GOVERNO DO ESTADO
RIO DE JANEIRO

ANEXO ÚNICO

Instrução Normativa PRODERJ/PRE Nº 02/2022

PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO EM SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC A SEREM OBSERVADOS PELOS ÓRGÃOS E ENTIDADES INTEGRANTES DA ADMINISTRAÇÃO DIRETA E INDIRETA DO PODER EXECUTIVO DO ESTADO DO RIO DE JANEIRO.

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ

Presidente
JOSÉ MAURO DE FARIAS JUNIOR

Vice-Presidente de Administração
DIEGO HENRIQUE FERREIRA DOS SANTOS

Vice-Presidente de Tecnologia
FLÁVIO SEBASTIÃO RODRIGUES DA SILVA

Vice-Presidente de Governo Digital
PEDRO MACHADO PEREIRA JUNIOR

Vice-Presidente de Estratégia, Governança e Inovação.
BRUNO PEREIRA CUNHA

PRODERJ

Elaboração deste Documento

Diretor de Segurança da Informação
MARCELO SOARES LINTOMEN

Sumário

PREÂMBULO....7
Controle de Documento....7
Controle de Versões....7
Classificação: PÚBLICO....7
Normas e documentos complementares....8
Normas e documentos de referência....8
1. APRESENTAÇÃO....9
2. OBJETIVO....10
3. ABRANGÊNCIA E DIVULGAÇÃO....10
4. CONCEITUAÇÃO E DEFINIÇÕES....10
5. ESTRUTURA NORMATIVA....14
6. APROVAÇÃO....14
7. RESPONSABILIDADES....14
7.1. Introdução....14
7.2. Área de Infraestrutura....14
7.3. Área Desenvolvimento de Sistemas....15
7.4. Área de Recursos Humanos....15
7.5. Controlador....15
7.7. Usuários em geral....16
8. DIRETRIZES....17
8.1. Gestão de ativos....17
8.1.2. Classificação da Informação quanto ao acesso....17
8.1.3. *Backup* e recuperação de dados....19
8.2. Segurança em recursos humanos....19
8.2.1. Antes da contratação....19
8.2.2. Durante a contratação....19
8.2.3. Encerramento e mudança na contratação....20
8.3. Controle de acesso lógico....20
8.3.3. Acesso à rede, ao sistema operacional e às aplicações....20
8.3.4. Utilização de senhas....21
8.3.5. Uso de dispositivos móveis....22
8.3.6. Trabalho Remoto....22

8.3.7. Procedimentos de *logging*....22
8.4. Criptografia....23
8.5. Anonimização e Pseudonimização....23
8.6. Segurança física e do ambiente....23
8.6.1. Entrada e saída de pessoas....23
8.6.2. Entrada e saída de equipamentos de TIC....24
8.6.3. Proteção predial e infraestrutura....24
8.7. Comunicação segura....24
8.7.1. Segurança dos serviços de rede....24
8.7.2. Transferência de informações....25
8.8. Aquisição, desenvolvimento e manutenção de sistema de informação....25
8.8.1. Requisitos de segurança em sistemas de informação....25
8.8.2. Processamento correto nas aplicações....26
8.8.3. Segurança no processo de desenvolvimento e suporte....26
8.8.4. Gestão de vulnerabilidades técnicas....26
8.8.5. Testes....26
8.9. Relacionamento com o fornecedor....27
8.9.1. Termo de Responsabilidade e Confidencialidade para Fornecedores....27
8.9.2. Cláusulas de segurança na contratação....27
8.9.3. Computação em Nuvem (*Cloud computing*)....27
8.10. Gestão de Mudança....27
8.11. Gestão de incidentes de segurança da informação....27
8.12. Desvio de Segurança da Informação....28
8.13. Orientações ao colaborador em geral....28
8.13.1. Uso aceitável dos ativos....28
8.13.2. Cuidados cotidianos....28
8.13.3. Transferência de informações....28
8.13.4. Acesso à Internet, redes sociais e comunicadores instantâneos....29
8.13.5. Conscientização de Segurança da Informação....29
8.13.6. Acesso ao correio e a ferramentas de colaboração....29
8.13.7. Proteção contra códigos maliciosos....30
8.14. Gestão de riscos e Continuidade de Operações....30
8.14.1. Análise, avaliação e tratamento de riscos....30

8.14.2. Gestão de continuidade de operações....30
8.15. Monitoramento e auditoria....30
8.16. Gestão de Indicadores de Segurança....31
9. PENALIDADES E PROCESSO DISCIPLINAR....31
10. ATUALIZAÇÃO....31
11. REFERÊNCIAS LEGAIS E NORMATIVAS (CONFORMIDADE)....32
Anexo I: critérios de restrição à informação reservada....32
Anexo II: modelo de Termo de Confidencialidade e Sigilo....34

PREÂMBULO

Controle de Documento

Controle de Versões

Versão	Alteração	Data	Alterado por
0.9	Primeira versão para aprovação	30/11/2020	Marcelo Soares Lintomen
1.0	Segunda versão para aprovação	15/07/2021	Manuelito de Sousa Reis Júnior
1.1	Nova versão, alinhada com a norma setorial de segurança da informação.	19/11/2021	Bruno Pereira Cunha Manuelito de Sousa Reis Júnior Marcelo Soares Lintomen

Obs. Cópias Impressas deste documento podem não corresponder à última versão aprovada e em uso. A versão mais atualizada pode ser encontrada no Portal do Sistema Estadual de Tecnologia de Informação e Comunicação (SETIC) do Governo do Estado do Rio de Janeiro: http://www.setic.rj.gov.br/?q=content/legisla%C3%A7%C3%A3o-1

Classificação: PÚBLICO
Documento com acesso público de disponibilização imediata, na forma do art. 50, do Decreto nº 46.730/2019.

Normas e documentos complementares

- Lei nº 12.527/2011 - Lei de Acesso à Informação - LAI;
- Lei nº 12.965/2014 - Marco Civil da Internet;
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD;
- Decreto nº 46.475/2018 – regulamenta o acesso às informações previstas na Constituição Federal;
- Decreto nº 46.730/2019 – dispõe sobre a produção e tramitação eletrônica de documentos e processos administrativos na Administração Pública Estadual, e dá outras providências;
- Decreto nº 47.278/2020, art. 5º - atribui ao PRODERJ a competência para a Direção Geral do Sistema Estadual de Tecnologia da Informação e Comunicação – SETIC;
- Portaria PRODERJ/PRE nº 825/2021 - institui a Política da Governança, a estratégia da governança e as normas do Plano Estratégico e Diretor de Tecnologia da Informação e Comunicação – PEDTIC, no âmbito do Poder Executivo da Administração Pública Estadual Direta e Indireta do Estado do Rio de Janeiro e dá outras providências;
- Instrução Normativa PRODERJ/PRE nº 01/2021 - regulamenta os procedimentos para a contratação e celebração de acordos envolvendo soluções de Tecnologia da informação e Comunicação – TIC a serem observados pelos órgãos e entidades integrantes da Administração Direta e Indireta do Poder Executivo do Estado do Rio de Janeiro;
- ABNT NBR ISO/IEC 27001:2013 - especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização;
- ABNT NBR ISO/IEC 27002:2013 – fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;

Normas e documentos de referência

- Decreto nº 10.332/2020 - Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;
- Instrução Normativa nº 1/2020, do Gabinete de Segurança Institucional da Presidência da República - que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- Instrução Normativa nº 14/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República - estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem;

- Resolução nº 20/2018, do Ministério da Integração Nacional, que aprova a Política de Segurança da Informação e das Comunicações - POSIC e seus anexos I e II - dispõe sobre o manuseio, tratamento, controle e a proteção dos dados, informações e conhecimentos produzidos na Superintendência de Desenvolvimento da Amazônia – SUDAM.

1. APRESENTAÇÃO

1.1. A informação constitui um ativo valioso e de extrema importância e necessita ser convenientemente protegida, independentemente de sua natureza ou de sua origem.

1.2. A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, nuvem e até mesmo por meio da comunicação oral.

1.3. Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada. A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos ao Governo do Estado do Rio de Janeiro.

