsto na legislação nacional, por um período nunca inferior a 7 anos.

5.5.3. Proteção do Arquivo

O arquivo encontra-se protegido de acordo com o que está igualmente previsto para a proteção dos registos de auditoria. Mais se acrescenta que o arquivo se encontra protegido de modo a que apenas os membros autorizados dos Grupos de Trabalho possam consultar e aceder ao mesmo.

5.5.4. Procedimentos para Cópia de Segurança do Arquivo

Consultar ponto 5.4.5.

5.5.5. Requisitos para Validação Cronológica de Registos

Os sistemas de informação utilizados pela EC GTS devem garantir o registo da data e hora do momento, tendo por base uma fonte de tempo segura.

5.5.6. Sistema de Recolha de Arquivo (Interno vs. Externo)

Consultar ponto 5.4.6.

5.5.7. Procedimentos para Obter e Verificar Informação de Arquivo

Só os membros devidamente autorizados dos Grupos de Trabalho têm acesso aos arquivos para a verificação da integridade da informação, de modo a garantir que os mesmos se encontram em bom estado e que podem ser recuperados.

5.6. Renovação de Chaves

Não estipulado.

5.7. Recuperação em Caso de Desastre ou Comprometimento

Esta seção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

5.7.1. Procedimentos em Caso de Incidente ou Comprometimento

Na eventualidade de incidente de segurança grave ou comprometimento da EC GTS, devem ser tomados os procedimentos seguintes:

- Notificação, sem demora indevida, mas sempre no prazo de 24 horas após ter tomado conhecimento do ocorrido, a entidade supervisora e, se necessário, outras entidades, como a entidade nacional competente em matéria de segurança da informação ou a autoridade

responsável pela proteção de dados, de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados;

- Se a violação da segurança ou perda de integridade constatada for suscetível de prejudicar a pessoa singular ou coletiva a quem o serviço de confiança tiver sido prestado, será notificada também sem demora indevida a referida pessoa singular ou coletiva da violação da segurança ou da perda de integridade;
- Adicionalmente, e dependendo do tipo de incidente, a EC afetada poderá ser desligada.

Se necessário, em particular se a violação de segurança ou a perda de integridade disserem respeito a dois ou mais Estados-Membros, a entidade supervisora notificada informa do facto as entidades supervisoras dos outros Estados-Membros em causa e a ENISA.
A entidade supervisora notificada informa o público ou exige que o prestador do serviço de confiança o faça, se considerar que a divulgação da violação da segurança ou perda de integridade é do interesse público.

5.7.2. Processos de Recuperação caso os Recursos informáticos, Software e/ou Dados, sejam corrompidos

Caso os recursos de hardware, software e/ou dados tenham sido alterados ou exista a suspeita de que estes tenham sido corrompidos, deverá iniciar-se um processo de gestão de incidentes tendo em vista o restabelecimento das condições seguras com inclusão de novos componentes de eficácia credível.
A GTS suspenderá os seus serviços e notificará todas as Entidades envolvidas caso se verifique que esta situação tenha afetado os certificados emitidos, incluindo a notificação dos titulares dos mesmos.

5.7.3. Procedimentos em caso de Comprometimento de Chave Privada da Entidade

Se algum dos algoritmos, ou parâmetros associados, utilizados pela EC GTS ou seus titulares se tornarem insuficientes para o fim a que se destinam, a EC GTS deve:

- Informar todos os titulares e outras entidades com as quais a EC GTS tenha acordos ou outra forma de relações estabelecidas. Adicionalmente, esta informação deve ser disponibilizada para outras entidades dependentes;
- Informar o Repositório de Raiz da Mozilla e outros repositórios de raiz que tenham estabelecido uma relação de confiança com a hierarquia do PKI GTS;
- Agendar a revogação de qualquer certificado afetado.

5.7.4. Capacidades de Continuidade de Negócio em caso de Desastre

A GTS dispõe de um plano de continuidade da atividade, onde estão descritos todos os procedimentos a acionar em caso de desastre onde haja perda ou corrupção de dados, software e equipamentos. O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade de disponibilidade estão disponíveis no Local Alternativo e que os dados da EC GTS necessários para retomar as operações são copiados e armazenados em locais seguros e adequados para permitir retomar devidamente as operações da EC GTS em caso de incidentes/desastres. As cópias de segurança de informações e software essenciais são realizadas regularmente. Devem ser fornecidas instalações de apoio adequadas para garantir que todas as informações e software essenciais possam ser recuperados após um desastre ou falha nos meios de comunicação (media). Os mecanismos de salvaguardas devem ser testados regularmente para garantir que respondem aos requisitos dos planos de continuidade do negócio.

5.8. Procedimentos em caso de extinção da Entidade de Certificação ou Entidade de Registo

A GTS deve em caso de cessação de atividades, atempadamente proceder às ações seguintes:

- Informar a Entidade Supervisora (Gabinete Nacional de Segurança);
- Informar todos os titulares dos certificados a partir de uma notificação explanatória com antecedência à cessação formal das atividades da EC GTS;
- Revogar todos os certificados;
- Garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos;
- Proceder à destruição definitiva de toda a informação classificada ou garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC GTS, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

Caso se procedam a alterações do organismo/estrutura responsável de gestão da atividade da EC GTS, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

6. Controlos de Segurança Técnica

6.1. Geração e Instalação do Par de Chaves

Esta seção define as medidas de segurança implementadas para a PKI GTS de forma a proteger as chaves criptográficas geradas por esta, e respetivos dados de ativação. O nível de segurança atribuído

à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras, assim como dados de ativação, estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas. A geração dos pares de chaves da EC GTS é processada de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1. Geração do Par de Chaves

6.1.1.1. Geração de par de chaves CA

A geração dos pares de chaves da EC GTS é processada de acordo com os requisitos e algoritmos definidos nesta declaração, através de um procedimento formal datado, realizado e assinado por elementos autorizados dos Grupos de Trabalho da Administração de Segurança e de Auditoria. A CA GTS não gera pares de chaves para certificados que têm a extensão EKU contendo o atributo ***KeyPurposeIds id-kp-serverAuth*** ou ***anyExtendedKeyusage***.

6.1.1.2. Geração de par de chaves RA

Não estipulado.

6.1.1.3. Geração de par de chaves utilizador

Ver ponto 4.5.1.

6.1.2. Entrega de Chave Privada ao Subscritor/Titular

Não estipulado.

6.1.3. Entrega de Chave Pública ao Emissor do Certificado

Ver ponto 4.1.

6.1.4. Entrega da Chave Pública da EC às Partes Confiantes

Ver ponto 2.2.

6.1.5. Tamanhos de Chaves

No que respeita à dimensão das chaves, foram seguidas as recomendações da norma ETSI TS 119 312 – Electronic Signatures and Infrastructures – Cryptographic Suites. A dimensão definida para as chaves é a seguinte:

- 4096 bits RSA para a chave das entidades certificadoras da GTS.

- 2048 bits RSA para chaves associadas aos restantes certificados que sejam emitidos pela GTS com algoritmo de assinatura sha256RSA.

6.1.6. Geração dos Parâmetros de Chave Pública e Verificação de Qualidade

O processo de geração das chaves é, obrigatoriamente, efetuado diretamente num módulo criptográfico em hardware (HSM). O módulo criptográfico cumpre os requisitos FIPS 140-2 nível 3. Estes certificados são assinados pela ROOT CA GTS. A ROOT CA GTS funciona em modo *offline*.
A geração das chaves da EC GTS deverá ser feita de acordo com o estipulado no PKCS#11.

6.1.7. Finalidades de Utilização da Chave (de acordo com o campo key usage X.509 v3)

Consultar ponto 1.4.

6.2. Proteção de Chave Privada e Controlos de Engenharia de Módulo Criptográfico

Nesta secção são considerados os requisitos para proteção das chaves privadas e para os módulos criptográficos da PKI GTS. A Global Trusted Sign implementou uma combinação de controlos físicos, lógicos e procedimentais, devidamente documentados, de forma a assegurar a confidencialidade e integridade das chaves privadas da PKI GTS.

6.2.1. Controlos e Standards de Módulo Criptográfico

A EC GTS utiliza módulos criptográficos (HSM) para as operações que dizem respeito à geração, armazenamento e assinatura. Os módulos criptográficos estão em conformidade com o Common Criteria v2.3, FIPS 140-2 e FIPS 140-2 nível 3 (para o módulo criptográfico da EC GTS). A segurança do módulo criptográfico da EC GTS é garantida durante o seu ciclo de vida, garantindo:

- A instalação e ativação das chaves privadas no módulo criptográfico é efetuada por elementos de Grupos de Trabalho bem identificados (secção 14.2 Controlos dos Processos e 14.3 Medidas de Segurança de Pessoal);
- As chaves privadas de assinatura guardadas no módulo criptográfico são apagadas no final do seu ciclo de vida;
- O módulo criptográfico não foi adulterado durante o seu transporte;
- O módulo criptográfico não é adulterado enquanto permanece nas instalações seguras da GTS;
- O módulo criptográfico tem um funcionamento correto.

6.2.2. Controlo Multi Pessoal (n de m) da Chave Privada

A geração e instalação dos dados de ativação para a chave privada da EC GTS é feita por pessoal autorizado em ambiente seguro através de um setup inicial do HSM, que exige controlo simultâneo por dois membros dos grupos de trabalho.

6.2.3. Custódia de Chave Privada

A EC GTS efetua a retenção da sua chave privada e das chaves privadas de todos os seus clientes através de um HSM guardado em ambiente seguro.

- São arquivadas internamente em ambientes seguros e por longos períodos de tempo.
- São geradas e armazenadas em HSM não sendo possível a transferência das mesmas para outros meios ou dispositivos.
- As chaves privadas da EC GTS têm pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original e são alvo de cópias de segurança.
- São armazenadas de forma cifrada em HSM.

6.2.4. Cópia de Segurança da Chave Privada

Consultar ponto anterior.

6.2.5. Arquivo de Chave Privada

Consultar ponto 6.2.3.

6.2.6. Transferência da Chave Privada para/de um Módulo Criptográfico

A transmissão dos dados de ativação das chaves privadas para outros HSM é feita, apenas e só quando necessário, de modo a garantir a sua proteção e disponibilidade.

6.2.7. Armazenamento da Chave Privada em Módulo Criptográfico

Consultar ponto 6.2.3.

6.2.8. ~~Ativação~~ da Chave Privada

A chave privada deverá ser ativada quando o sistema/aplicação da ROOT CA é ligado. Esta ativação só será efetivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação por quórum *k* em N

onde k = 2. Isto é, é necessário *k* utilizadores em *N* para efetuar uma operação administrativa nos HSM (incluindo a ativação da chave privada).

6.2.9. ~~D~~esativação da Chave Privada

A chave privada deverá ser desativada quando o sistema/aplicação da ROOT CA é desligado. Esta desativação só será efetivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação por quórum *k* em N onde k = 2. Isto é, é necessário *k* utilizadores em *N* para efetuar uma operação administrativa nos HSM (incluindo a desativação da chave privada).

6.2.10. ~~D~~estruição da Chave Privada

As várias chaves privadas da EC GTS deverão ser destruídas sempre que deixem de ser necessárias. De uma forma geral, a destruição de chaves deve ser precedida sempre pela revogação do certificado, no caso de estar em vigor, ou caso tenha sido atingido o fim da sua data de validade. Nesse sentido, as chaves deverão ser apagadas/destruídas através de um método formal aditável, de modo a que não seja possível a sua posterior reconstrução. De igual forma, as respetivas cópias de segurança deverão também ser alvo de destruição.

6.2.11. Capacidades do Módulo Criptográfico

Consultar ponto 6.2.1.

6.3. Outros Aspetos da Gestão do Par de Chaves

6.3.1. Arquivo da Chave Pública

A EC GTS efetua o arquivo das suas chaves e das chaves por si emitidas (para efeitos de assinatura digital), permanecendo armazenadas após a expiração dos certificados correspondentes para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos Operacionais do Certificado e Períodos de Utilização do Par de Chaves

O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que após expiração do certificado as chaves deixam de poder ser utilizadas, dando origem à cessação permanente da sua operacionalidade e da utilização que lhes foi destinada. A validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados, é a seguinte:

- O certificado da ROOT CA GTS tem uma validade mínima de 20 anos;

- Um certificado para entidade subordinada emitido pela EC GTS tem uma validade mínima de 1 ano, e máxima de 6 anos.
- Um certificado SSL EV ou OV tem a validade máxima de 398 dias.
- Todos os certificados emitidos por GTS são validos desde o momento da sua emissão até ao momento que caducam. Nenhum certificado emitido para um servidor pode superar um período de validade de mais de 825 dias.

6.4. Dados de Ativação

6.4.1. Geração e Instalação de Dados de Ativação

Consultar ponto 6.2.2.

6.4.2. Proteção de Dados de Ativação

Os dados de ativação da chave privada são guardados em ambientes seguros.

6.4.3. Outros Aspetos dos Dados de Ativação

Os dados de ativação são destruídos assim que a chave privada associada for igualmente destruída.

6.5. Controlos de Segurança Computacional

6.5.1. Requisitos Técnicos Específicos de Segurança Computacional

O acesso aos servidores do PKI GTS é restrito aos membros dos Grupos de Trabalho. A ROOT CA GTS é uma EC offline, sendo apenas ativada no âmbito de manutenção periódica e desativada logo de seguida. As EC Subordinadas do PKI GTS têm um funcionamento ativo, sendo o pedido de emissão de certificados efetuado a partir do Sistema de Gestão do Ciclo de Vida dos Certificados (SGCVC) e/ou da consola de operação.

6.5.2. Avaliação/Nível de Segurança Computacional

Os vários sistemas e produtos utilizados pelo PKI GTS são fiáveis e protegidos contra modificações. Os módulos criptográficos estão em conformidade com o Common Criteria v2.3, FIPS 140-2 e FIPS 140-2 nível 3 para o módulo criptográfico da ROOT CA GTS.

6.6. Controlos Técnicos do Ciclo de Vida

6.6.1. Controlos de Desenvolvimento de Sistema

Todo o desenvolvimento, configuração e alteração do Software/Hardware associados à infraestrutura de chave pública são executadas e auditadas por membros autorizados da EC GTS. A EC GTS possui mecanismos para controlar e monitorizar as configurações dos sistemas deste a sua primeira ativação até à eventual cessação de atividades. Todas as operações de atualização e manutenção são executadas por membros autorizados de acordo com os procedimentos adequados para o efeito.

6.6.2. Controlos de Gestão da Segurança

Todos os sistemas da EC GTS estão na Zona e de Alta Segurança (ZAS). Através dos controlos implementados, é possível garantir a identificação, autenticação e administração dos acessos.

6.6.3. Controlos de Segurança do Ciclo de Vida

As operações de atualização e manutenção dos produtos e sistemas da PKI GTS, seguem o mesmo controlo que o equipamento original e são instalados pelos membros dos Grupos de Confiança da GTS com formação adequada para o efeito, seguindo os procedimentos definido.

6.7. Controlos de Segurança de Rede

A PKI GTS dispõe de dispositivos de proteção de fronteira, nomeadamente sistema firewall. Cumpre com os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditoria e troca de informação. A PKI GTS assegura, por conseguinte, que o conjunto de controlos implementados estão em conformidade com todos os requisitos de segurança de rede do "CA/Browser FORUM - Network and Certificate System Security Requirements".

6.8. Validação Cronológica

A informação relacionada com a EC GTS é registada com a data e hora da criação. Toda a infraestrutura é sincronizada temporalmente por relógio atómico interno, e adicionalmente por duas fontes UTC alternativas:

- Royal Observatory of Belgium (ORB), Bélgica, Bruxelas - ntp1.oma.be
- Observatoire de Paris (LNE-SYRTE), Paris, França - ntp-p1.obspm.fr

7. Perfis de Certificado, CRL e OCSP

7.1. Perfil do Certificado

A emissão de certificados segue o perfil de certificados recomendado pela ITU-T X.509 versão 3. O armazenamento das chaves envolvidas em todos os processos de assinatura ou geração de certificados são guardados num Dispositivo Seguro de Hardware (HSM) certificado e que cumpre os requisitos definidos na legislação nacional e europeia. O perfil do certificado da EC GTS está de acordo com o conjunto de standards:

- Regulamento (UE) N. o 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers, e os standards relacionados com os serviços qualificados de confiança;
- Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

Informação detalhada sobre os perfis dos Certificados da EC GTS pode ser consultada em: https://pki.globaltrustedsign.com/index.html

7.1.1. Número(s) de Versão

O campo "*version*" do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é 3 (V3).

7.1.2. Conteúdo e extensões do certificado, aplicabilidade do RFC 5280

7.1.2.1. Certificado da Root CA

Informação encontra-se disponível nos certificados em arquivo, consultáveis através do acesso ao repositório https://pki.globaltrustedsign.com/index.html e através da PL11 – Política de certificação da ROOT GTS.

7.1.2.2. Certificados da EC subordinada da GTS

Consultar ponto 7.1.2.1.

7.1.2.3. Subscritores dos certificados

Informação encontra-se disponível nos certificados em arquivo, consultáveis através do acesso ao repositório https://pki.globaltrustedsign.com/

7.1.2.4. Todos os certificados

Informação encontra-se disponível nos certificados em arquivo, consultáveis através do acesso ao repositório https://pki.globaltrustedsign.com/index.html e através da PL01_GTS - Política de Certificados para Assinatura Qualificada, PL02_GTS - Política de Certificados para Selos Eletrónicos PL03_GTS - Política de Certificados SSL EV, PL04_GTS - Política de Certificados SSL OV, PL16_GTS - Política de Certificados para Assinaturas Avançadas, PL17_GTS - Política de Certificados para Selos Eletrónicos Avançados e PL14_GTS - Política de Certificados para Selos Temporais.

7.1.2.5. Aplicabilidade do RFC 5280

As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

7.1.3. Identificadores de Objeto de Algoritmo

Aplicam-se os requisitos ao campo de parâmetros de chave pública disponível nos certificados.

7.1.3.1. SubjectPublicKeyInfo

Informação encontra-se disponível nos certificados em arquivo, consultáveis através do acesso ao repositório https://pki.globaltrustedsign.com/index.html e através da PL01_GTS - Política de Certificados para Assinatura Qualificada, PL02_GTS - Política de Certificados para Selos Eletrónicos PL03_GTS - Política de Certificados SSL EV, PL04_GTS - Política de Certificados SSL OV, PL16_GTS - Política de Certificados para Assinaturas Avançadas, PL17_GTS - Política de Certificados para Selos Eletrónicos Avançados e PL14_GTS - Política de Certificados para Selos Temporais.

7.1.3.2. Signature AlgorithmIdentifier

O campo "*signatureAlgorithm"* do certificado contém o OID do algoritmo criptográfico utilizado pela EC GTS para assinar o certificado (1.2.840.113549.1.1.11 - sha256WithRSAEncryption).

7.1.4. Formatos de Nome

7.1.4.1. Nomes de codificação

Consultar ponto 3.1.

7.1.4.2. informações relativas ao Assunto - Certificados de Utilizadores

Consultar ponto 3.1.

7.1.4.3. informações relativas ao Assunto - Certificado da Raiz e Certificados CA Subordinados

Consultar ponto 3.1.

7.1.5. Restrições de Nome

A GTS pode incluir restrições de nomes no campo "*nameConstraints*" quando aplicável.

7.1.6. Identificador de Objeto de Política de Certificado

7.1.6.1. Identificadores de política de certificados reservados

O certificado da Root não contém OID. Todavia, os certificados emitidos pelas Subordinadas do PKI GTS contêm os seguintes qualificadores: "*policyQualiflierID*= CPS" e "*cPSuri*", que aponta para o URL onde se encontra a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*". São incluídos outros identificadores de objetos de política de certificado, dependendo do tipo de certificado.

Todos os certificados que têm um identificador de política têm como número base: 1.3.6.1.4.1.50302

7.1.6.2. Certificados de CA Raiz

Consultar 7.1.6.1.

7.1.6.3. Certificados de CA Subordinados

Consultar 7.1.6.1.

7.1.6.4. Certificados de utilizadores

Consultar 7.1.6.1.

7.1.7. Utilização de Extensão de Restrições de Política

Não estipulado.

7.1.8. Sintaxe e Semânticas de Qualificadores de Política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores de certificados e autores da política de certificado. O tipo de qualificador é o "*CPSuri*", que contém um apontador, na forma de URL, para a Declaração de Práticas de Certificação publicada pela

EC e o "*userNotice explicitText*", que contém um apontador, na forma de URL, para a Política de Certificado.

7.1.9. Processamento de Semânticas para a Extensão de Políticas de Certificado Críticas

Não estipulado.

7.2. Perfil CRL

7.2.1. Número(s) de Versão

As LRC emitidas contêm os campos básicos e conteúdos específicos na tabela seguinte:

Campo	Valor
Versão	V2
Algoritmo de Assinatura	O algoritmo utilizado pela EC para assinar o certificado é sha256WithRSAEncryption
Emissor	DN da entidade certificadora emissora da LCR
Data Efetiva	A indicação de quando a LCR foi gerada.
Próxima atualização	A indicação de quando será gerada nova LCR.
Certificados Revogados	Lista dos certificados revogados que fornece informação do estado dos certificados no que diz respeito, respetivamente, ao número de série do certificado revogado, a data em que foi revogado e o motivo da sua revogação.

Informação mais detalhada sobre os perfis das LRC pode ser consultada em:

- Lista de Revogação de Certificados (LRC) da EC GTS
    - https://pki.globaltrustedsign.com/index.html
    - https://pki02.globaltrustedsign.com/index.html

O perfil dos certificados OCSP pode ser consultado em:

- http://ocsp.globaltrustedsign.com

7.2.2. CRL e Extensões da CRL

Extensão	Valor
Authority Key Identifier	Identificador da EC emissora da CRL
CRL Number	Número sequencial da CRLS

7.3. Perfil OCSP

7.3.1. Número(s) de Versão

Os pedidos e respostas OCSP emitidos pela PKI GTS estão em conformidade com a versão 1 do RFC 6960.

7.3.2. Extensões OCSP

Não estipulado.

8. Auditoria de Conformidade e Outras Avaliações

A GTS irá efetuar auditorias e avaliações de conformidade regulares para assegurar a conformidade da Entidades Certificadoras constituintes da sua hierarquia de confiança de acordo com legislação nacional bem como com as normas internacionais aplicáveis.

8.1. Frequência ou Circunstâncias da Avaliação

Na EC GTS, as auditorias de conformidade serão realizadas regularmente de acordo com a legislação aplicável por uma entidade externa registada e reconhecida para o efeito, tomando como base as normas existentes sendo os seus resultados comunicados à entidade supervisora.
Os documentos (declaração de práticas e políticas de certificados) são validados anualmente, de acordo com a data de referência identificada no próprio documento, ou sempre que verifique alguma alteração.

8.2. Identificação/Qualificações do Avaliador

O Organismo de avaliação da conformidade (Conformity Assessment Body – CAB) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

8.3. Relação do Avaliador com a Entidade Avaliada

O organismo de avaliação da conformidade e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria. Na Relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual. O Auditor e a parte auditada (Entidade Certificadora) não devem ter nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses. O cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares da EC GTS.

8.4. Tópicos Abrangidos pela Avaliação

Uma auditoria de segurança é efetuada com base nos requisitos definidos na presente DPC e em conformidade com a legislação nacional aplicável. Tem por objetivo determinar a conformidade dos serviços da EC GTS com esta Declaração de Práticas e com as Políticas de Certificados definidas. Deve também determinar a correta adequação em relação a diversos documentos, nomeadamente a política de segurança, segurança física, avaliação tecnológica, gestão dos serviços da EC, seleção de pessoal, declarações de práticas de certificação e políticas de certificados em vigor, contratos e política de privacidade. Pode ser efetuada de forma completa ou parcial, e pode incidir sobre qualquer tipo de documentos/processos.

8.5. Ações Tomadas como Resultado de Deficiências

Quando são detetadas irregularidades numa auditoria, a CAB procede da seguinte forma:

- Documentar todas as irregularidades encontradas durante a auditoria;
- No final do processo de auditoria, reunir com os responsáveis da entidade submetida a auditoria e apresentar de forma sucinta o relatório de primeiras impressões (RPI);
- Elaborar o relatório de auditoria de acordo com as regras e práticas estabelecidas pela Entidade Supervisora;
- Submeter o relatório de auditoria à Entidade auditada;
- A entidade submetida à auditoria deve enviar um relatório de correção de irregularidades (RCI) para a Entidade Supervisora, descrevendo as ações, metodologia e tempo necessário para a correção das irregularidades identificadas;
- A Entidade Supervisora, após a análise do relatório submetido, consoante o nível de gravidade/severidade das irregularidades, tomará uma das três opções seguintes:
    - Aceitar os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;

- Permitir que a entidade continue em atividade por um período máximo de 90 dias para a correção das irregularidades;
- Revogação imediata das atividades.

8.6. Comunicação de Resultados

Os resultados de todo o processo serão comunicados aos auditores responsáveis e à GTS.

8.7. Auditorias Internas

Durante o período em que a EC GTS emite certificados, monitoriza, por conseguinte, a adesão às Políticas de Certificados e Declarações de Práticas de Certificação controlando, desta forma, todos os requisitos de garantia qualitativa de serviço através de auditorias internas realizadas trimestralmente, por amostra selecionada, de forma aleatória, de pelo menos três por cento dos certificados emitidos durante o período a que a auditoria se refere. Esta auditoria é realizada por membros do Grupo de Confiança da GTS, de acordo com as diretrizes adotadas pelo CA/B FORUM.

9. Outras Matérias Legais e de Negócio

Estabelecem-se alguns aspetos legais e de negócio que importa salientar de seguida:

- Poderão ser cobradas taxas pelos processos de emissão, e/ou renovação de certificados;
- Poderão ser cobradas taxas pelos serviços de validação cronológica;
- Não serão cobradas taxas pela disponibilização dos certificados em repositório;
- O acesso a informação sobre o estado ou lista de revogação de certificados (LRC) é livre e gratuita, não se podendo aplicar qualquer taxa;
- Não estão previstos reembolsos aplicáveis à prestação de serviços de revogação de certificados.

9.1. Taxas

9.1.1. Taxas de Emissão ou Renovação de Certificado

As taxas cobradas pela GTS estão identificadas em https://globaltrustedsign.com/ ou numa proposta formal realizada pela GTS.

9.1.2. Taxas de Acesso a Certificado

Não estipulado.

9.1.3. Taxas de Acesso a Informação de Estado ou Revogação

O acesso à informação sobre o estado de certificado ou revogação (CRL) é gratuita.

9.1.4. Taxas para Outros Serviços

As taxas para outros serviços são identificadas numa proposta formal.

9.1.5. Política de Reembolso

A EC GTS não tem uma política de reembolso específica.
A emissão correta de um certificado digital, seja de que tipo for, pressupõe o início da execução de um contrato, pelo que de acordo com a legislação aplicável a defesa do consumidor, em tais casos, o Titular perde o seu direito de rescisão, e por consequência reembolso.

9.2. Responsabilidade Financeira

9.2.1. Cobertura de Seguro

As Entidades Certificadoras devem respeitar a legislação em vigor no que se concerne aos seguros de cobertura de responsabilidade civil. Nesse sentido, a GTS dispõe de um seguro de responsabilidade civil, de acordo com o artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril.

9.2.2. Outros Recursos

Não estipulado.

9.2.3. Cobertura de Seguro ou Garantia para Utilizadores Finais

A GTS dispõe de um seguro de responsabilidade civil, de acordo com o artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril e do ponto 8.4 do Guidelines for the Issuance and Management of Extended Validation Certificates, CA/Browser Forum 1.8.4.

9.3. Confidencialidade de Informação de Negócio

9.3.1. Âmbito de Informação Confidencial

Considera-se informação confidencial:

- As chaves privadas das Entidades Certificadoras;
- As chaves privadas dos titulares dos certificados;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;

- Toda a informação de carácter pessoal proporcionada à EC GTS durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;
- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Dados dos membros dos grupos de trabalho da EC GTS.

9.3.2. Informação fora do Âmbito de Informação Confidencial

Considera-se informação de acesso público:

- Declarações de Práticas de Certificação;
- Políticas de Certificados;
- Listas de Revogação de Certificados (LRC);
- Toda a informação classificada como "pública".

A EC GTS permite o acesso a informação não confidencial, sem prejuízo do que se venha a estabelecer nas DPC, no domínio dos controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

9.3.3. Responsabilidade de Proteção de Informação Confidencial

As práticas da EC GTS garantem a proteção da confidencialidade e integridade dos dados de registo, especialmente quando transmitida entre a EC GTS e os subscritores e titulares, bem como durante a comunicação entre os componentes distribuídos dos sistemas da EC GTS. No âmbito dos serviços prestados, é necessário manter evidências digitais por questões de conformidade com a legislação em vigor e aplicável à EC GTS. Estas evidências são mantidas de modo a garantir a sua recolha, transmissão e armazenamento seguros.

9.4. Privacidade de Informação Pessoal

9.4.1. Plano de Privacidade

O Sistema de Gestão do Ciclo de Vida do Certificado (SGCVC) é responsável pela implementação de medidas que asseguram a privacidade de dados pessoais, de acordo com a legislação Portuguesa e Europeia aplicável.

9.4.2. Informação Privada

Informação privada é toda a informação fornecida pelo titular do certificado que não esteja publicamente disponível.

9.4.3. Informação Não Considerada Privada

Informação considerada não-privada é toda a informação tornada pública a partir de certificados e, como tal, não é considerada privada.

9.4.4. Responsabilidade pela Proteção de Informação Privada

A responsabilidade de proteção da informação privada, estão de acordo com a legislação portuguesa, nomeadamente com o regulamento geral de proteção de dados (regulamento 2016/679).

9.4.5. Notificação e Consentimento para Utilização de Informação Privada

Os procedimentos para notificação e consentimento para utilização da informação privada estão de acordo com a legislação portuguesa, nomeadamente com o regulamento geral de proteção de dados (regulamento 2016/679).

9.4.6. Divulgação Resultante de Processo Judicial ou Administrativo

Não há qualquer cedência de dados pessoais a terceiros, salvo por motivos legais devidamente fundamentados.

9.4.7. Outras Circunstâncias de Divulgação de Informação

Não há qualquer cedência de dados pessoais a terceiros, salvo por motivos legais devidamente fundamentados.

9.5. Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID, DPC, PC, bem como qualquer outro documento relacionado, são propriedade da EC GTS. As chaves privadas e as chaves públicas são propriedade do titular, independentemente do meio físico que se empregue para o seu armazenamento. O titular conserva sempre o direito sobre as suas marcas, produtos ou nome comercial contido no certificado.

9.6. Representações e Garantias

9.6.1. Representações e Garantias da EC

É obrigação da EC GTS cumprir as diretivas seguintes:

- Realizar as suas operações de acordo com esta Declaração de Práticas;
- Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado;

- Cumprir com as especificações contidas na legislação sobre Proteção de Dados Pessoais;
- Proteger, em caso de existirem, as suas chaves privadas e as que estejam sob sua custódia;
- Emitir certificados de acordo com o standard X.509;
- Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de input de dados;
- Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
- Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
- Utilizar sistemas fiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir pessoas não autorizadas altere os dados;
- Arquivar sem alteração os certificados emitidos;
- Garantir que pode determinar, com precisão da data e hora, em que emitiu, ou revogou, ou suspendeu um certificado;
- Empregar pessoal com qualificações, conhecimento e experiências necessárias para a prestação de serviços de certificação;
- Revogar os certificados nos termos previstos no presente documento, e atualizar a lista de certificados revogados na LCR, com a frequência estipulada na presente DPC;
- Publicar a sua DPC e as Políticas aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;
- Notificar, com a máxima brevidade possível, por meio de correio eletrónico, os titulares dos certificados nos casos em que a EC GTS proceda à revogação ou suspensão dos mesmos, indicando o motivo que originou a situação;
- Colaborar com as auditorias externas exigidas pela Entidade Supervisora;
- Operar em conformidade com as políticas, normas e legislação que sejam aplicáveis;
- Garantir a disponibilidade da LCR de acordo com as disposições do presente documento, bem como a disponibilidade do serviço de OCSP;
- Em caso de cessação de atividades deverá comunicar esse facto com uma antecedência mínima de três meses à Entidade Supervisora, assim como todos os titulares de certificados emitidos pela EC GTS;
- Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento durante o prazo estabelecido no presente documento;
- Disponibilizar os certificados da EC GTS.

9.6.2. Representações e Garantias da AR

A Autoridade de Registo (AR) é a entidade responsável pela análise e avaliação dos pedidos de serviços da GTS, nomeadamente à veracidade dos documentos e validação da identidade dos titulares dos certificados e pedidos. Esta AR tem o direito de aprovar ou rejeitar os pedidos após a devida validação. Adicionalmente a AR tem autoridade para aprovar a revogação de certificados. As Autoridades de Registo da Global Trusted Sign estão em conformidade com os requisitos estabelecidos neste documento e estão sujeitas a Auditorias Externas independentes, assim como Auditorias Internas realizadas Global Trusted Sign regularmente.

a) Autoridade de Registo Interna

No âmbito da Entidade de Certificação Global Trusted Sign, a autoridade de registo é executada pelos serviços internos da mesma, que têm responsabilidade de validação dos dados necessários, conforme explicitado nas Políticas especificas da Global Trusted Sign, para cada um dos serviços disponibilizados.

b) Autoridade de Registo Externa

A Global Trusted Sign, não dispõe de Autoridades de Registo Externas.

9.6.3. Representações e Garantias dos Subscritores/Titulares

É obrigação dos titulares dos certificados emitidos cumprir as diretivas seguintes:

- Limitar e adequar a utilização dos certificados de acordo com a legislação vigente e com as utilizações previstas no presente documento;
- Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;
- Solicitar de imediato a revogação de um certificado, em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado, de acordo com os procedimentos especificados no presente documento;
- Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspendido ou por ter expirado o período de validade;
- Submeter às Entidades Certificadoras (ou de Registo) a informação que considerem exata e completa em relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;
- Não monitorizar, manipular ou efetuar ações de “engenharia inversa” sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da EC GTS.

9.6.4. Representações e Garantias das Partes Confiantes

É obrigação das partes confiantes dos certificados emitidos pela EC GTS:

- Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com a legislação vigente e com o presente documento;
- Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
- Assumir a responsabilidade na correta verificação das assinaturas digitais;
- Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;
- Assumir a responsabilidade na correta verificação dos certificados emitidos;
- Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;
- Notificar qualquer acontecimento ou situação anómala relativa aos certificados, utilizando os meios que a EC GTS publique no seu espaço Web.

9.6.5. Representações e Garantias de outros Participantes

Não estipulado.

9.7. Renúncia de Garantias

A EC GTS recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

9.8. Limitações de Responsabilidade

A EC GTS responde pelos danos ou prejuízos causados aos utilizadores finais e partes confiantes decorrentes da sua atividade, conforme legislação aplicável. A EC GTS não se responsabiliza por qualquer dano ou prejuízo decorrente utilizações abusivas ou fora do âmbito do contrato estabelecido com os utilizadores e/ou partes confiantes. A EC GTS não assume qualquer responsabilidade em caso falha dos serviços relacionada com causas de força maior, como desastres naturais, guerra ou outros similares.

9.9. Indemnizações

A EC GTS assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável em vigor.

9.10. Prazo e Terminação

9.10.1. Prazo

Esta DPC entra em vigor desde o momento de sua publicação no repositório da EC GTS e após aprovação, nos termos do presente documento. Esta DPC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão, nos termos do presente documento, ou pela renovação das chaves da EC GTS, momento em que, obrigatoriamente, se redigira uma nova versão.

9.10.2. Terminação

Esta DPC será substituída por uma nova versão, com independência da transcendência das mudanças efetuadas na mesma, de modo que será sempre de aplicação na sua totalidade. Quando a DPC ficar revogada será retirada do repositório público, garantindo-se, contudo, que será conservada durante o período definido no presente documento.

9.10.3. Efeito da Terminação e Sobrevivência

As obrigações e restrições que estabelece esta DPC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da EC GTS, nascidas sob a sua vigência, subsistirão após sua substituição ou revogação, por uma nova versão, em tudo o que não se oponha a esta.

9.11. Notificações Individuais e Comunicações aos Participantes

Todos os participantes devem utilizar os mecanismos apropriados para a comunicação coletiva, onde se engloba o correio eletrónico assinado digitalmente, correio postal e formulários assinados, entre outros, recorrendo ao meio mais adequando em função da natureza de cada assunto.

9.12. Alterações

9.12.1. Procedimento para Alteração

As alterações a esta DPC devem ser aprovadas pelo Grupo de Gestão. As alterações devem ser efetuadas através de documentos, contendo as novas alterações à DPC.

9.12.2. Mecanismo de Notificação e Período

No caso em que o Grupo de Gestão julgue que as mudanças à especificação podem afetar a aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores dos certificados correspondentes, que se efetuou uma mudança e que devem consultar a nova DPC no

repositório estabelecido. O mecanismo de comunicação será o sítio da internet https://www.globaltrustedsign.com.

9.12.3. Circunstâncias nas quais o OID deve ser alterado

Se a EC GTS determinar que a alteração ao identificador (OID) da DPC ou política de certificados é necessária, a alteração deve conter os novos identificadores. De outra forma, as alterações não devem implicar uma mudança no identificador da política de certificados.

9.13. Disposições de Resolução de Conflito

As reclamações devem ser endereçadas ao Grupo de Gestão da EC GTS, através de carta registada. Qualquer litígio decorrente da interpretação ou aplicação deste documento regem-se pela lei portuguesa. Para regular esses litígios, as partes elegem o foro judicial da Comarca de Funchal, com exclusão de qualquer outro. Todas as reclamações entre os utilizadores e a EC GTS poderão ser comunicadas à Entidade Supervisora com a finalidade da resolução de conflitos que possam eventualmente surgir.

9.14. Legislação Aplicável

A seguinte legislação é aplicável às entidades certificadoras prestadoras de serviços de confiança:

- Regulamento (UE) N. o 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.
- Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

9.15. Conformidade com a Legislação Aplicável

O presente documento (DPC) é objeto de aplicação de leis nacionais e Europeias, regras, regulamentos, ordenações, decretos e ordens incluindo, mas não limitadas a restrições na exportação ou importação de software, hardware ou informação técnica.

Se um tribunal ou órgão governamental com jurisdição sobre as atividades cobertas por esta DPC determinar que o cumprimento de qualquer requisito obrigatório é ilegal ou não adequado ao país onde a EC está implementada, tal requisito será considerado reformulado na extensão mínima necessária para tornar o requisito válido e legal. Isso se aplica apenas a operações ou emissões de certificados que estão sujeitas às leis dessa jurisdição. A GTS compromete-se a notificar o CA/ Browser Fórum sobre os fatos, circunstâncias e leis envolvidas, para que o CA/ Browser Fórum possa reavaliar estas Diretrizes em conformidade.

9.16. Outras Disposições

9.16.1. Acordo Completo

As partes confiantes assumem, na sua totalidade, o conteúdo da última versão desta DPC. Em caso, de existirem uma ou mais estipulações do presente documento, que sejam ou tendam a ser inválidas, nulas, ou irreclamáveis em termos jurídicos, deverão ser consideradas como não efetivas. Estas determinações são válidas, apenas e só apenas nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade do Grupo de Gestão avaliar a essencialidade das mesmas. As práticas adotadas pela EC GTS garantem a independência dos membros dos grupos de confiança e da administração de topo, e a liberdade face a pressões comerciais, financeiras ou outras que possam influenciar a confiança nos serviços por eles prestados. A EC GTS garante as condições para que os seus serviços da sua hierarquia sejam utilizados por pessoas com deficiência, em conformidade com o regulamento europeu 910/2016.

9.16.2. Atribuição

As partes que operam no âmbito desta DPC ou acordos aplicáveis não podem atribuir os seus direitos ou obrigações sem o prévio consentimento por escrito do Grupo de Confiança da GTS.

9.16.3. Severidade

Se uma disposição desta DPC, incluindo cláusulas de limitação de responsabilidade, for considerada ineficaz ou não executável, a restante desta DPC deve ser interpretada no sentido da intenção original das partes. Qualquer disposição desta DPC que estabeleça uma limitação de responsabilidade deve ser segregável e independente de qualquer outra disposição e deve ser aplicada como tal.

9.16.4. Execução (Honorários de Advogados e Renúncia de Direitos)

A GTS pode requerer a indemnização e honorários advocatícios de uma parte por danos, perdas e/ou despesas relacionadas com a conduta dessa parte. A falha da GTS em aplicar uma cláusula desta DPC não renuncia ao direito da GTS de aplicar a mesma cláusula posteriormente ou ao direito de aplicar quaisquer outras cláusulas desta DPC. Para ter efeito, qualquer renúncia deve ser feita por escrito e assinada pela GTS.

9.16.5. Força Maior

As cláusulas de força maior estão incluídas nas Condições Gerais de Emissão – FO31.

9.17. Outras Provisões

Não estipulado.

Assinado com Assinatura
Digital Qualificada por:
TOLENTINO DE DEUS
FARIA PEREIRA
Data: 06-07-2023 12:49:15