



BOLETIM DE SERVIÇOS

Nº 7, DE 28 JANEIRO DE 2022



Ministério das Comunicações

Secretaria-Executiva

Subsecretaria de Orçamento e Administração



BOLETIM DE SERVIÇO N.º 7



BRASÍLIA/DF

28 de janeiro de 2022

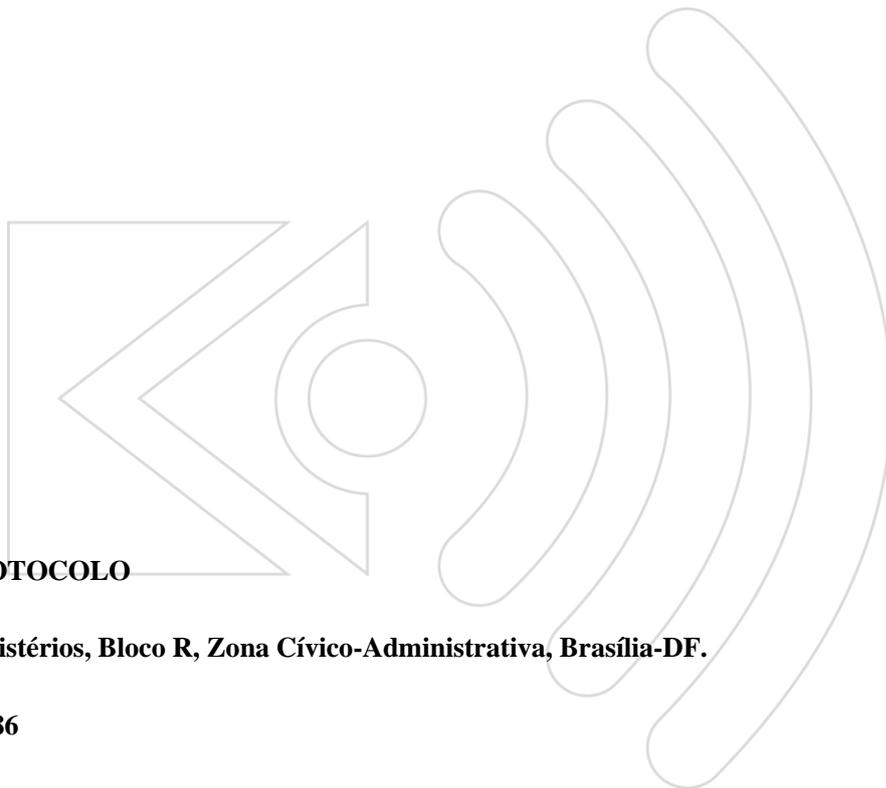
MINISTRO DAS COMUNICAÇÕES Fábio Faria
SECRETÁRIA-EXECUTIVA Maria Estella Dantas Antonichelli
SECRETÁRIA-EXECUTIVA ADJUNTA Flávia Duarte Nascimento
SUBSECRETÁRIO DE ORÇAMENTO E ADMINISTRAÇÃO Djair Fiorillo Lopes

APRESENTAÇÃO

O Boletim de Serviço – BS é uma publicação que Ministério das Comunicações - MCom edita em cumprimento à Lei 4.965, de 05 de maio de 1966, que “dispõe sobre a publicação dos atos relativos aos servidores públicos civis do Poder Executivo e dá outras providências”, e em consonância com a Portaria n.º 283, de 02 de outubro de 2018, da Imprensa Nacional.

Este periódico é veiculado diariamente, sendo constituído por atos administrativos de natureza interna da Instituição, tais como: designação de equipes de contratação, designação de gestores e fiscais contratuais, afastamentos, viagens a serviço, diárias, licenças, comunicação de férias, bem como outras vantagens cuja publicação é dispensável no Diário Oficial da União.

Desta forma, o Boletim de Serviço constitui-se em um instrumento formal que objetiva a transparência e, sobretudo, a legalidade dos atos da administração do MCom.



SERVIÇO DE PROTOCOLO

Esplanada dos Ministérios, Bloco R, Zona Cívico-Administrativa, Brasília-DF.

CEP: 70044-902

Fone: (61) 2027-6386

Boletim de Serviço / Ministério das Comunicações

Serviço de Protocolo.

Brasília: Mcom, 2022.

Páginas 25

Periodicidade Diária

I. Boletim de Serviço.

II. Brasil. Ministério das Comunicações.



SUMÁRIO

SUMÁRIO	
Atos da Subsecretaria de Orçamento e Administração	
PORTARIA Nº 4522, DE 24 DE JANEIRO DE 2022	7
PORTARIA Nº 4527, DE 25 DE JANEIRO DE 2022	8
PORTARIA Nº 4530, DE 25 DE JANEIRO DE 2022	9
PORTARIA Nº 4545, DE 28 DE JANEIRO DE 2022	10
PORTARIA MCOM Nº 4.547/2021 DE 28 DE JANEIRO DE 2021	11
PORTARIA MCOM Nº 4.549/2021 DE 28 DE JANEIRO DE 2021	17
DESPACHO Nº 9263653 DE 28 DE JANEIRO DE 2022	22
DESPACHO Nº 9263844 DE 27 DE JANEIRO DE 2022	23
DESPACHO Nº 9291795 DE 27 DE JANEIRO DE 2022	24



PORTARIA Nº 4522, DE 24 DE JANEIRO DE 2022

O COORDENADOR GERAL DE RECURSOS LOGÍSTICOS DO MINISTÉRIO DAS COMUNICAÇÕES, no uso da competência que lhe foi atribuída pela Portaria MCOM nº 2.388, de 12 de abril de 2021; Portaria nº 3.408, de 19 de agosto de 2020; Portaria MCOM nº 3.525, de 3 de setembro de 2021; Lei nº 10.520, de 17 de julho de 2002; Decreto nº 3.555, de 08 de agosto de 2000; Decreto nº 10.024, de 20 de setembro de 2019; e a Lei nº 8.666, de 21 de junho de 1993, resolve:

Art. 1º Designar os servidores abaixo relacionados para compor a Equipe de Planejamento da Contratação, que elaborará os documentos elencados na Instrução Normativa nº 1, de 4 de abril de 2019, alterada pela Instrução Normativa nº 31, de 23 de março de 2021, referentes à contratação de solução de conectividade de Datacenter.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Filipe Carneiro Guimarães	Integrante Requisitante	SIAPE: 1443304
Victor Henrique Hisao Taira	Integrante Requisitante Substituto	SIAPE: 2270979
Alessandro Magalhães Cosenza	Integrante Técnico	SIAPE: 3251200
Jair Rodrigues Fernandes	Integrante Técnico Substituto	SIAPE: 3213825
José Alves Tavares Mendes	Integrante Administrativo	SIAPE: 2276407
Cristiane Reis Peixoto Serra	Integrante Administrativo Substituto	SIAPE: 3220162

Art. 2º Cada integrante deverá colaborar com a equipe considerando suas competências e habilidades, bem como observar as atividades e requisitos especificados no Documento de Indicação da Equipe de Planejamento que previamente notificou sobre a designação e atribuições.

Art. 3º Fica revogada a Portaria nº 4376, de 27 de dezembro de 2021.

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

IVANCIR GONÇALVES DA ROCHA CASTRO FILHO

Coordenador-Geral de Recursos Logísticos



PORTARIA Nº 4527, DE 25 DE JANEIRO DE 2022

O COORDENADOR GERAL DE RECURSOS LOGÍSTICOS DO MINISTÉRIO DAS COMUNICAÇÕES, no uso da competência que lhe foi atribuída pela Portaria MCOM nº 2.388, de 12 de abril de 2021; Portaria nº 3.408, de 19 de agosto de 2020; Portaria MCOM nº 3.525, de 3 de setembro de 2021; Lei nº 10.520, de 17 de julho de 2002; Decreto nº 3.555, de 08 de agosto de 2000; Decreto nº 10.024, de 20 de setembro de 2019; e a Lei nº 8.666, de 21 de junho de 1993, resolve:

Art. 1º Designar os servidores abaixo relacionados para compor a Equipe de Planejamento da Contratação, que elaborará os documentos elencados na Instrução Normativa nº 5, de 26 de maio de 2017, referentes à contratação de serviço de locação de veículos em âmbito nacional, exceto o Distrito Federal, tipo automóvel sedã, com motorista, para transporte de autoridades e servidores em serviço, sob demanda, incluindo despesas com combustível, manutenção, seguro, pessoal, diárias, pedágios e demais custos inerentes que incidem sobre os veículos.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

José Alves Tavares Mendes	Integrante Requisitante	SIAPE: 3220028
Adriana da Silva Cavalcante	Integrante Requisitante Substituta	SIAPE: 3211373

Art. 2º Cada integrante deverá colaborar com a equipe considerando suas competências e habilidades, bem como observar as atividades e requisitos especificados no Documento de Indicação da Equipe de Planejamento que previamente notificou sobre a designação e atribuições.

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

IVANCIR GONÇALVES DA ROCHA CASTRO FILHO
Coordenador-Geral de Recursos Logísticos



PORTARIA Nº 4530, DE 25 DE JANEIRO DE 2022

O COORDENADOR GERAL DE RECURSOS LOGÍSTICOS DO MINISTÉRIO DAS COMUNICAÇÕES, no uso da competência que lhe foi atribuída pela Portaria MCOM nº 2.388, de 12 de abril de 2021; Portaria nº 3.408, de 19 de agosto de 2020; Portaria MCOM nº 3.525, de 3 de setembro de 2021; Lei nº 10.520, de 17 de julho de 2002; Decreto nº 3.555, de 08 de agosto de 2000; Decreto nº 10.024, de 20 de setembro de 2019; e a Lei nº 8.666, de 21 de junho de 1993, resolve:

Art. 1º Designar os servidores abaixo relacionados para compor a Equipe de Planejamento da Contratação, que elaborará os documentos elencados na Instrução Normativa nº 5, de 26 de maio de 2017, referentes ao atendimento dos serviços de apoio administrativo, com contratação de empresa especializada na prestação, de forma contínua, de serviços de apoio administrativo de Carregador/Estiva, a serem executados nas dependências do Ministério das Comunicações.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Adriana da Silva Cavalcante	Integrante Requisitante	SIAPE: 3211373
José Alves Tavares Mendes	Integrante Requisitante Substituto	SIAPE: 3220028

Art. 2º Cada integrante deverá colaborar com a equipe considerando suas competências e habilidades, bem como observar as atividades e requisitos especificados no Documento de Indicação da Equipe de Planejamento que previamente notificou sobre a designação e atribuições.

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

IVANCIR GONÇALVES DA ROCHA CASTRO FILHO
Coordenador-Geral de Recursos Logísticos



PORTARIA Nº 4545, DE 28 DE JANEIRO DE 2022

O COORDENADOR GERAL DE RECURSOS LOGÍSTICOS DO MINISTÉRIO DAS COMUNICAÇÕES, no uso da competência que lhe foi atribuída pela Portaria MCOM nº 2.388, de 12 de abril de 2021; Portaria nº 3.408 de 19 de agosto de 2021; Portaria MCOM nº 3.525, de 3 de setembro de 2021, conforme Instrução Normativa nº 05, de 26 de maio de 2017, e tendo em vista o disposto na Lei n.º 8.666, de 21 de junho de 1993, resolve:

Art. 1º Designar os servidores abaixo relacionados para compor a Equipe de Planejamento que irá elaborar os documentos elencados na IN nº 05/2017-SEGES/ME, referente à contratação de empresa especializada na prestação de serviço de transporte, “porta a porta”, de mobiliário em geral (mudança) de propriedade dos servidores e seus dependentes, cargas e volumes fracionados, veículos automotores e outros bens de propriedade ou interesse do Ministério das Comunicações, na modalidade terrestre, com abrangência nacional, intermunicipal ou interestadual.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Nome	SIAPE
Adriana da Silva Cavalcante	3211373
Cristiane Reis Peixoto Serra	3220162
José Alves Tavares Mendes	3220028

Art. 2º A equipe designada deverá observar a Instrução Normativa nº 05, de 26 de maio de 2017, e suas alterações, bem como legislação pertinente, no que couber, para executar as atribuições de planejamento do Contrato.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

IVANCIR GONÇALVES DA ROCHA CASTRO FILHO
Coordenador-Geral de Recursos Logísticos



PORTARIA MCOM Nº 4.547/2021 DE 28 DE JANEIRO DE 2021

Aprova a Norma Complementar para Cópia de Segurança e Restauração de Dados .

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Cópia de Segurança e Restauração de Dados.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS

OBJETIVO

Esta norma tem por objetivo estabelecer a política de cópia de segurança e restauração de dados com as diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Coordenação-Geral de Tecnologia da Informação (CGTI), visando garantir a segurança, integridade e disponibilidade no âmbito do Ministério das Comunicações - MCOM.

APLICAÇÃO

Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

REFERÊNCIA LEGAL E NORMATIVA

Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação;

Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;

Portaria MCOM Nº 67, de 4 de março de 2021, que designa a Gestora de Segurança da Informação do



Ministério das Comunicações.

Acórdão nº 1109/2021 – TCU – Plenário, de 12 de maio de 2021.

1. CONCEITOS E DEFINIÇÕES:

- 1.1. Administrador de backup: agente público responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes, testes dos procedimentos de backup e restauração. O Coordenador de Infraestrutura e Serviços de Tecnologia da Informação deve ser designado com Administrador de Backup. O respectivo substituto deve ser designado entre os empregados ou servidores públicos da CGTI;
- 1.2. Gestor da informação: agente público formalmente responsável pela administração do serviço de TI e/ou sistema e pelas informações produzidas em seu processo de trabalho. Preferencialmente, deve ser um gestor da área negocial. O respectivo substituto deve ser, preferencialmente, da área negocial;
- 1.3. Ativo: tudo que tenha valor para a organização, material ou não (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional);
- 1.4. Backup: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;
- 1.5. Backup Completo (Full): modalidade de backup em que todos os dados a serem guardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup;
- 1.6. Backup Diferencial: modalidade de backup em que são guardados apenas dados novos ou modificados desde o último backup completo efetuado;
- 1.7. Backup Incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup - seja ele completo, diferencial ou incremental - são guardados;
- 1.8. Base de Dados ou Banco de Dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;
- 1.9. Código fonte: é o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica;
- 1.10. Criticidade: grau de importância da informação para a continuidade das atividades e serviços;
- 1.11. Custódia: consiste na responsabilidade de guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;
- 1.12. Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;
- 1.13. Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;
- 1.14. 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;
- 1.15. Incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
- 1.16. Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- 1.17. Janela de Backup: intervalo de tempo durante o qual as cópias de segurança sob execução



agendada ou manual poderão ser executadas;

1.18. Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

1.19. Mídia: mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, compact disk (CD), fitas, papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

1.20. Nuvem: composta de rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema. Estes servidores são responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer serviços ou conteúdos, que podem ser acessados de qualquer dispositivo com acesso à Internet;

1.21. Plano de Backup: Documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de Backup;

1.22. Repositório de Arquivo: Conjunto de documentos ou lugar onde os documentos são guardados;

1.23. Retenção: intervalo de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração; e

1.24. Rotina de Backup: procedimentos de realização de cópias de segurança.

2 DISPOSIÇÕES GERAIS

2.1. Esta Norma Complementar aplica-se a todos sistemas, bases de dados, máquinas físicas ou virtuais e repositórios de arquivos institucionais, em formato digital, em uso e de propriedade do Ministério das Comunicações.

2.2. Deverá ser elaborado um Plano de Backup, conforme requisitos presentes no item 3.1.3 desta Norma, para todos os sistemas, bases de dados, máquinas físicas ou virtuais e repositórios de arquivos institucionais do MCOM que serão objeto de cópias de segurança, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização.

2.3. Os dados armazenados localmente, em microcomputadores dos usuários ou em quaisquer outros dispositivos fora do centro de processamento de dados mantido pelo MCOM, ou que não façam parte de um plano de backup formalmente definido não terão backup e não haverá garantia de recuperação.

2.4. A guarda dos dados em formato digital pertencentes ao MCOM, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, devem estar garantidos nos acordos ou contratos que formalizam a relação entre os envolvidos.

2.5. São atribuições do administrador de backup:

- a) propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo MCOM;
- b) providenciar a criação e manutenção dos backups;
- c) configurar as soluções de backup;
- d) manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
- e) definir os procedimentos de restauração e neles auxiliar;
- f) verificar os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;
- g) tomar medidas preventivas para evitar falhas;

- h) gerenciar mensagens e registros de auditoria (LOGs) de execução dos backups;
- i) disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;
- j) solicitar restaurações de dados, com anuência do gestor da informação;
- k) propor modificações visando ao aperfeiçoamento desta Norma; e
- l) providenciar a execução dos testes de restauração.

2.6. São atribuições dos gestores da informação:

- a) solicitar, formalmente, a guarda das informações geridas;
- b) solicitar, formalmente, a recuperação dos dados;
- c) autorizar a solicitação de recuperação de dados feitas pela CGTI;
- d) validar, negocialmente, o resultado das restaurações eventualmente solicitadas; e
- e) validar, negocialmente, o resultado dos testes de restauração dos backups.

3 PROCEDIMENTOS

3.1. Solicitação de backup

3.1.1. As solicitações de backup devem ser realizadas pelo gestor da informação, em formulário específico no Sistema de Processo Eletrônico, e enviadas ao administrador de backup.

3.1.2. O administrador de backup analisará a solicitação.

3.1.2.1. Não sendo viável o atendimento da solicitação, o administrador de backup encaminhará, pelo Sistema de Processo Eletrônico, resposta ao gestor da informação.

3.1.2.2. Sendo viável o atendimento, o administrador de backup deverá elaborar o Plano de Backup em conjunto com o gestor da informação, de modo a atender as necessidades específicas de negócio.

3.1.2.3. O administrador de backup, caso identifique a necessidade de guarda de informação, pode entrar em contato com o gestor da informação para a elaboração, em conjunto, do Plano de Backup.

3.1.3. O Plano de Backup, assinado pelo gestor da informação e pelo administrador do backup, deverá conter, no mínimo, as seguintes informações:

- a) escopo: dados digitais a serem salvaguardados, com apontamento do local, tais como:
 - i) código fonte;
 - ii) banco de dados;
 - iii) repositório de arquivos;
 - iv) arquivos de configuração de servidores e ativos de rede; e
 - v) máquinas virtuais.
- b) tipo de backup: completo, incremental, diferencial, podendo ser uma associação destes;
- c) frequência temporal de realização do backup: diária, semanal, mensal, anual, podendo ser uma associação destes;
- d) retenção: período em que o dado copiado no backup ficará retido e disponível para uso numa eventual recuperação antes de ser substituído por uma versão mais nova). Deverá ser definido com base na criticidade, frequência da atualização dos dados e características específicas de cada sistema;
- e) unidade de armazenamento: indicação da unidade de armazenamento a ser utilizada, podendo ser storage, fita ou outras unidades em uso no MCOM.
- f) local de armazenamento: indicação da localização de armazenamento do backup, incluindo se o backup



- é acessível por meio da rede, se não é acessível pela rede ou se a unidade de armazenamento se encontra em outra localidade remota, sendo em serviço de nuvem ou em edifício distinto do MCOM;
- g) testes previstos: devem ser previstos a periodicidade, a abrangência e os procedimentos relativos aos testes que serão realizados;
 - h) procedimento de recuperação: documentar o procedimento para recuperar o backup quando necessário.
 - i) logs: previsão de criação e armazenamento de registros sobre a execução dos testes e das recuperações realizadas, a fim de detectar eventuais falhas e assegurar que houve a realização integral do backup.
 - j) RPO (recovery point objective): indicador que mensura o prazo máximo de perda dados em caso de incidentes; e
 - k) RTO (recovery time objective): indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após um incidente.

3.1.4. Os backups devem ter, no mínimo, duas cópias realizadas em unidades de armazenamento distintos, sendo um online e outro offline ou disposto em outra localidade.

3.1.5. Os Planos de Backup devem ser criados e executados conforme os dispositivos desta Norma.

3.2. Rotinas de backup

3.2.1. As rotinas de backup devem ser realizadas em soluções específicas e próprias para esta finalidade, preferencialmente de forma automatizada.

3.2.2. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TI.

3.2.3. Os backups devem estar em conformidade com a legislação vigente, em especial ao que compete à LGPD.

3.2.4. Os backups, quando couber, devem ser criptografados, considerando as melhores práticas de mercado, normas vigentes e as ferramentas disponíveis.

3.2.5. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

3.2.6. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do MCOM, garantindo que o tráfego necessário às suas atividades não ocasione problemas aos demais serviços de TI.

3.2.7. A realização do backup deve ser, preferencialmente, concentrada no período de janela de backup, definido pela CGTI.

3.2.8. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos gestores das informações.

3.3. Armazenamento de backup

3.3.1. Todos os ativos relacionados ao armazenamento dos backups devem ser acondicionados em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de backup.

3.3.2. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

3.4. Testes de backup

3.4.1. Os backups devem ser testados periodicamente, com o objetivo de garantir a confiabilidade e a integridade dos dados salvaguardados.

3.4.2. Os testes de restauração dos backups devem ser realizados em equipamentos diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

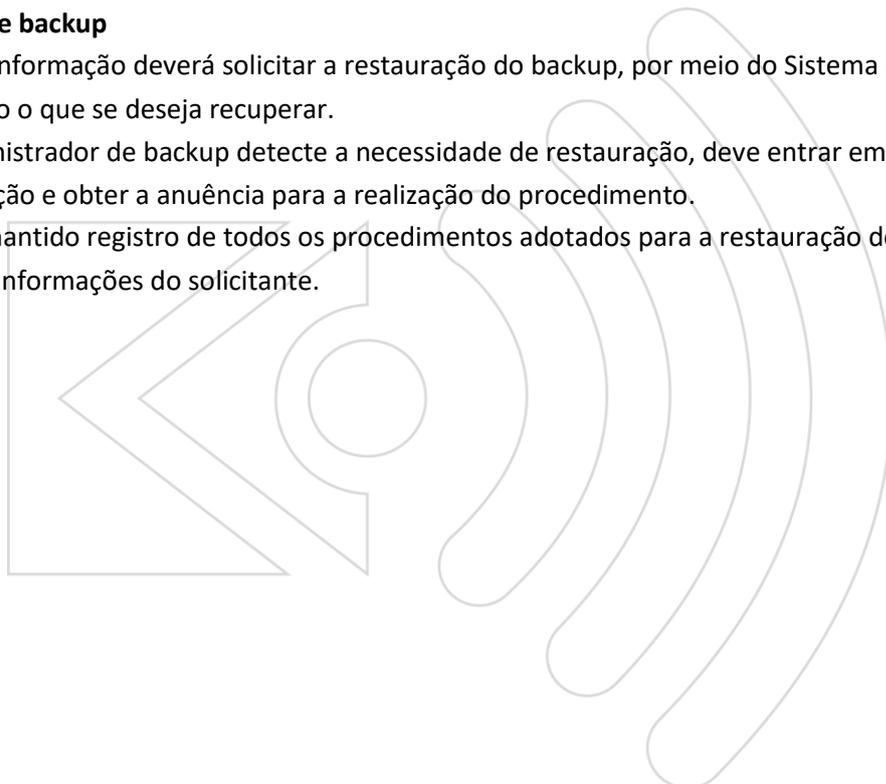
3.4.3. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup devem ser devidamente registradas no plano de backup.

3.5. Restauração de backup

3.5.1. O gestor da informação deverá solicitar a restauração do backup, por meio do Sistema de Processo Eletrônico, indicando o que se deseja recuperar.

3.5.2. Caso o administrador de backup detecte a necessidade de restauração, deve entrar em contato com o gestor da informação e obter a anuência para a realização do procedimento.

3.5.3. Deverá ser mantido registro de todos os procedimentos adotados para a restauração do backup, juntamente com as informações do solicitante.





PORTARIA MCOM Nº 4.549/2021 DE 28 DE JANEIRO DE 2021

Aprova a Norma Complementar para Inventário e Mapeamento de Ativos de Informação.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Inventário e Mapeamento de Ativos de Informação.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

OBJETIVO

Estabelecer diretrizes para o Processo de Inventário e Mapeamento de Ativos de Informação do Ministério das Comunicações - MCOM.

APLICAÇÃO

Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

REFERÊNCIA LEGAL E NORMATIVA

Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;

Portaria MCOM Nº 67, de 4 de março de 2021, que designa a Gestora de Segurança da Informação do Ministério das Comunicações;

Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação;

Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

Revisão 01 da Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.



1. CONCEITOS E DEFINIÇÕES:

- 1.1. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
- 1.2. Agente responsável pela gestão de ativos: servidor público ou empregado público, ocupante de cargo efetivo incumbido de gerenciar o processo de inventário e mapeamento de ativos de informação;
- 1.3. Ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
- 1.4. Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
- 1.5. Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;
- 1.6. Contêiner dos ativos de informação: local onde se encontra o ativo de informação. Geralmente, um contêiner descreve algum tipo de ativo tecnológico -hardware, software ou sistema de informação (mas também pode se referir a pessoas ou mídias como papel, CD-ROM ou DVD-ROM). Um contêiner, portanto, é qualquer tipo de ativo dentro do qual um ativo de informação é armazenado, transportado ou processado. Ele pode ser um único ativo tecnológico (como um servidor), uma coleção de ativos tecnológicos (como uma rede) ou uma coletânea de mídias digitais, entre outros;
- 1.7. Custodiante da informação: qualquer indivíduo ou estrutura de órgão ou entidade da administração pública federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança, em conformidade com as exigências de segurança da informação, comunicadas pelo proprietário da informação;
- 1.8. 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;
- 1.9. Documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;
- 1.10. Gestão de Continuidade de Negócios: 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;
- 1.11. Gestão de Riscos de 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;
- 1.12. Gestor de segurança da informação e comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do MCOM;
- 1.13. Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- 1.14. Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- 1.15. Proprietário da informação: parte interessada do órgão ou entidade da administração pública federal, direta e indireta, ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;
- 1.16. Valor do ativo de informação: valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos do MCOM, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado;
- 1.17. Vulnerabilidade: condição que, quando explorada por um criminoso cibernético, pode resultar



em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha;

2 DISPOSIÇÕES GERAIS

2.1. O processo de inventário e mapeamento de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

2.2. O processo de mapeamento de ativos de informação deve considerar, preliminarmente:

- a) os objetivos estratégicos da organização;
- b) os processos internos da organização;
- c) os requisitos legais; e
- d) a estrutura do órgão ou da entidade.

2.3. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter:

- a) os responsáveis - proprietários e custodiantes - de cada ativo de informação;
- b) as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação;
- c) os contêineres de cada ativo de informação; e
- d) as interfaces de cada ativo de informação e as interdependências entre eles.

2.4. O registro de ativos de informação deverá ser homologado por meio de ato do titular do órgão ou da entidade.

2.5. O Processo de Inventário e Mapeamento de Ativos de Informação está limitado ao escopo das ações de Segurança da Informação no âmbito do MCOM, e tais ações compreendem os ativos de informação considerados críticos pela Gestora de Segurança da Informação do MCOM, que deverão ter asseguradas a sua disponibilidade, integridade, confidencialidade e autenticidade.

2.6. São atribuições do Gestor de Segurança da Informação:

- a) coordenar o processo de inventário e mapeamento de ativos de informação nas unidades administrativas do Ministério;
- b) indicar o agente responsável pela gestão de ativos de informação;
- c) analisar os resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação; e
- d) propor ajustes e de medidas preventivas e proativas ao órgão.

2.7. São atribuições do agente responsável pela gestão dos ativos de informação:

- a) identificar e classificar os ativos de informação por nível de criticidade;
- b) identificar potenciais ameaças aos ativos de informação;
- c) identificar vulnerabilidades dos ativos de informação;
- d) consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;
- e) autorizar a atualização do relatório mencionado na alínea “d” do caput; e
- f) avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

2.8. São atribuições do proprietário do ativo de informação:

- a) descrever o ativo de informação.

- b) definir as exigências de segurança da informação e comunicações do ativo de informação;
- c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;
- d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo; e
- e) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação.

2.9. São atribuições do custodiante:

- a) proteger um ou mais ativos de informação, isto é, como o ativo é armazenado, transportado e processado, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação; e
- b) proteger os contêineres dos ativos de informação, e, conseqüentemente, aplicar os níveis de controles de segurança conforme as exigências de segurança da informação e comunicações, comunicadas pelo(s) proprietário(s) do(s) ativo(s) de informação.

3 PROCEDIMENTOS

3.1. O Gestor de Segurança da Informação definirá a estratégia para o Processo de Inventário e Mapeamento de Ativos para cada ciclo de execução, que incluirá:

- a) o escopo de coleta;
- b) o conjunto mínimo de informações de cada ativo e a identificação de seus responsáveis;
- c) a caracterização dos contêineres;
- d) a definição dos requisitos de segurança da informação e comunicações;
- e) os critérios para a definição do valor do ativo de informação.

3.2. O Processo de Inventário e Mapeamento de Ativos de Informação é composto pelas seguintes etapas:

- a) Etapa 1: Coleta de informações gerais dos ativos de informação;
- b) Etapa 2: Detalhamento dos ativos de informação;
- c) Etapa 3: Caracterização dos contêineres dos ativos de informação;
- d) Etapa 4: Definição dos requisitos de segurança da informação e comunicações;
- e) Etapa 5: Estabelecimento do valor do ativo de informação.

3.3. Etapa 1: Coleta de Informações Gerais dos Ativos de Informação

3.3.1. Esta etapa consiste na definição dos responsáveis pela coleta e na utilização de um conjunto essencial de informações para cada ativo de informação.

3.3.2. Poderão fazer parte do escopo do inventário os ativos de informação do MCOM relacionados a:

- a) Tecnologia da Informação (equipamentos, sistemas, aplicativos, serviços e comunicação de dados);
- b) Documentos Físicos e Digitais (ostensivos, sigilosos e classificados);
- c) Processos de Negócio e seus Viabilizadores (recursos tangíveis e intangíveis).

3.3.3. O Gestor de Segurança da Informação e Comunicações definirá o escopo do inventário para cada ciclo de execução.

3.4. Etapa 2: Detalhamento dos Ativos de Informação

3.4.1. O detalhamento do ativo deve contemplar informações que:

- a) determinem com clareza e objetividade o conteúdo do ativo de informação;



- b) identifiquem o(s) responsável(is) - proprietário(s) e custodiante(s) - de cada ativo de informação;
- c) identifiquem o valor de cada ativo de informação;
- d) identifiquem os respectivos requisitos de segurança da informação e comunicações dos ativos de informação.

3.5. Etapa 3: Caracterização dos Contêineres dos Ativos de Informação

3.5.1. O contêiner é o local onde "vive" o ativo de informação e, assim, recomenda-se que tal contêiner seja caracterizado, no mínimo, com a lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes.

3.5.2. Para completa caracterização do contêiner, devem ser definidos os limites do ambiente que deve ser examinado para o risco e devem ser descritos os relacionamentos que necessitam ser compreendidos para atendimento das exigências de segurança da informação e comunicações.

3.6. Etapa 4: Definição dos Requisitos de Segurança da Informação e Comunicações

3.6.1. Os requisitos de segurança da informação e comunicações devem ser definidos por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

3.6.2. Os critérios devem ser categorizados, no mínimo, em 5 categorias de controle:

- a) tratamento da informação;
- b) controles de acesso físico e lógico;
- c) gestão de risco de segurança da informação e comunicações;
- d) tratamento e respostas a incidentes em redes computacionais;
- e) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.

3.7. Etapa 5: Estabelecimento do Valor do Ativo de Informação

3.7.1. O(s) proprietário(s) do ativo da informação deve(m) indicar o valor do ativo, o qual deve refletir o quanto cada ativo de informação é importante para a que organização alcance seus objetivos estratégicos, e o quanto o ativo de informação é imprescindível aos interesses da sociedade e do Estado.

3.7.2. Cabe ao(s) proprietário(s) dos ativos de informação indicar o valor do ativo para o negócio do Ministério, considerando fatores do(s) risco(s) aos quais os ativos possam estar expostos, como ameaça, vulnerabilidade e impacto.



DESPACHO

Processo nº: 53115.001618/2022-80

Interessado: Mateus Matos Diniz

Assunto: Concessão - Afastamento Licença Paternidade

Ao Senhor Subsecretário de Orçamento e Administração,

Considerando a apresentação da documentação comprobatória para a concessão da Licença Paternidade e sua prorrogação ao servidor **Mateus Matos Diniz**, encaminho o presente processo para providências quanto à publicação do referido afastamento no Boletim de Serviços, conforme abaixo:

" Conceder licença paternidade ao servidor **Mateus Matos Diniz**, Matrícula SIAPE nº 1085985, nos termos a seguir:

Período	Legal	Amparo	Quantidade de dias
15/01/2022 a 19/01/2022	Art. 208, Lei nº 8.112, de 11 de Dezembro de 1990		5
20/01/2022 a 03/02/2022		Decreto nº 8.737, de 03/05/2016	15

ALESSANDRA XAVIER NUNES
Coordenadora-Geral de Gestão de Pessoas



DESPACHO

Processo nº: 53115.001622/2022-48

Interessado: Cleverson Da Silva Oliveira

Assunto: Concessão - Afastamento Licença Paternidade

Ao Senhor Subsecretário de Orçamento e Administração,

Considerando a apresentação da documentação comprobatória para a concessão de Licença Paternidade e sua prorrogação ao servidor **Cleverson Da Silva Oliveira**, encaminho o presente processo para providências quanto à publicação do referido afastamento no Boletim de Serviços, conforme abaixo:

" Conceder licença paternidade ao servidor **Cleverson Da Silva Oliveira**, Matrícula SIAPE nº 1052573, nos termos a seguir:

Período	Legal	Amparo	Quantidade de dias
14/01/2022 a 18/01/2022	Art. 208, Lei nº 8.112, de 11 de Dezembro de 1990		5
19/01/2022 a 02/02/2022		Decreto nº 8.737, de 03/05/2016	15

"

ALESSANDRA XAVIER NUNES
Coordenadora-Geral de Gestão de Pessoas



DESPACHO

Processo nº: 53115.001949/2022-10

Interessado: Larissa Aparecida de Souza e Silva

Assunto: Concessão - Afastamento Licença Maternidade

Ao Senhor Subsecretário de Orçamento e Administração,

Considerando a apresentação da documentação comprobatória para a concessão da Licença Maternidade e sua prorrogação a servidora **Larissa Aparecida de Souza e Silva**, encaminho o presente processo para providências quanto à publicação do referido afastamento no Boletim de Serviços, conforme abaixo:

" Conceder licença Maternidade ao servidor Larissa Aparecida de Souza e Silva, Matrícula SIAPE nº 1875274, nos termos a seguir:

Período	Legal	Amparo	Quantidade de dias
20/01/2022 a 19/05/2022	Art. 207, Lei nº 8.112, de 11 de Dezembro de 1990		120
20/05/2022 a 18/07/2022		Decreto nº 6.690, de 11/12/2008	60

ALESSANDRA XAVIER NUNES

Coordenadora-Geral de Gestão de Pessoas



gov.br/**mcom**

 mincomunicacoes

MINISTÉRIO DAS
COMUNICAÇÕES



PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL