Governo do Estado do Rio de Janeiro

Junta Comercial do Estado do Rio de Janeiro

PORTARIA JUCERJA/SUPINF N.º 01 DE 11 DE NOVEMBRO DE 2024

INSTITUI A POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS NO ÂMBITO DA JUNTA COMERCIAL DO ESTADO DO RIO DE JANEIRO - JUCERJA.

O SUPERINTENDENTE DE INFORMÁTICA DA JUNTA COMERCIAL DO ESTADO DO RIO DE JANEIRO – JUCERJA, no exercício das suas atribuições que lhe conferem a Portaria JUCERJA N. 2233 de 2024, e tendo em vista o disposto na Instrução Normativa PRODERJ/PRE Nº 02 de 28 de abril de 2022 e no Processo Administrativo n.º SEI-220005/002335/2024;

CONSIDERANDO:

- a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e sua regulamentação pelo Decreto nº 43.597, de 17 de maio de 2012;

- a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

- o Decreto Estadual nº 48.891/2024, de 10 de janeiro de 2024, que institui a Política de Governança em Privacidade e Proteção de Dados Pessoais no Estado do Rio de Janeiro.

- a Portaria PRODERJ/PRE Nº 825, de 26 de fevereiro de 2021, que institui a Estratégia da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – EGTIC/RJ;

- a Portaria JUCERJA nº 2041/2022, que institui a Política de Segurança da Informação e Comunicações da Junta Comercial do Estado do Rio de Janeiro;

R E S O L V E:

Art. 1º Fica instituída a Política de BACKUP e Restauração de Dados no âmbito do Junta Comercial do Estado do Rio de Janeiro.

Art. 2º Escopo:

I - Esta Política se aplica a todos os dados no âmbito da JUCERJA, incluindo dados fora da Instituição armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem Planilhas Eletrônicas, Arquivos de texto, imagens e outros dados críticos para organização, ex.: e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos e sistemas

operacionais;

II - A definição de dados críticos e o escopo desta política de backup serão revisados em intervalos não superior a três anos;

III - Ficam previamente estabelecidos os sistemas e serviços críticos da Instituição, os quais se referem a todos os sistemas computacionais, bases de dados e webservices, próprios ou contratados, por meio dos quais sejam armazenados, trafegados ou tratados dados relativos ao registro e licenciamento empresarial, e sobretudo, dados pessoais de servidores, colaboradores e usuários da JUCERJA;

IV - Esta política se aplica a servidores, colaboradores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da JUCERJA;

V - Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade integral do usuário a manutenção da guarda e sigilo dos dados em seus dispositivos;

VI - A salvaguarda dos dados em formato digital armazenados na JUCERJA, mas recebidos e/ou custodiados por outras entidades, públicas ou privadas, tais como serviços em nuvem, Termos de Cooperações etc. deve ser garantida nos instrumentos de formalização de acordos ou contratos que pactuem a relação entre os envolvidos.

Art. 3º Termos e Definições:

I - BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada;

II - CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura da JUCERJA, 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 pela Política de Segurança da Informação e Comunicações da JUCERJA ou nesta Política de Backup;

III - ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

IV - MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui nuvem, mídias eletrônicas, discos ópticos, magnéticos, CDs, fitas e papel, entre outros;

V - INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político ou à segurança;

VI - Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

VII - Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

VIII – GESTOR DA INFORMAÇÃO – indivíduo responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades institucionais.

Art. 4º Dos princípios gerais:

I - A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação da **JUCERJA**.

II - A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

III - As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

IV - As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

V - As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

VI - O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

VII - A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

VIII - Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

IX - Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Art. 5º Da frequência dos procedimentos e tempo de retenção:

I - Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar

frequência e tempo de retenção diferenciados estabelecidos a seguir:

a) Diária: 1 Mês;

b) Mensal: 12 meses;

c) Anual: 5 Anos;

II – Tipos de backup:

a) Full (Completo);

b) Incremental;

c) Diferencial;

d) Log.

III - A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pela Assessoria de Redes e Assessoria de Banco de Dados no caso de banco de dados, com a anuência prévia e formal do Gestor de Segurança da Informação, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

a) Escopo (dados digitais a serem salvaguardados);

b) Tipo de *backup* (completo, incremental, diferencial);

c) Frequência temporal de realização do backup (diária, semanal, mensal, anual);

d) Retenção;

e) RPO;

f) RTO.

IV - A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas aos responsáveis pelo Backup. A aprovação para execução da alteração depende da anuência do Gestor de Segurança da Informação, da Assessoria de Redes e da Assessoria de banco de Dados.

V - Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

VI - Os backups dos serviços de TI críticos da JUCERJA deverão ser realizados utilizando-se as seguintes frequências temporais:

a) Banco de dados de Produção:

- Full 1 x na semana

- Diferencial 4 x ao dia em 6 em 6h

- Log:

- de 0h às 6h a cada 1h

- de 6h30 às 8h59 a cada 10 minutos
- de 9h às 17h59 a cada 3 minutos
- de 18h30 às 23h58 a cada 30 minutos

b) Servidores
- Job Produção Windows
- Full 1x por semana
- Incremental todos os dias ás 18:30

- Job Produção Linux
- Full 1x por semana
- Incremental todos os dias ás 18:30

- Job DC
- Full 1x por semana
- Incremental todos os dias ás 18:30

- Job Exchange
- Full 1x por semana
- Incremental todos os dias ás 18:30

- Job Homologção (Storage secundario)
- Full 1x por semana
- Incremental todos os dias ás 20:00

- Job produção (Storage secundario)
- Full 1x por semana
- Incremental todos os dias ás 20:00

- Job Produção (nuvem)
- Full 1x por semana
- Incremental todos os dias ás 18:30

c) Arquivos de usuários

- Job File Server
- Full 1x por semana
- Incremental todos os dias ás 18:30

VII - Os serviços de TI críticos da JUCERJA devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

- Job Produção Windows - 30 dias
- Job Produção Windows – Mensal com retenção de 12 meses
- Job Produção Windows – Anual com retenção de 5 anos

- Job Produção Linux - 30 dias
- Job Produção Linux - Mensal com retenção de 12 meses
- Job Produção Linux - Anual com retenção de 5 anos

- Job Produção DC - 30 dias
- Job Produção DC - Mensal com retenção de 12 meses
- Job Produção DC - Anual com retenção de 5 anos

- Job Produção Exchange - 30 dias
- Job Produção Exchange - Mensal com retenção de 12 meses
- Job Produção Exchange - Anual com retenção de 5 anos

- Job Homologação (Storage secundário) – 14 dias
- Job Produção – (Storage secundário) – 14 dias

- Job Produção (Nuvem) – 30 dias

- Job File Server – 30 dias
- Job File Server – Mensal com retenção de 12 meses
- Job File Server – Anual com retenção de 5 anos

VIII – Mensalmente, a Assessoria de banco de Dados deverá emitir relatório detalhado, por meio do qual seja possível identificar as pastas de rede e bases de dados contempladas no processo de cópia de segurança, a conformidade e, quando existir, desconformidade dos serviços de backup, assim como, as capacidades utilizadas e disponíveis para armazenamento de dados e cópias de segurança, tanto na infraestrutura interna da Instituição, como em eventuais recursos em nuvem contratados à terceiros;

IX - Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:

a) Backup incremental diário (segunda a domingo), Storage / Nuvem;

b) Backup completo semanal (segunda a domingo), armazenado externamente. Sempre que possível, os backups devem ser iniciados às 18:30 h da noite de sexta para permitir mais tempo durante o fim de semana para realizar o backup e tempo suficiente para lidar com quaisquer problemas que possam surgir

durante o processo de backup.

Art. 6º Uso da rede:

I - O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da JUCERJA, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da Instituição;

II - A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup;

III – O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a Assessoria de Redes, área técnica responsável pela administração da rede de dados da JUCERJA.

Art. 7º Do armazenamento e transporte

I - As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

a) A criticidade do dado salvaguardado;

b) O tempo de retenção do dado;

c) A probabilidade de necessidade de restauração;

d) O tempo esperado para restauração;

e) O custo de aquisição da unidade de armazenamento de backup;

f) A vida útil da unidade de armazenamento de backup.

II - O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo, quando couber, a melhor solução para cada caso.

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

IV - A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

V - No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo 5 anos. Após esse período os arquivos poderão ser excluídos a qualquer tempo.

VI - As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas, conforme estabelecido na Política de Segurança da Informação e Comunicações da JUCERJA. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

VII - 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.

Art. 8º Dos testes de backup:

I - Os backups deverão ser verificados periodicamente:

a) Diariamente, os diferenciais e logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.

b) Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.

c) A ASSBD manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.

d) Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

II - Os testes de restauração dos backups devem ser realizados, por amostragem, semanalmente, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos, assim como, se foram atendidos

os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.

III - Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso

IV - Quaisquer exceções a esta política deverão ser totalmente documentadas e aprovadas pelo Gestor de Segurança da Informação - GSIC.

Art. 9º Do procedimento de restauração do backup:

I – O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

a) A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, na ferramenta disponibilizada pelo link http://helpdesk.intranet.jucerja.rj.gov.br/;

b) A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup;

c) A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações;

d) O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

II - O tempo de restauração, preferencialmente, será definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC, e será estimada com base no volume de dados necessários para o restore;

III - Backups externos serão disponibilizados em conformidade com a disponibilidade dos ambientes e equipes técnicas envolvidas no processo, conforme Acordos de Níveis de Serviços pactuado, observando a prioridade para restauração de acordo com a criticidade de cada um;

Art. 10 Do descarte de mídias:

I – A qualquer tempo, se necessário realizar descarte de mídias que contenham backups, decorridos os prazos de retenção, a Assessoria de Redes poderá realizar o descarte das mídias, desde que autorizado pelo Gestor de Segurança da Informação;

II – A Assessoria de Redes e a Assessoria de Banco de Dados garantirão o respeito aos prazos de descarte, assim como, a indisponibilidade dos conteúdos das mídias;

III – A Assessoria de Redes garantirá a destruição física das mídias em processo de descarte.

Art. 11 Das responsabilidades:

I – Todos os procedimentos de backup, teste e restore são de responsabilidade da Assessoria de Banco de Dados, assim como:

a) Providenciar a criação e manutenção dos backups;

b) Propor soluções de cópias de segurança das informações digitais corporativas produzidas e custodiadas;

c) Configurar as soluções de backup, teste e restore;

d) Manter a funcionalidade, segurança, integridade, disponibilidade e inviolabilidade dos backups;

e) Definir procedimentos adicionais.

II – A Assessoria de Banco de dados, para realização de suas atribuições relativas aos procedimentos de backup, teste e restore. Poderá se valer do apoio de outras unidades técnicas da Superintendência de

Informática;

III - Cabe a Assessoria de Banco de dados informar ao Gestor de Segurança da Informação qualquer desconformidade técnica e/ou operacional que comprometa a garantia dos procedimentos de backup, teste e restore;

IV – Cabe a Assessoria de Banco de Dados, apoiada pela Assessoria de Redes, monitorar e providenciar, quando necessário, recursos de hardware, software, licenciamentos e outros necessários a manutenção e regularidade dos procedimentos de backup, testes e restore.

Art. 12 Das sanções:

I – As sanções pelo descumprimento ou inobservância desta política podem incluir, mas não se limitam a um ou mais das seguintes:

a) Processo administrativo de apuração de responsabilidades;

b) Quando comprovada imperícia ou desídia, por parte de equipe ou empresa contratada, sem prejuízo das sanções previstas em contrato, além da responsabilização civil e criminal, até a rescisão unilateral do contrato;

Art. 13 Esta Portaria entra em vigor na data de sua publicação

Rio de Janeiro, 11 de novembro de 2024.

ALDO FERNANDES ÁVILA

Superintendente de Informática

Documento assinado eletronicamente por **Aldo Fernandes Ávila**, **Superintendente**, em 11/11/2024, às 12:41, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **87194345** e o código CRC **678B6574**.