1.4. É diretriz que toda informação de propriedade do Governo do Estado do Rio de Janeiro seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade, autenticidade ou disponibilidade destas.

1.5. A Segurança da Informação consiste na adoção de medidas para proteção da informação com a finalidade de atingir os seguintes objetivos:

1.5.1. **Disponibilidade**: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las;

1.5.2. **Integridade**: garantir que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais;

1.5.3. **Confidencialidade**: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas; e

1.5.4. **Autenticidade**: confirmar a identidade de quem se diz ser.

1.6. As diretrizes de segurança da informação em soluções de TIC ora instaurados no âmbito da Administração Pública Estadual correspondem a uma declaração formal acerca do compromisso com a proteção, o controle e o monitoramento das informações processadas, armazenadas, transmitidas ou custodiadas pelo Governo do Estado do Rio de Janeiro, que sejam de sua propriedade ou estejam sob a sua guarda.

1.7. Este documento apresenta as diretrizes que deverão orientar toda a Administração, seus órgãos, repartições e funcionalismo, nas ações para iniciar, implementar, manter e melhorar a gestão da Segurança da Informação, de maneira a promover a criação de alicerces para a proteção desse ativo.

1.8. As diretrizes aqui apresentadas estão baseadas nas recomendações das publicações da família de normas NBR ISO/IEC 27000.

2. OBJETIVO

2.1. O objetivo é definir as diretrizes e documentos complementares que viabilizem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações críticas e continuidade digital do Governo do Estado do Rio de Janeiro.

3. ABRANGÊNCIA E DIVULGAÇÃO

3.1. Os procedimentos apontados neste instrumento deverão ser cumpridos por todos os colaboradores, incluindo servidores, consultores, dirigentes, empregados, estagiários, prestadores de serviços e visitantes de toda Administração Direta e Indireta do Poder Executivo do Estado do Rio de Janeiro.

3.2. Os documentos que integram a estrutura normativa da Segurança da Informação aqui apontados, deverão estar disponíveis no Portal do SETIC: http://www.setic.rj.gov.br/?q=content/legisla%C3%A7%C3%A3o-1

3.3. Este documento, em sua estrutura textual, poderá servir de base e modelo para os órgãos, autarquias e empresas do Governo do Estado do Rio de Janeiro elaborarem os seus próprios procedimentos de segurança da informação.

4. CONCEITUAÇÃO E DEFINIÇÕES

4.1. **Alta Administração** – é o quadro diretivo do órgão, com legitimidade para representá-lo. Por exemplo: diretores, vice-presidentes, presidentes, reitores, secretários, dentre outros;

4.2. **Análise de risco** – processo pelo qual são relacionados os eventos, os impactos e avaliadas as probabilidades destes eventos tornarem-se reais;

4.3. **Ativo** – qualquer bem, tangível ou intangível, que tenha valor para a organização;

4.4. **Ativos de Tecnologia da Informação e Comunicação** – estações de trabalho, servidores, *softwares*, mídias e quaisquer equipamentos eletrônicos relacionados à tecnologia da informação e comunicação, bem como processos, pessoas e ambientes;

4.5. **Autenticidade** – propriedade pela qual se assegura a fidedignidade da fonte da informação através de processos de autenticação, é possível confirmar a identidade de quem presta a informação;

4.6. ***Backup*** – cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados existentes;

4.7. **Certificação digital** – tecnologia para criptografia de dados para fins de segurança no trânsito virtual;

4.8. **Colaborador** – funcionário ou qualquer pessoa que preste serviços ao Governo do Estado do Rio de Janeiro, seja através de contrato individual de trabalho ou por vínculo a um contrato de prestação de serviço ou nomeação;

4.9. **Computação em nuvem *(Cloud Computing)*** – modelo de negócio que disponibiliza (compartilha) recursos computacionais e serviços sob demanda, configuráveis pelo próprio cliente, de acordo com a sua necessidade, e cobrados apenas pelo que foi consumido. A computação na nuvem oferece escalabilidade e mecanismos de gestão dos serviços;

4.10. **Confidencialidade** – propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

4.11. **Conformidade** – aderência a um padrão previamente estabelecido e aceito como ideal;

4.12. **Controlador** – agente de tratamento, que pode ser uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, sendo responsável por assegurar o registro das operações de tratamento realizadas, observar o cumprimento das instruções fornecidas e das normas sobre a matéria;

4.13. **Controle de acesso** – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra requer procedimentos de autenticação;

4.14. **Controles de segurança** – medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de hash, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão, backups, entre outros;

4.15. **Criticidade** – nível de crise ou impacto que pode advir da divulgação ou uso indevido da informação;

4.16. **Dado Anonimizado** – dado pessoal que passou por técnica de desassociação das informações que inviabiliza de maneira irreversível a identificação direta do titular de um dado pessoal;

4.17. **Dado organizacional** – qualquer dado, próprio ou de terceiros, de interesse organizacional ou sob a guarda da Administração;

4.18. **Dado Pseudoanonimizado** – dado pessoal que passou por tratamento por meio do qual perdeu a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro e, portanto, poderá posteriormente ter restabelecida a associação ao seu titular;

4.19. **Dado Pessoal** - informação relacionada à pessoa natural identificada (diretamente) ou identificável (indiretamente);

4.20. **Dado Pessoal Sensível** – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

4.21. **Defesa cibernética** – ações realizadas no espaço cibernético para fins de proteção dos ativos de informação de interesse da Administração, bem como para a obtenção de dados para a produção de conhecimentos de inteligência;

4.22. **Desvio de Segurança da Informação** – é um resultado não previsto ou indesejado em um procedimento. É um desvio no procedimento adequado de segurança da informação;

4.23. **Disponibilidade** – diz respeito à garantia de que a informação estará acessível às pessoas, processos automatizados, órgãos ou entidades quando for requerida.

Logo, a disponibilidade está relacionada à prestação continuada de um serviço, sem interrupções no fornecimento de informações;

4.24. **Dispositivos móveis** – qualquer equipamento ou acessório portátil, capaz de se conectar à internet e ou armazenar dados, tais como: *smartphone*, *tablet*, *notebook*, *netbook*, PDA (palmtops), *pendrive*, CD/DVD, HD externo e assemelhados;

4.25. **Espaço cibernético** – espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações humanas ou automatizadas, conduzidas através desse ambiente;

4.26. **Gestão da conformidade** – conjunto de medidas que asseguram que uma entidade está em conformidade com as normas vigentes, ou seja, se está cumprindo todas as obrigatoriedades dos órgãos de regulamentação, dentro de todas as políticas exigidas para a execução de sua atividade;

4.27. **Gestor de Segurança da Informação** – servidor designado para a coordenação e gerenciamento das ações voltadas à segurança da informação no âmbito dos órgãos e entidades estaduais, com as competências previstas no art. 23 do instrumento normativo do qual este documento é anexo único;

4.28. **Incidente de Segurança da Informação -** qualquer evento adverso, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação;

4.29. **Integridade** – é fidedignidade da informação, que deve ser assegurada como garantia de que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional;

4.30. **Não repúdio –** propriedade de assegurar que, em um processo de envio e recebimento de informações, nenhum participante originador, nem destinatário de informação possa, em um momento posterior, negar a respectiva atuação;

4.31. **Normas Complementares** – possuem função de complementar e detalhar os procedimentos e instruções de segurança descritos neste documento. As normas complementaras são subordinadas a este e à legislação vigente;

4.32. **Operador** - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de informações em nome do controlador, Agente de tratamento, que pode ser uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de informações em nome do controlador, devendo manter o registro das operações de tratamento realizadas, bem como cumprir as instruções e normas acerca da matéria nos moldes delineados pelo controlador;

4.33. **Perímetro** – delimitação da área física ou lógica onde são aplicadas proteções contra acessos indevidos;

4.34. **Procedimentos Operacionais** – ações padronizadas a serem implementadas no âmbito dos órgãos, baseadas nas instruções deste documento e do instrumento normativo do qual é anexo único, para fins de implementação de um sistema de controle e de segurança da informação e da comunicação;

4.35. **Recursos de tecnologia da informação e comunicação** – diferentes formas de união entre hardware e software no oferecimento de aplicações ou serviços que interferem ou mediam os processos informacionais e comunicativos, ou seja, são conjuntos de bens e/ou serviços que apoiam processos de negócios, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

4.36. **Risco** – resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento e o impacto resultante;

4.37. **Segurança cibernética** - conjunto de práticas para a proteção de informação armazenada nos computadores e aparelhos de computação, transmitida através das redes de comunicação, incluindo a Internet e telefonia móvel;

4.38. **Segurança da Informação** – proteção da Informação de vários tipos de ameaças para garantir a continuidade dos processos computacionais, minimizando os riscos e maximizando a disponibilidade, integridade e confidencialidade;

4.39. **Segurança física** – adoção de medidas por meio de pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubos, sabotagens e outros prejuízos causados por ações humanas não autorizadas;

4.40. **SEI-RJ** – (Sistema Eletrônico de Informação) Sistema oficial de autuação, produção, tramitação e consulta de documentos e processos administrativos eletrônicos no âmbito dos órgãos e das entidades da administração pública estadual e fundacional do Estado do Rio de Janeiro, instituído pelo Decreto nº 46.730/2019;

4.41. **Sensibilidade** – grau de sigilo necessário à informação;

4.42. **Tratamento de dados pessoais** – toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

4.43. **Vulnerabilidade** – uma fraqueza em um ativo, ou grupo de ativos, de informação que pode ser explorada por uma ameaça. Exemplos: data center ao lado de um rio, portas destrancadas, atribuição errada de direitos de senha, falta de manutenção etc.

5. ESTRUTURA NORMATIVA

5.1. A estrutura normativa da Segurança da Informação será composta por este documento e pelas disposições da instrução normativa do qual é anexo único, pelas normas complementares referidas no art. 22 da mesma instrução normativa, bem como pelas normas e documentos técnicos listados após o preâmbulo deste documento.

6. APROVAÇÃO

6.1. Os procedimentos aqui estabelecidos serão publicados nos meios de comunicação oficiais pelo Presidente do Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ, reafirmando o compromisso do Estado do Rio de Janeiro com a Segurança da Informação.

7. RESPONSABILIDADES

7.1. Introdução

7.1.1. É responsabilidade de cada colaborador, independentemente de cargo ou função, observar e cumprir o estabelecido neste documento.

7.1.2. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades quotidianas contando, sempre que necessário, com a orientação do Gestor de Segurança da Informação do seu órgão ou entidade.

7.1.2.1. As responsabilidades aqui definidas visam abranger as estruturas organizacionais do maior número possível de órgãos/entidades do Estado do Rio de Janeiro, assim sendo, nem todos possuirão todas as áreas definidas a seguir ou podem utilizar outras nomenclaturas para designá-las.

7.2. Área de Infraestrutura

7.2.1. É responsabilidade da área de Infraestrutura:

7.2.1.1. Operar a plataforma para prevenção, detecção e reação a incidentes de segurança;

7.2.1.2. Tratar incidentes lógicos de Segurança da Informação;

7.2.1.3. Reportar a ocorrência de incidentes de Segurança da Informação ao Gestor da Segurança da Informação;

7.2.1.4. Corrigir as vulnerabilidades nos ativos tecnológicos;

7.2.1.5. Manter atualizado proativamente, com as últimas correções de segurança, todo o parque de ativos sob sua responsabilidade;

7.2.1.6. Monitorar os serviços de proteção e gerar relatórios periódicos dos equipamentos de Segurança da Informação;

7.2.1.7. Implementar e monitorar mecanismos de proteção do perímetro;

7.2.1.8. Implementar mecanismos de proteção (segurança lógica) nas plataformas tecnológicas (bancos de dados, sistemas operacionais, redes, armazenamento, nuvem, etc.) sob a sua responsabilidade;

7.2.1.9. Seguir estritamente a norma de Gestão de Mudança, sempre que houver uma manutenção no ambiente que possa impactar a disponibilidade de ativos;

7.2.1.10. Cumprir e garantir o cumprimento de seus colaboradores a este instrumento e suas normas complementares.

7.3. Área Desenvolvimento de Sistemas

7.3.1. É responsabilidade da área de desenvolvimento:

7.3.1.1. Garantir a implantação de segurança no processo e no código dos sistemas desenvolvidos;

7.3.1.2. Garantir a atualização dos códigos desenvolvidos bem como seus frameworks, visando a remoção de vulnerabilidades que venham a ser descobertas;

7.3.1.3. Garantir a devida segregação dos ambientes de desenvolvimento, homologação e produção;

7.3.1.4. Controlar de forma segura as credenciais de acesso sob sua custódia;

7.3.1.5. Seguir os processos de gestão de mudança para qualquer alteração que necessite ser realizada em produção;

7.3.1.6. Apoiar e contribuir, em sua área de atuação, para a melhoria das ações de Segurança da Informação;

7.3.1.7. Informar aos responsáveis pelo gerenciamento das credenciais sobre a criação e necessidade de alteração nos acessos dos colaboradores;

7.3.1.8. Reportar não conformidades ao Gestor da Segurança da Informação.

7.4. Área de Recursos Humanos

7.4.1. É responsabilidade da Área de Recursos Humanos:

7.4.1.1. Informar aos responsáveis pelo gerenciamento das credenciais sobre as mudanças nos acessos dos colaboradores;

7.4.1.2. Dar conhecimento formal aos novos colaboradores acerca deste documento, bem como suas normas complementares;

7.4.1.3. Reportar a ocorrência de incidentes e não conformidades de segurança ao Gestor da Segurança da Informação;

7.4.1.4. Informar ao Gestor da Segurança da Informação quando da necessidade de excluir acessos dos colaboradores;

7.4.1.5. Cumprir este instrumento e suas normas complementares.

7.5. Controlador

7.5.1. Dentro do escopo deste documento, é o controlador das informações sobre as quais tem plena autonomia de decisão quanto ao respectivo tratamento, sendo o responsável por sua guarda e integridade.

7.5.2. O Controlador da Informação terá a autoridade e a responsabilidade de:

7.5.2.1. Definir a espécie de tratamento de dados a ser realizado pelo operador, a base legal correspondente e a finalidade da operação envolvida na relação jurídica;

7.5.2.2. Definir as necessidades de proteção dos ativos de informação, incluindo como deverá ser realizado o tratamento dos dados pessoais, caso se aplique;

7.5.2.3. Determinar o nível de relevância e classificação correta das informações utilizadas nos ativos sob sua responsabilidade, de forma a subsidiar as decisões de classificação a serem aplicadas;

7.5.2.4. Definir uma estratégia de segurança da informação e proteção de dados pessoais do serviço;

7.5.2.5. Definir o escopo e a periodicidade do *backup* e de teste de recuperação de dados;

7.5.2.6. Autorizar as mudanças que sejam realizadas em produção;

7.5.2.7. Gerir a informação sob sua responsabilidade respeitando sempre as melhores práticas gerenciais, o interesse público, bem como este instrumento e suas normas complementares;

7.5.2.8. Cumprir este instrumento e suas normas complementares.

7.6. Operador

7.6.1. Dentro do escopo deste documento é o responsável pelo tratamento e custódia das informações sob sua guarda e terá a responsabilidade de:

7.6.1.1. Administrar os controles definidos pelo respectivo controlador da informação;

7.6.1.2. Administrar o acesso aos ativos de informação;

7.6.1.3. Providenciar a proteção física dos ativos de informação;

7.6.1.4. Simular e executar os planos de continuidade;

7.6.1.5. Realizar o tratamento dos dados pessoais de acordo com as instruções e finalidades descritas pelo controlador e em conformidade com a LGPD;

7.6.1.6. Resolver as não conformidades de Segurança da Informação;

7.6.1.7. Informar ao Gestor de Segurança da Informação quando da necessidade de excluir acessos dos colaboradores;

7.6.1.8. Cumprir este instrumento e suas normas complementares.

7.7. Usuários em geral

7.7.1. Reportar a ocorrência de incidentes de Segurança da Informação e não conformidades ao Gestor da Segurança da Informação do órgão ou entidade;

7.7.2. Apoiar e sugerir, em sua área de atuação, as ações de Segurança da Informação;

7.7.3. Cumprir as prescrições dispostas neste documento, bem como as suas normas complementares.

8. DIRETRIZES

8.1. Gestão de ativos

8.1.1. Os ativos disponibilizados deverão estar aderentes às melhores práticas de segurança da informação, devendo passar por procedimentos padronizados de configurações e adequações às melhores práticas de segurança (*hardening*) visando mitigar riscos e tornar o ativo mais resiliente no enfrentamento a tentativas de ataque. Uma norma complementar será elaborada para a gestão de ativos.

8.1.2. Classificação da Informação quanto ao acesso

8.1.2.1. Toda informação armazenada ou mantida deverá ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade, tendo por parâmetros o Decreto nº 46.730/2019, o Decreto nº 46.475/2018 e a Lei nº 13.709/2018, nas categorias: PÚBLICA, RESERVADA, SECRETA, ULTRASSECRETA ou PESSOAL. Os gestores da Informação devem assegurar que as classificações sejam revisadas periodicamente.

8.1.2.2. Não poderão ser incluídos no SEI-RJ documentos que possuam informações classificáveis nos níveis de sigilo estabelecidos nos arts. 23 e 24 da Lei Federal nº 12.527/2011 e no art. 26 do Decreto Estadual nº 46.475/2018, a saber: ultrassecreto, secreto e reservado.

8.1.2.3. A informação será **PÚBLICA** quando não estiver classificada em grau RESERVADO, SECRETO, ULTRASSECRETO ou PESSOAL.

8.1.2.3.1. O acesso à informação PÚBLICA é livre, não havendo restrição a sua divulgação, resguardadas as informações de divulgação obrigatória constantes dos arts. 8º e 9º do Decreto nº 46.475/2018.

8.1.2.4. A informação será **RESERVADA** quando enquadrada nos eventos com suas respectivas fundamentações legais, listados no anexo II deste documento (i.e., procedimentos operacionais, documentos em fase de preparação, memorandos internos) e que não esteja classificada como SECRETA, ULTRASSECRETA ou PESSOAL. Será RESERVADA também a informação que se enquadre nos §§ 2º ao 6º, do art. 29 do Decreto nº 46.475/2018.

8.1.2.4.1. Tem competência para a atribuição do grau RESERVADO, qualquer servidor que exerça cargo de comando, direção ou chefia, na forma do inciso III do art. 30 do Decreto nº 46.475/2018.

8.1.2.4.2. A restrição de caráter RESERVADO terá duração máxima de 5 anos, na forma do inciso III do art. 29 do Decreto nº 46.475/2018, podendo ser anualmente reavaliada a sua condição.

8.1.2.5. A Informação será **SECRETA**, observado o Decreto nº 46.475/2018, conforme o entendimento e critérios das autoridades exclusivamente competentes para esta classificação, Governador, Vice Governador, Secretários e titulares de autarquias, fundações, empresas públicas e

sociedades de economia mista, ou por quem estes venham a delegar tal competência, vedada a subdelegação, sendo observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados: a gravidade do risco ou dano à segurança da sociedade e do Estado; o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.

8.1.2.5.1. A manipulação de documentos classificados como SECRETOS devem observar as orientações referentes a não exposição pública, tal como permanecer sobre mesas e locais de acesso público, impressoras, copiadoras, entre outros, garantindo a confidencialidade dos mesmos.

8.1.2.5.2. Documentos SECRETOS não devem ser expostos à visualização ou acesso público de nenhuma forma.

8.1.2.6. A informação será **ULTRASSECRETA**, observado o Decreto nº 46.475/2018, conforme o entendimento e critérios das autoridades exclusivamente competentes para esta classificação, Governador, Vice Governador e Secretários, ou por quem estes venham a delegar tal competência, vedada a subdelegação, sendo observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados: a gravidade do risco ou dano à segurança da sociedade e do Estado; o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.

8.1.2.6.1. Só devem ter acesso a informações ULTRASSECRETAS pessoas devidamente autorizadas pela respectiva autoridade que assim classificou a informação, independentemente do cargo ocupado.

8.1.2.7. O pedido de acesso à informação de caráter RESERVADO, SECRETO ou ULTRASSECRETO se dará nos termos dos arts. 12 ao 20, ou do §7º do art. 29, todos do Decreto nº 46.475/2018, resguardada a possibilidade recurso em caso de negativa de autorização de acesso, na forma dos arts. 21 ao 25.

8.1.2.8. A informação deverá ser classificada como **PESSOAL** quando abranger os aspectos relacionados a qualquer indivíduo, enquanto pessoa natural, considerando-se os aspectos dos incisos I e II, do art. 5º, da Lei nº 13.709/2018.

8.1.2.8.1. As informações de natureza PESSOAL, por exigência da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), devem ser resguardadas com máxima atenção e efetividade, sob pena de incidência das penalidades previstas na referida lei, para hipóteses de incidentes, vazamentos, ocasionados por omissão ou ausência de adoção dos protocolos preventivos e eventos danosos.

8.1.2.9. Será instituída uma norma complementar, sobre classificação da informação, para fins de regulação sobre a guarda, a disponibilização, a circulação e o descarte das informações. Até lá, tais procedimentos devem resguardar as boas práticas de governança e os princípios

inerentes ao quanto disposto neste documento e no instrumento normativo do qual é anexo, bem como, nas suas normas complementares.

8.1.2.10. A classificação da informação disposta neste item poderá ser revista a qualquer tempo para fins de atendimento de novos normativos ou para melhor aproveitar as disposições já instituídas em instrumentos normativos diversos. A nova classificação será imediatamente disponibilizada no portal online do SETIC.

8.1.3. *Backup* e recuperação de dados

8.1.3.1. Os ativos devem possuir *backup* com escopo e periodicidade definida pelo Controlador;

8.1.3.2. O Controlador da Informação deverá também definir procedimentos de teste de restauração;

8.1.3.3. As cópias de segurança (*backup*) devem ser armazenadas em local seguro, em rede exclusiva e isolada dos demais ativos, com acesso restrito e controlado por Firewall;

8.1.3.4. Os acessos à rede de *backup* devem ocorrer apenas durante a duração do *backup*;

8.1.3.5. Todos os acessos a essa rede deverão ser devidamente registrados;

8.1.3.6. Sistemas ou serviços que possuam atualização constante deverão ter uma estratégia de *backup* mais agressiva a ser definida pelo Controlador da Informação;

8.1.3.7. A critério do Controlador, poderá ser especificada necessidade de guarda *offline* dos *backups*;

8.1.3.8. Os procedimentos para *backup* deverão prever o local e a forma de armazenamento, o tempo de retenção, mecanismos de teste de recuperação dos dados, transporte e meios para o descarte seguro das mídias do *backup*;

8.1.3.9. Deverá ser realizado com periodicidade anual um teste de recuperação de desastres, simulando a recuperação dos dados dos principais ativos do data center, através de um Plano de Continuidade.

8.2. Segurança em recursos humanos

8.2.1. Antes da contratação

8.2.1.1. Quando da admissão de colaborador mediante concurso público ou processo seletivo similar, deverá ser prevista em edital e em cláusula contratual uma seleção criteriosa, especificando a obrigatoriedade da apresentação de cópia de certidão negativa de registro criminal, bem como a assinatura de termo de responsabilidade e confidencialidade.

8.2.2. Durante a contratação

8.2.2.1. A gestão de recursos humanos deverá, com apoio do Gestor de Segurança da Informação definir os requisitos de segurança necessários para o

exercício de cargos e funções de natureza sensível, assim como o grau de sensibilidade dos cargos e das funções existentes, no intuito de identificar formalmente aqueles que, em razão de suas atribuições, tarefas e responsabilidades, possam acessar informações sensíveis.

8.2.2.2. As credenciais de acesso só deverão ser entregues ao(s) contratado(s) quando todos os documentos que descrevem as obrigações relativas à Segurança da Informação estiverem assinados, incluindo os acordos de responsabilidade e confidencialidade.

8.2.3. Encerramento e mudança na contratação

8.2.3.1. Estes processos deverão contemplar a comunicação com os responsáveis pelo gerenciamento dos acessos lógicos, de forma a garantir que sempre as credenciais de acesso dos colaboradores estejam atualizadas e em conformidade com a situação do vínculo contratual atual.

8.2.3.2. Deverá ser normatizado o procedimento de desligamento, de forma a interromper o acesso aos sistemas corporativos e a vinculação com o colaborador desligado, bem como o procedimento de devolução de ativos de informação sob custódia do(s) contratado(s).

8.2.3.3. Todos os acessos dos colaboradores desligados deverão ser removidos.

8.3. Controle de acesso lógico

8.3.1. O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

8.3.2. Periodicamente, os acessos concedidos ao colaborador devem ser revistos e auditados pelo Gestor de Segurança da Informação.

8.3.3. Acesso à rede, ao sistema operacional e às aplicações

8.3.3.1. O acesso aos recursos computacionais deverá ser individual, pessoal e intransferível, ficando o usuário responsável pela guarda de suas credenciais de acesso aos recursos computacionais.

8.3.3.2. O controle de acesso lógico deverá ser composto por processos que contemplem autenticação, autorização e auditoria.

8.3.3.3. O acesso lógico à rede deverá ser controlado de forma centralizada através de procedimentos formais a partir do perfil de cada usuário, no qual estará definido seu nível de autorização.

8.3.3.4. Uma norma complementar deverá ser elaborada pelo PRODERJ, para o controle de acesso lógico.

8.3.3.5. Todo serviço de rede não autorizado deverá ser bloqueado ou desabilitado.

8.3.3.6. Todas as transações em rede deverão estar protegidas através de mecanismos de segurança.

8.3.3.7. O acesso a sistemas e aplicações deverá ocorrer sempre através de um procedimento seguro de acesso ao sistema (no mínimo login e senha), projetado para minimizar oportunidades de acessos não autorizados.

8.3.3.8. O acesso aos ativos deverá estar estritamente vinculado à execução do trabalho de cada usuário, e deve ser concedido em conformidade ao princípio do privilégio mínimo.

8.3.3.9. É vedada a utilização de logins genéricos com senha padrão de conhecimento por mais de um colaborador.

8.3.3.9.1. Quando não for possível, por necessidade de processo ou deficiência tecnológica remover esse tipo de acesso, o mesmo deverá ser mapeado como Desvio de Segurança da Informação e deverá ser inserido no mapa de riscos e de não conformidades.

8.3.3.9.2. Usuários genéricos devem ser autorizados pelo Gestor de Segurança da Informação e, cada um deles, deve possuir um único responsável, identificável com matrícula, que será responsabilizado por eventuais incidentes de segurança relacionados e essa credencial.

8.3.3.10. Visando proteger a infraestrutura contra ataques do tipo *ransomware*, *zero day* ou de *worms,* usuários administrativos (locais ou de domínio) não podem ser utilizados para tarefas que não requeiram privilégios administrativos. Devendo ser usados pontualmente, apenas para tarefas que requeiram elevação de privilégios.

8.3.3.11. Deverão ser estabelecidas normas complementares para uso da rede *wi-fi* disponibilizada, tanto por seus colaboradores quanto para os visitantes, e para a instalação e configuração de sistemas operacionais, aplicativos e demais programas nas estações de trabalho.

8.3.4. Utilização de senhas

8.3.4.1. Não é permitido o compartilhamento de senhas.

8.3.4.2. Recomendações de implantação de usos de senha:

8.3.4.2.1. As senhas devem ter – no mínimo - 10 caracteres e deve incluir letras maiúsculas e minúsculas, números e símbolos.

8.3.4.2.2. Utilizar senhas diferentes para cada conta de um mesmo usuário.

8.3.4.2.3. Não utilizar palavras e nomes próprios nas senhas, ou informações pessoais, como o próprio nome, nome de um membro da família ou animal de estimação, data de nascimento, etc.

8.3.4.2.4. Alterar as senhas regularmente. Se há indício de comprometimento de conta, alterar as senhas imediatamente. Não reutilizar senhas antigas.

8.3.4.2.5. Não permitir que o gerenciador de senhas do navegador armazene as senhas; alguns navegadores armazenam e exibem senhas em texto não criptografado e não implementam proteção por senha por padrão.

8.3.4.2.6. Não permitir que sites façam *login* automaticamente em uma conta; muitos serviços armazenam essas informações localmente e podem ser exploradas por invasores para obter acesso sem uma senha.

8.3.4.2.7. Não compartilhar senhas com ninguém e não responder a e-mails ou telefonemas solicitando as credenciais de login. Empresas legítimas nunca solicitarão credenciais de login por meio desses métodos.

8.3.4.2.8. Não utilizar o e-mail institucional para cadastro em sites pessoais ou para tratar de assuntos particulares.

8.3.4.2.9. Sempre que disponível, utilizar a autenticação em dois fatores que consiste em algo conhecido (senha) e algo que possua (telefone celular, chave física, etc.).

8.3.5. Uso de dispositivos móveis

8.3.5.1. O uso de dispositivos móveis deverá ser regulamentado através de norma complementar. Esses dispositivos somente poderão ser utilizados para acessar a rede e ou recursos computacionais caso ofereçam suporte para autenticação, no mínimo, por usuário e senha, ferramentas de criptografia e proteção contra malwares. Procedimentos adicionais deverão ser elaborados para assegurar a gestão e o monitoramento desses equipamentos.

8.3.6. Trabalho Remoto

8.3.6.1. Deverá ser estabelecida documentação complementar e procedimento operacional quanto ao uso, gestão, responsabilidades e controles dos acessos efetuados por usuários (colaboradores, clientes e fornecedores) à rede e ou recursos computacionais em trabalho remoto, assim considerado aquele realizado fora das instalações físicas da administração estadual.

8.3.7.* Procedimentos de *logging

8.3.7.1. Os softwares de segurança deverão manter registros sobre os acessos dos usuários para atender a legislação pertinente, conforme norma complementar específica sobre o tema;

8.3.7.2. Os sistemas gerenciadores de bancos de dados, os principais servidores, serviços e ativos de conexão de rede, deverão gerar logs próprios e enviá-los para servidores de armazenamento de forma que permitam a recuperação do histórico das operações realizadas na organização;

8.3.7.3. Convém adotar uma solução de análise e gestão de logs que permita a consolidação de *logging*, geração de relatórios e emissão automática de alertas para os eventos que possam representar riscos para a segurança da infraestrutura tecnológica e dos sistemas de informação;

8.3.7.4. Em atendimento ao Marco Civil, os logs deverão ser mantidos pelo período mínimo de um ano, sempre respeitando as restrições e determinações da LGPD.

8.4. Criptografia

8.4.1. Gestão de chaves criptográficas e uso de criptografia

8.4.2. É recomendado o uso de criptografia em serviços de rede e web, redes e canais de comunicação de dados, mecanismos para autenticação em sistemas e demais ambientes tecnológicos.

8.4.3. Deverá ser definido um processo formal para proteger chaves criptográficas corporativas, contemplando os requisitos referentes ao gerenciamento ao longo de todo o seu ciclo de vida incluindo a geração, armazenagem, arquivamento, recuperação, distribuição, retirada e destruição das chaves, considerando a geração de registro e auditoria das atividades relacionadas com o gerenciamento das mesmas.

8.5. Anonimização e Pseudonimização

8.5.1. É recomendável a utilização de dados anonimizados, procedendo a exclusão dos identificadores diretos (ex.: nome, RG, CPF, passaporte), de forma definitiva, promovendo, o descarte de possíveis registros e rastros remanescentes que recuperar tais dados;

8.5.1.1. Dados anonimizados não serão considerados dados pessoais para fins da Lei 13.709/18;

8.5.2. A utilização de pseudonimização é recomendável quando houver necessidade transitória de um mascaramento dos dados pessoais, haja vista ser possível a recuperação do dado;

8.5.2.1. Dados pseudonimizados são considerados dados pessoais para fins de incidência da LGPD.

8.6. Segurança física e do ambiente

8.6.1. Entrada e saída de pessoas

8.6.1.1. A movimentação de pessoal nos ambientes institucionais, deverá ser registrada e monitorada, para serem utilizados em caso de incidentes de segurança da informação cuja investigação e resolução possam ser feitas com o auxílio destes instrumentos. Uma norma complementar deverá ser elaborada para a segurança física e do ambiente, incluindo o controle de acesso físico.

8.6.1.2. Deverão ser criados mecanismos para identificação e controle de acesso de colaboradores, e estabelecidos os controles necessários e suficientes que salvaguardem o acesso às instalações que contenham ativos de TIC.

8.6.1.3. Os colaboradores deverão utilizar algum tipo de identificação em todas as dependências institucionais do Governo do Estado do Rio de Janeiro.

8.6.1.4. Deverão ser criados mecanismos de controle de acesso em horários especiais, fora do expediente normal, indicando quem teve acesso, data e hora e quem autorizou.

8.6.1.5. Os visitantes deverão ser acompanhados durante o todo o período em que permanecerem nas instalações institucionais, pretendendo-se assim evitar que circulem em locais de acesso restrito.

8.6.2. Entrada e saída de equipamentos de TIC

8.6.2.1. É extremamente importante o registro da tramitação de equipamentos de TIC dentro de instituições públicas, uma vez que estes fazem parte do patrimônio do Estado.

8.6.2.2. Para a segurança das informações, além dessa tramitação, deverão ser registradas informações pertinentes a quem é o gestor do patrimônio, quem é o responsável por ele e com quem está a sua custódia.

8.6.2.3. Os equipamentos de TIC institucionais só poderão sair das instalações institucionais mediante a apresentação autorização de saída de material assinada pelo gestor da área responsável pela custódia do ativo e pelo responsável do setor de patrimônio.

8.6.3. Proteção predial e infraestrutura

8.6.3.1. Quanto a instalações e equipamentos de TIC considerados críticos, deverá ser estabelecida norma complementar que discipline as exigências de segurança física, tais como: restrições de acesso ao público; critérios para contratação de seguros; proteção de instalações elétricas e de telecomunicação; segurança em escritórios, salas e instalações; proteção contra ameaças externas e do meio ambiente; áreas de entrega e de carregamento, quanto à remoção ou descarte de ativos de TIC e outras.

8.6.3.2. Deverá ser estabelecida uma norma complementar para regulamentar o uso de câmeras de monitoramento por CFTV para controle de movimentações e para auxiliar na investigação e resolução de problemas envolvendo equipamentos de TIC. Devem ser estabelecidos os prazos mínimos, aceitáveis legalmente, para garantir o armazenamento destas imagens de forma que estejam disponíveis para uso posterior.

8.7. Comunicação segura

8.7.1. Segurança dos serviços de rede

8.7.1.1. O ambiente de rede deve ser segmentado, separando ambientes computacionais de acordo com a sua característica e finalidade com controle de acesso seguro por funcionalidade (Ex.: rede local de usuários, de serviços em desenvolvimento, de serviços em homologação, de serviços em produção, etc.);

8.7.1.2. A rede deve ser monitorada, para viabilizar a rastreabilidade em auditorias. Deverão ser adotados controles e mecanismos de gerenciamento dos serviços de rede em todos os níveis;

8.7.1.3. Uma norma complementar deverá ser estabelecida para formalizar e documentar essa segmentação.

8.7.2. Transferência de informações

8.7.2.1. Deverão ser definidas as regras e procedimentos de segurança, norteados pela legislação pertinente, como a LGPD – Lei nº 13.709 – para troca de informações e softwares internamente, entre os órgãos e entidades da Administração Pública do Poder Executivo Estadual e ou com quaisquer entidades externas.

8.8. Aquisição, desenvolvimento e manutenção de sistema de informação

8.8.1. Requisitos de segurança em sistemas de informação

8.8.1.1. Requisitos relacionados com Segurança da Informação deverão ser incluídos entre os requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

8.8.1.2. Deverão ser utilizados métodos para identificar os requisitos de segurança da informação, como a necessidade de conformidade com políticas e regulamentações, ameaças, análises de incidentes ou de vulnerabilidades. O resultado desta identificação deve ser documentado e analisado criticamente pelas partes interessadas.

8.8.1.3. A identificação e gestão dos requisitos de segurança da informação e os processos associados devem estar integrados aos estágios iniciais dos projetos de sistemas da Informação.

8.8.1.4. Requisitos de segurança deverão ser compatíveis com o nível de segurança exigido pelas regras operacionais e com o impacto gerado em caso de falha.

8.8.1.5. Deve haver um processo formal para aquisição de sistemas de informação onde sejam especificados os requisitos de segurança da informação e seus testes. O não atendimento de algum requisito deve ter sua análise de riscos avaliada criticamente antes da aquisição. Os contratos com os fornecedores devem conter o atendimento aos requisitos de segurança da informação identificados.

8.8.1.6. Os requisitos de segurança da informação devem contemplar: requisitos de autenticação do usuário, identificação da responsabilidade e obrigações dos usuários e operadores, definição dos requisitos de disponibilidade, confidencialidade e integridade, requisitos de registros de transações (logs), monitoramento e não repúdio, necessidade de detecção de vazamento de dados, segurança do sistema operacional e proteção dos canais de comunicação de redes. Uma norma complementar deverá ser elaborada para aquisição, desenvolvimento e manutenção de sistemas de informação.

8.8.2. Processamento correto nas aplicações

8.8.2.1. Deverão ser disponibilizados ambientes segregados para desenvolvimento, homologação, testes e produção de sistemas, para reduzir as oportunidades de uso e modificações indevidas não autorizadas.

8.8.2.2. O acesso ao ambiente de produção deverá ser restrito para evitar comprometimento da integridade das informações.

8.8.3. Segurança no processo de desenvolvimento e suporte

8.8.3.1. Deverá ser adotada metodologia de desenvolvimento de sistemas formal que contemple as fases de iniciação, planejamento, desenvolvimento, implantação, operação e manutenção e desativação para orientar as atividades do desenvolvimento de sistemas de informação em todo o seu ciclo de vida.

8.8.3.2. Deverão ser contempladas na metodologia de desenvolvimento de sistemas, desde a fase inicial, etapas que apresentem orientações e remetam a identificação dos requisitos de segurança da informação e conformidades, a verificações e testes de segurança.

8.8.3.3. A metodologia utilizada para o desenvolvimento de sistemas deve conter atividades e tarefas relativas à segurança da informação em todo o ciclo de vida de desenvolvimento do sistema.

8.8.3.4. Uma norma complementar deverá ser escrita formalizando essa metodologia.

8.8.3.5. É recomendada a elaboração e manutenção de um manual de boas práticas para a construção de códigos seguros.

8.8.3.6. O desenvolvimento de software terceirizado deve garantir que a parte externa esteja em conformidade com as regras de desenvolvimento seguro.

8.8.4. Gestão de vulnerabilidades técnicas

8.8.4.1. Deverão ser contempladas na metodologia de desenvolvimento de sistemas atividades que identifiquem antecipadamente vulnerabilidades que possam ser eliminadas antes da implantação do sistema em produção.

8.8.5. Testes

8.8.5.1. Os requisitos de segurança deverão ser testados de forma rigorosa por equipe que não esteve envolvida diretamente no desenvolvimento da aplicação.

8.9. Relacionamento com o fornecedor

8.9.1. Termo de Responsabilidade e Confidencialidade para Fornecedores

8.9.1.1. No caso dos prestadores de serviço, as obrigações relativas ao sigilo de informações deverão ser formalizadas através da assinatura do Termo de Responsabilidade e Confidencialidade para Fornecedores.

8.9.2. Cláusulas de segurança na contratação

8.9.2.1. Os contratos, resguardada a devida consulta antecedente à Procuradoria Geral do Estado, deverão prever os requisitos de segurança pertinentes, regras de conduta internas e externas, responsabilidades das partes durante a execução do contrato, acordos de nível de serviço (SLA) e as penalidades aplicáveis em caso de não cumprimento de cláusulas relativas à Segurança da Informação e proteção de dados pessoais.

8.9.3. Computação em Nuvem (*Cloud computing*)

8.9.3.1. A contratação de serviço em nuvem deverá atender aos requisitos deste documento e das normas e legislação estadual, quanto a confidencialidade e propriedade, bem como a localização dos dados armazenados.

8.9.3.2. A empresa contratada deverá assegurar que segue padrões nacionais e internacionais de segurança em computação na nuvem.

8.9.3.3. Uma norma complementar deverá ser elaborada pelo PRODERJ, para uso de computação na nuvem.

8.10. Gestão de Mudança

8.10.1. A adequada gestão de mudança exerce papel fundamental na garantia da disponibilidade e integridade dos serviços prestados. O Gestor de Segurança da Informação deverá estabelecer e garantir que seja cumprido um procedimento de gestão de mudança.

8.10.2. Uma norma complementar para a gestão de mudança será estabelecida a fim de garantir que modificações em recursos de Tecnologia da Informação sejam processadas, levando-se em consideração o grau de importância dos sistemas e processos de negócio envolvidos.

8.11. Gestão de incidentes de segurança da informação

8.11.1. O Gestor de Segurança da Informação deve estabelecer um processo para resposta a incidentes de forma a assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

8.11.2. Todos os incidentes de segurança da informação deverão ser imediatamente comunicados ao Gestor de Segurança da Informação.

8.11.3. A não comunicação dos incidentes de segurança configura falta grave.

8.11.4. Uma norma complementar para a gestão de incidentes de segurança da informação será estabelecida pelo Gestor de Segurança da Informação.

8.12. Desvio de Segurança da Informação

8.12.1. Caso um colaborador ou um setor identifique impedimento ou não possa adotar um ou mais itens determinados neste documento, deve solicitar um Desvio de Segurança da Informação.

8.12.2. O Gestor de Segurança da Informação deverá analisar, identificar qualitativa e quantitativamente os riscos inerentes ao desvio. A área solicitante deverá arcar com os riscos identificados.

8.12.3. O Gestor de Segurança da Informação poderá vetar a solicitação caso identifique um risco grave à segurança.

8.12.4. O Gestor de Segurança da Informação deverá manter os registros dos Desvios de Segurança da Informação autorizados e revisar anualmente estas concessões, visando reduzir o nível de risco.

8.13. Orientações ao colaborador em geral

8.13.1. Uso aceitável dos ativos

8.13.1.1. Apenas os equipamentos e *software* disponibilizados e/ou homologados podem ser instalados e conectados à rede;

8.13.1.2. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização;

8.13.1.3. Os ativos são destinados às atividades laborais, sendo vedado o uso para fins que não sejam do interesse da administração pública;

8.13.1.4. Todo o resultado do trabalho efetuado com os ativos institucionais é propriedade do Governo do Estado do Rio de Janeiro.

8.13.2. Cuidados cotidianos

8.13.2.1. Nenhuma informação classificada como secreta, ultrassecreta ou pessoal deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

8.13.2.2. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

8.13.2.3. Monitores deverão ser bloqueados sempre que não estiverem em uso.

8.13.3. Transferência de informações

8.13.3.1. Todo envio e/ou recebimento de documentos classificados como reservado, secreto, ultrassecreto ou pessoal, por meios digitais, deverá ser feito somente para as pessoas que possuam direito a ter acesso às informações conforme definição do Controlador.

8.13.3.2. Quando utilizados meios digitais, a comunicação deverá, sempre que possível, ser criptografada. Quando não for possível a utilização de criptografia, esse Desvio de Segurança da Informação deverá ser informado e ser contabilizado no mapa de risco.

8.13.4. Acesso à Internet, redes sociais e comunicadores instantâneos

8.13.4.1. É permitida a utilização de Internet por padrão. Essa utilização deve servir às funções profissionais e o interesse público respeitando este documento e todas as normas complementares, bem como a legislação em vigor.

8.13.4.2. A utilização de redes sociais deve ser restrita às funções que necessitam destes acessos para atividades profissionais. Esses acessos deverão ser devidamente solicitados pelo respectivo setor e autorizados pelo Gestor de Segurança da Informação. Esses acessos são passíveis de auditoria.

8.13.4.3. A utilização de comunicadores instantâneos, (tais como WhatsApp, Messenger, Telegram, Signal entre outros) não é permitida por padrão. A utilização é permitida para fins profissionais, com autorização do setor solicitante e avaliação de risco por parte do Gestor de Segurança da Informação.

8.13.4.4. Todos os acessos são registrados e as atividades podem ser monitoradas visando sempre à melhoria da segurança da informação bem como o cumprimento da legislação existente.

8.13.4.5. Não é permitido o envio ou recebimento (upload e download) de qualquer informação classificada para redes sociais, comunicadores instantâneos ou qualquer site da Internet.

8.13.4.6. Deverão ser estabelecidas normas complementares para o uso da Internet e de outras redes públicas de computadores, bem como para o uso seguro de redes sociais, com o objetivo de reduzir o risco a que estão expostos os ativos de Tecnologia da Informação do Governo do Estado Rio de Janeiro, tendo em vista que a Internet tem sido veículo de muitas ações prejudiciais às organizações, gerando perdas de imagem, perdas de produtividade, danos aos sistemas e à organização, entre outras consequências.

8.13.5. Conscientização de Segurança da Informação

8.13.5.1. O Gestor de Segurança da Informação deverá desenvolver programas de capacitação específicos e campanhas para conscientização e divulgação destes procedimentos de segurança da informação e da comunicação, bem como de suas normas complementares, visando a ampliação da cultura organizacional, quanto à importância da Segurança da Informação e seu valor estratégico.

8.13.6. Acesso ao correio e a ferramentas de colaboração

8.13.6.1. Deverão ser estabelecidas regras para utilização de correio eletrônico e ferramentas de colaboração providas pelo Governo do Estado do Rio de Janeiro. Uma norma complementar deverá ser elaborada para acesso ao correio eletrônico.

8.13.7. Proteção contra códigos maliciosos

8.13.7.1. Deverão ser estabelecidas regras para a proteção dos recursos de Tecnologia da Informação contra ação de códigos maliciosos e programas impróprios. Uma norma complementar será elaborada para regulamentar a proteção contra código malicioso.

8.14. Gestão de riscos e Continuidade de Operações

8.14.1. Análise, avaliação e tratamento de riscos

8.14.1.1. O Gestor de Segurança da Informação deverá estabelecer regras para implementar um processo sistêmico de gerenciamento de riscos de Segurança da Informação, contemplando análise e avaliação, tratamento, aceitação e comunicação de riscos. Uma norma complementar deverá ser elaborada para a gestão de riscos.

8.14.1.2. O Gestor de Segurança da Informação deve manter um mapa de risco atualizado que contemple os aspectos quantitativos e qualitativos, bem como as ações e projetos para mitigar cada tipo de risco identificado.

8.14.1.3. A Infraestrutura tem como missão manter o nível de risco o mais baixo possível.

8.14.1.4. Os riscos deverão ser identificados através de:

- auditorias;
- análises de Vulnerabilidades;
- testes de Invasão;
- desvios de Segurança da Informação;
- e-mails enviados recebidos;
- consultorias externas;
- recomendações do PRODERJ, da ABNT, bem como de outros órgãos governamentais e entidades de caráter técnico com notória importância nos estudos sobre o tema.

8.14.2. Gestão de continuidade de operações

8.14.2.1. O Gestor de Segurança da Informação deverá estabelecer regras e princípios que regulamentem a gestão da continuidade operacional, através de um processo sistêmico, para que se construa uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes críticos de segurança da informação e salvaguardar as atividades e a reputação da Administração Direta e Indireta do Governo do Estado do Rio de Janeiro. Uma norma complementar será elaborada para a gestão da continuidade de operações

8.15. Monitoramento e auditoria

8.15.1. Deverão ser estabelecidas, pelo PRODERJ, regras para criação de um programa de auditoria do processo de Gestão da Segurança da Informação, visando a verificar o cumprimento dos procedimentos determinados neste documento e

se os controles implementados estão atendendo eficazmente à conformidade dos requisitos.

8.15.2. Um plano de ação deverá ser elaborado, com base no relatório da auditoria e a análise crítica do PRODERJ, para estabelecer ações preventivas e corretivas para a melhoria contínua do processo de Gestão de Segurança da Informação.

8.15.3. O resultado de auditoria de Segurança da Informação deverá ser caracterizado como informação reservada, quando este puder comprometer a segurança dos processos.

8.16. Gestão de Indicadores de Segurança

8.16.1. É responsabilidade do Gestor de Segurança da Informação elaborar e manter indicadores de Segurança da Informação que permitam avaliar o grau de maturidade em relação à de exposição de risco de segurança, objetivando monitorar, através de uma análise crítica, o desempenho e eficácia dos controles implementados. Os indicadores deverão ser criados baseados nos objetivos estratégicos da Segurança da Informação.

8.16.2. A análise crítica deverá ser realizada em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia e demonstrar apoio e comprometimento com a Segurança da Informação.

9. PENALIDADES E PROCESSO DISCIPLINAR

9.1. Nos casos em que houver violação deste documento ou de suas normas e demais documentos complementares, sanções administrativas e ou jurídicas poderão ser adotadas, resguardados o devido processo legal, o contraditório e a ampla defesa.

9.2. As violações de segurança devem ser informadas ao Gestor de Segurança da Informação. Toda violação, configura Desvio de Segurança da Informação e deve ser investigada para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

9.3. Exemplos que podem ocasionar sanções:

9.3.1. Uso ilegal de software;

9.3.2. Introdução (intencional ou não) de vírus de informática;

9.3.3. Tentativas de acesso não autorizado a dados e sistemas;

9.3.4. Compartilhamento de informações ou documentos classificados como reservado, secreto, ultrassecreto ou pessoal;

9.4. Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta norma, o colaborador deve entrar em contato com o Gestor de Segurança da Informação do seu órgão ou entidade.

9.5. A não comunicação de incidentes de segurança da informação é falta grave.

10. ATUALIZAÇÃO

10.1. Deverá ser estabelecida a periodicidade, mínima de um ano e máxima de cinco anos, para a revisão deste documento, bem como os demais documentos

normativos gerados a partir dele, a fim de que não fiquem ultrapassados ou desatualizados.

10.1.1. Sempre que se fizer necessário, este documento poderá ser revisado independentemente da periodicidade aqui estabelecida.

10.1.2. As alterações feitas deverão ser registradas no campo adequando em Controle do Documento.

11. REFERÊNCIAS LEGAIS E NORMATIVAS (CONFORMIDADE)

11.1. Deverá ser disponibilizada, pelo PRODERJ, no portal do SETIC, para o conhecimento de todos, relação de normas e leis referentes à Segurança da Informação.

11.2. A gestão de Segurança da Informação deverá atender aos requisitos legais dos órgãos regulatórios do Governo Estadual e Federal, assim como às normas ABNT – relativos à Segurança de Informação – aplicáveis, entre elas as normas NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação.

Anexo I: critérios de restrição à informação reservada

- comprometer atividades (art. 23, VIII, da Lei 12.527/11);
- conteúdo das propostas (art. 3º, §3º, da lei n 8.666/93);
- controle interno (art. 26, §3º, da lei 10.180/01);
- direito autoral (art. 24, III, da lei 9.610/98);
- documentos preparatórios (art. 7º, §3º, da lei n 12.527/11);
- informação pessoal (art. 31, da lei 12.527/11);
- informação de adolescente (art. 143 e 247, da lei 8.069/90 – ECA);
- informação para instruir processo arbitral (art. 27, par. Único, Código de Ética);
- informação para instruir processo judicial (art. 27, par. Único, Código de Ética);
- informações privilegiadas de sociedades anônimas (art. 155, §2º, lei 6.404/76);
- interceptação de comunicações telefônicas (art. 8º, caput, lei n 9.296/96);
- investigação de responsabilidade de servidor (art. 150, lei 8.112/90);
- lei de mediação (art. 30, lei 13.140/15);
- livros e registros contábeis empresariais (art. 1.190, do Código Civil);
- operações bancárias (art. 1º da Lei Complementar n 105/2001);
- preservação da imagem (art. 12, §3º, do Decreto nº 46.336/18);
- proteção da propriedade intelectual de software (art. 2º, lei 9.609/98);

- proteção relativa às informações (art. 20 e art. 3º, XII, Decreto nº 7.724/12);
- protocolo – pendente análise de restrição de acesso (art. 6º, III, lei 12.527/11);
- segredo industrial (art. 195, XIV, lei 9.279/96);
- segredo de justiça no processo civil (art. 189, CPC);
- segredo de justiça no processo penal) art. 201, §6º, CPP);
- segurança de instituições, autoridades e familiares (art. 23, VII, lei 12.527/11);
- sigilo bancário (art. 1º Lei Complementar 105/2001);
- sigilo das comunicações (art. 3º, V, lei 9.472/97);
- sigilo de empresa em situação falimentar (art. 169, da lei n 11.101/05);
- sigilo de inquérito policial (art. 20, do CPP);
- situação econômico-financeira de sujeito passivo (art. 198, caput, da lei 5.172/66-CTN);
- índices de participação dos municípios – ICMS (art. 20, da Resolução SEFAZ n 720/2014).

Anexo II: **m**odelo de termo de confidencialidade e sigilo

TERMO DE CONFIDENCIALIDADE E SIGILO

Eu, _____,

inscrito(a) no CPF sob o n°_____, na condição de [prestador de serviço, visitante, doravante designado simplesmente **RESPONSÁVEL**, me comprometo, por intermédio do presente TERMO DE CONFIDENCIALIDADE E SIGILO, a não divulgar, sem autorização prévia e formal, exceto aquelas as quais o cargo autorizar, quaisquer informações de propriedade do [NOME DO ÓRGÃO], em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA

O objeto deste instrumento é o compromisso de sigilo, para fins de resguardo e proteção de toda e qualquer informação a que o RESPONSÁVEL venha a obter do [NOME DO ÓRGÃO] em razão da [prestação de serviço / visitação / outros a especificar].

CLÁUSULA SEGUNDA

O **RESPONSÁVEL** obriga-se a manter o sigilo e a não utilizar nenhum tipo de informação obtida, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros, bem como a não realizar nenhum tipo de repasse dessas informações, salvo nas hipóteses legais ou acordadas.

CLÁUSULA TERCEIRA

O **RESPONSÁVEL** obriga-se a informar imediatamente ao [NOME DO ÓRGÃO] qualquer violação das regras de sigilo ora estabelecidas, que tenham ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus colaboradores, prepostos e prestadores de serviços.

CLÁUSULA QUARTA

O descumprimento de quaisquer das cláusulas do presente termo acarretará responsabilização administrativa, civil e criminal dos que, comprovadamente, estiverem

envolvidos no descumprimento ou violação, resguardados o devido processo legal, o contraditório e a ampla defesa.

CLÁUSULA QUINTA

Este termo torna-se válido a partir da data de sua efetiva assinatura.

CLÁUSULA DÉCIMA TERCEIRA

O presente Termo tem natureza imprescritível, irrevogável, irretratável e o seu não cumprimento acarretará todos os efeitos de ordem penal, civil e administrativa contra seus transgressores.

Para dirimir quaisquer dúvidas oriundas do presente Termo, fica eleito o foro da Comarca [definir o foro], com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E por estarem justas e acordadas, as PARTES assinam este instrumento em 02 (duas) vias de idêntico conteúdo e forma, na presença de 02 (duas) testemunhas, abaixo arroladas.

[CIDADE/RJ] ,_____ de _____ de _____.

_____
ASSINATURA E NOME DO RESPONSÁVEL:
CPF:

_____
ASSINATURA E NOME DA TESTEMUNHA:
CPF:

_____
ASSINATURA E NOME DA TESTEMUNHA:
CPF: