

XXVI - direito de acesso - privilégio associado a um cargo, pessoa ou processo, para ter acesso a um ativo.

XXVII - disponibilidade - propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

XXVIII - dispositivos móveis - equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: e-books, notebooks, netbooks, smartphones, tablets, pendrives, USBdrives, HD externo, e cartões de memória.

XXIX - documentos classificados - documentos que contenham informação classificada em qualquer grau de sigilo.

XXX - eliminação - exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado.

XXXI - e-mail - sigla de correio eletrônico (electronic mail)

XXXII - encarregado - pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

XXXIII - equipe de prevenção, tratamento e resposta a incidentes cibernéticos - grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede.

XXXIV - estruturado - munido de organização, o que é estruturalmente organizado.

XXXV - gestão de continuidade de negócios em segurança da informação - processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

XXXVI - gestão de incidentes cibernéticos: processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação do Ministério do Turismo.

XXXVII - gestão de riscos em segurança da informação - processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

XXXVIII - gestão de segurança da informação - processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação.

XXXIX - gestão de vulnerabilidades técnicas: processo que visa prevenir a exploração de vulnerabilidades na rede corporativa do Ministério do Turismo por meio da aplicação sistemática de ações de identificação, classificação e tratamento de vulnerabilidades, sendo regulamentada por norma interna de segurança da informação do Ministério do Turismo, conforme diretrizes desta Política de Segurança da Informação.

XL - gestor de segurança da informação - responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

XLI - gestor de segurança e credenciamento - responsável pela segurança da informação classificada, em qualquer grau de sigilo, nos órgãos de registro e postos de controle.

XLII - guerra cibernética - atos de guerra, utilizando predominantemente elementos de tecnologia da informação em escala suficiente, por um período específico e em alta velocidade, em apoio às operações militares, por meio de ações tomadas exclusivamente no espaço cibernético, com a finalidade de abalar ou de incapacitar as atividades de uma nação inimiga, especialmente pelo ataque aos sistemas de comunicação, visando obter vantagem operacional militar significativa.

XLIII - incidente cibernético - ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema.

XLIV - incidente de segurança - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

XLV - informação - dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

XLVI - informação classificada em grau de sigilo: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é e que pode ser classificada como ultrassecreta, secreta ou reservada.

XLVII - informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, à vida privada, à honra e à imagem.

XLVIII - informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado e aquela abrangida pelas demais hipóteses legais de sigilo.

XLIX - integridade - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

L - internet - rede global, composta pela interligação de inúmeras redes, provendo comunicação e informações das mais variadas áreas de conhecimento.

LI - invasão - incidente de segurança no qual o ataque foi bem-sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema de organização.

LII - log (registro de auditoria) - registro de eventos relevantes em um dispositivo ou sistema computacional;

LIII - medidas de segurança - medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

LIV - níveis de acesso - especificam quanto de cada recurso ou sistema o usuário pode utilizar.

LV - perfil de acesso - conjunto de atributos, de cada usuário, definidos previamente como necessários para credencial de acesso.

LVI - perfil institucional - cadastro do órgão ou entidade da administração pública federal como usuário em redes sociais, alinhado ao planejamento estratégico e à Política de Segurança da Informação da instituição, com observância de sua correlata atribuição e competência.

LVII - periódico - que ocorre em regulares intervalos de tempo.

LVIII - política de segurança da informação - documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação. Este termo substituiu o termo Política de Segurança da Informação e Comunicação.

LIX - prestador de serviço - pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.

LX - rede de computadores - conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação.

LXI - redes sociais - estruturas sociais digitais, compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

LXII - reduzir risco - forma de tratamento de risco na qual a alta administração decide realizar a atividade adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

LXIII - segurança cibernética - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

LXIV - segurança da informação - ações que objetiva viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

LXV - serviços - meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos.

LXVI - sistema de informação - conjunto de elementos materiais ou intelectuais colocado à disposição dos usuários em forma de serviços ou bens que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada.

LXVII - termo de compromisso de manutenção de sigilo - termo utilizado para garantir o sigilo de uma informação classificada em grau de sigilo em caráter excepcional, mediante assinatura de pessoa natural não credenciada ou não autorizada por legislação.

LXVIII - termo de responsabilidade - termo assinado pelo usuário com a sua concordância em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

LXIX - tratamento da informação - conjunto de ações referente à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

LXX - tratamento da informação classificada - conjunto de ações referente à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada, independente do meio, suporte ou formato.

LXXI - trilha de auditoria - registro ou conjunto de registros gravado em arquivos de log ou outro tipo de documento ou mídia que possa indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

LXXII - uso compartilhado de dados - comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais, por órgãos e entidades públicas, no cumprimento de suas competências legais, ou entre esses entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

LXXIII - usuário de informação - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.

#### ANEXO II

##### TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu, \_\_\_\_\_, CPF nº \_\_\_\_\_, Carteira de Identidade nº \_\_\_\_\_, expedida pelo \_\_\_\_\_ em \_\_\_\_\_, lotado(a) no(a) \_\_\_\_\_, deste Ministério, na qualidade

de USUÁRIO ou CUSTODIANTE de informações do Ministério do Turismo, declaro ter CONHECIMENTO da Política de Segurança da Informação (POSIN), segundo a qual devo cumprir todas as suas diretrizes e orientações.

Estou ciente de meu compromisso no Ministério do Turismo e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto na POSIN do MTur e na legislação vigente.

Brasília - DF, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_

Assinatura  
(Usuário de Informação)

#### ANEXO III

##### TERMO DE CONFIDENCIALIDADE

A \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, sediada \_\_\_\_\_, por intermédio de seu representante legal, o Sr. (a) \_\_\_\_\_, portador(a) da Cédula de Identidade nº \_\_\_\_\_, expedida pelo (a) \_\_\_\_\_ e CPF nº \_\_\_\_\_, declara que, para fins da execução do contrato nº \_\_\_\_\_, comprometemo-nos a manter em sigilo, ou seja, não revelar ou divulgar as informações

confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços nas instalações do Ministério do Turismo, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a eles se referem e ainda respeitar as normas internas de segurança da informação vigentes.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar o Ministério do Turismo de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, danos, perdas, custas e despesas que porventura venha a sofrer como resultado da violação do disposto neste instrumento.

## Controladoria-Geral da União

### SECRETARIA EXECUTIVA

#### PORTARIA Nº 3.045, DE 11 DE SETEMBRO DE 2023

A SECRETARIA-EXECUTIVA DA CONTROLADORIA-GERAL DA UNIÃO, com fundamento no inciso IV do artigo 8º do Anexo I do Decreto nº 11.330, de 1º de janeiro de 2023, e no uso das atribuições previstas no art. 8º do Regimento Interno da CGU, aprovado pela Portaria Normativa CGU nº 38, de 16 de dezembro de 2022, resolve:

Art. 1º Delegar competência aos ocupantes dos seguintes cargos para a prática dos atos de gestão orçamentária e financeira referentes às Unidades Gestoras Executoras 370002/COGEP/DGC/SE/CGU e 370003/CGLCD/DGC/SE/CGU:

RESPONSÁVEL	ENCARGO
Diretor de Gestão Corporativa	Ordenador de Despesas
Diretor de Gestão Corporativa - Substituto	Ordenador de Despesas - Substituto
Coordenador-Geral de Orçamento, Finanças e Contabilidade	Gestor Financeiro
Coordenador-Geral de Orçamento, Finanças e Contabilidade - Substituto	Gestor Financeiro - Substituto

Art. 2º Nos casos de afastamentos legais do Coordenador-Geral de Orçamento, Finanças e Contabilidade - Substituto fica delegado ao Coordenador de Execução Orçamentária e Financeira o encargo de Gestor Financeiro - Substituto.

Art. 3º Fica revogada a Portaria nº 1.974, de 20 de agosto de 2021.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

VÂNIA LÚCIA RIBEIRO VIEIRA

