ANEXO ÚNICO

AGENTE DE SEGURANÇA SOCIOEDUCATIVA									
QUANT	**ID FUNCIONAL**	**VÍNCULO**	**NOME**	**REFERÊNCIA ATUAL**	**NOVA REFERÊNCIA**	**DATA DE EXERCÍCIO**	**DATA DA VALIDADE**	**PROCESSO**	**NOTA**
1	50367862	1	MARLON CASTELO SILVA	2o G 6	2o G 5	26/02/2015	24/02/2023	E-03/021/250/2019	35
2	50122347	3	ELSON JOSE GOMES DA SILVA	2o G 7	2o G 6	04/07/2018	03/07/2022	SEI-030022/001606/2023	30
3	5704669	1	HELENIVALDO DE SOUZA ALVES	2o G 3	2o G 2	02/05/2003	07/04/2023	E-03/90342/2008	34
5	50178636	1	LARISSA SILVA BARBOSA	2o G 6	2o G 5	10/10/2013	08/10/2021	E-03/021/2195/2017	36
6	5704375	1	MANOEL MARTINS DA SILVA FILHO	2o G 3	2o G 2	09/10/2002	04/10/2022	E-03/90140/2008	27
7	42806704	1	LUIZ CARLOS DA SILVA LEITE	2o G 4	2o G 3	13/06/2007	09/06/2023	E-03/90865/2012	36
8	50232720	1	GILCINEY ANTUNES FABIANO	2o G 6	2o G 5	17/01/2014	15/01/2022	E-03/021/100845/2018	35
9	50367099	1	DANIEL JESUS DE SOUZA LEAL	2o G 6	2o G 5	26/02/2015	24/02/2023	E-03/021/830/2019	36
10	50371797	1	RODRIGO COSTA DE SOUZA	2o G 6	2o G 5	26/03/2015	24/03/2023	E-03/021/982/2019	36
11	19874294	1	MOEMA NOGUEIRA FERREIRA BALTHAZAR	2o G 2	2o G 1	30/06/1999	24/06/2023	E-03/7137/2009	36
12	41771907	1	MARCOS ELIAS AQUINO SOARES	2o G 3	2o G 2	01/07/2003	26/06/2023	E-03/91534/2008	22
ASSISTENTE SOCIAL									
QUANT	**ID FUNCIONAL**	**VÍNCULO**	**NOME**	**REFERÊNCIA ATUAL**	**NOVA REFERÊNCIA**	**DATA DE EXERCÍCIO**	**DATA DA VALIDADE**	**PROCESSO**	**NOTA**
1	50359053	1	ANNE CAROLINE DE ALMEIDA SANTOS	SUP 6	SUP 5	16/01/2015	14/01/2023	E-03/021/379/2019	35
MEDICO									
QUANT	**ID FUNCIONAL**	**VÍNCULO**	**NOME**	**REFERÊNCIA ATUAL**	**NOVA REFERÊNCIA**	**DATA DE EXERCÍCIO**	**DATA DA VALIDADE**	**PROCESSO**	**NOTA**
1	19808631	1	AFFONSO SERGIO LIMA	SUP 2	SUP 1	09/09/1998	04/09/2022	E-03/91466/2008	36
CONTADOR									
QUANT	**ID FUNCIONAL**	**VÍNCULO**	**NOME**	**REFERÊNCIA ATUAL**	**NOVA REFERÊNCIA**	**DATA DE EXERCÍCIO**	**DATA DA VALIDADE**	**PROCESSO**	**NOTA**
1	51024748	1	JANSEN PUEYO PAZ	SUP 7	SUP 6	24/06/2019	23/06/2023	SEI-030022/007111/2023	36

Id: 2491103

SECRETARIA DE ESTADO DE EDUCAÇÃO
DEPARTAMENTO GERAL DE AÇÕES SOCIOEDUCATIVAS

ATO DO DIRETOR-GERAL

PORTARIA DEGASE Nº 1290 DE 06 DE JULHO DE 2023

AUTORIZA A PROGRESSÃO FUNCIONAL DE SERVIDORES DE CARREIRA DO QUADRO DE PESSOAL DO DEGASE.

O DIRETOR-GERAL DO DEPARTAMENTO GERAL DE AÇÕES SOCIOEDUCATIVAS DO ESTADO DO RIO DE JANEIRO - DEGASE, Órgão do Poder Executivo do Governo do Estado do Rio de Janeiro, vinculado à Secretaria de Estado de Educação, por força do Decreto nº 41.334/2008, publicado no D.O. de 02/06/2008, e da Resolução SEEDUC Nº 5.414, de 08/04/2016, publicado no D.O. de 12/04/2016, no uso das atribuições pela legislação em vigor, através do Decreto nº 18.493, de 26 de janeiro de 1993, e o que consta no Processo nº SEI-030022/000413/2020.

CONSIDERANDO:

- a Lei n° 4.802/2006, que dispõe sobre a reestruturação do Quadro de Pessoal do DEGASE e alteração pela Lei nº 6.834/2014, que modifica a redação do art. 10 da Lei em comento quanto à Progressão Funcional;

- o Decreto nº 45.282/2015, que dispõe sobre o regulamento geral para fins de progressão funcional dos servidores do Quadro de Pessoal do DEGASE;

- a Portaria DEGASE nº 171/2015, que dispõe sobre a Avaliação Periódica de Desempenho e a Avaliação Especial de Desempenho, nos termos dos arts. 14 e 21, para fins de Progressão Funcional de servidores pertencentes ao Quadro do DEGASE;

- o Despacho autorizativo para operacionalização da Progressão Funcional aprovada pela Procuradoria Geral do Estado do Rio de Janeiro em consonância com as legislações supramencionadas, conforme o que consta nos autos do Processo nº E-03/022/28/2017;

RESOLVE:

Art. 1º - Alterar a Progressão para os níveis descritos, conforme disposto no Decreto nº 45.282/2015, de 15 de junho de 2015, dos servidores (listados no anexo único) pertencentes ao Quadro de Pessoal do Departamento Geral de Ações Socioeducativas (DEGASE).

Parágrafo Único - A Progressão de que trata o caput terá efeitos financeiros retroativos, conforme a data especificada em planilha do Anexo Único.

Art. 2º - Esta Portaria entrará em vigor na data de sua publicação, revogadas as disposições em contrário.

Rio de Janeiro, 06 de julho de 2023

VICTOR POUBEL
Diretor-Geral - DEGASE

ANEXO ÚNICO

AGENTE DE SEGURANÇA SOCIOEDUCATIVA									
QUANT	**ID FUNCIONAL**	**VÍNCULO**	**NOME**	**REFERÊNCIA ATUAL**	**NOVA REFERÊNCIA**	**DATA DE EXERCÍCIO**	**DATA DA VALIDADE**	**PROCESSO**	**NOTA**
1	50371681	1	WELLINGTON DE SOUZA MACHADO	2o G 6	2o G 5	26/03/2015	24/03/2023	SEI-030022/004918/2022	36
2	50367072	1	ALEXANDRE DE JESUS DO SACRAMENTO	2o G 6	2o G 5	26/02/2015	24/02/2015	SEI-03/022/002786/2019	36
3	41771893	1	VALTER LIMA GONCALVES	2o G 3	2o G 2	01/07/2003	26/06/2023	E-03/90977/2008	36
4	5642434	1	JORGE SANDRO DE CAMPOS RAMIREZ	2o G 3	2o G 2	21/06/2002	16/06/2022	E-03/021/394/2016	35
5	19831854	1	ELIANA COIMBRA MENDONCA	2o G 2	2o G 1	19/03/1999	13/03/2023	E-03/90524/2009	35
6	19876947	1	OLIVIA VIEIRA DE ARAUJO	2o G 2	2o G 1	03/03/1997	25/02/2021	E-03/90363/2008	35
7	50368010	1	MARCOS UTRINI DE LIMA	2o G 6	2o G 5	26/02/2015	24/02/2023	E-03/021/238/2019	30
8	50368087	1	WAGNER VARGAS MENDONCA DE OLIVEIRA	2o G 6	2o G 5	26/02/2015	24/02/2023	E-03/021/292/2019	31
9	50371851	1	ALAN FRANCISCO MACHADO	2o G 6	2o G 5	26/03/2015	24/03/2023	E-03/021/456/2019	36
10	50367960	1	ROMERIO RIBEIRO MARTINS JUNIOR	2o G 6	2o G 5	12/03/2015	10/03/2015	E-03/021/1285/2019	36
11	42542464	1	LEANDRO PEREIRA DO NASCIMENTO	2o G 4	2o G 3	07/03/2006	03/03/2022	E-03/90504/2011	33
AGENTE ADMINISTRATIVO									
QUANT	**ID FUNCIONAL**	**VÍNCULO**	**NOME**	**REFERÊNCIA ATUAL**	**NOVA REFERÊNCIA**	**DATA DE EXERCÍCIO**	**DATA DA VALIDADE**	**PROCESSO**	**NOTA**
1	50975668	1	MARIA LAUDICEIA DIANO DE AZEVEDO	2o G 7	2o G 6	27/12/2018	26/12/2022	SEI-030022/000887/2023	36
2	50975501	1	GESSICA SILVA DA CRUZ	2o G 7	2o G 6	27/12/2018	26/12/2022	SEI-030022/000884/2023	36
3	50975579	1	PEDRO DA ROSA	2o G 7	2o G 6	27/12/2018	26/12/2022	SEI-030022/002468/2023	36
NUTRICIONISTA									
QUANT	**ID FUNCIONAL**	**VÍNCULO**	**NOME**	**REFERÊNCIA ATUAL**	**NOVA REFERÊNCIA**	**DATA DE EXERCÍCIO**	**DATA DA VALIDADE**	**PROCESSO**	**NOTA**
1	50367951	1	RITALENE DE OLIVEIRA PASSOS	SUP 7	SUP 6	26/02/2015	24/02/2023	E-03/021/425/2019	31

Id: 2491699

Secretaria de Estado de Ciência, Tecnologia e Inovação

ADMINISTRAÇÃO VINCULADA

SECRETARIA DE ESTADO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO
FUNDAÇÃO CARLOS CHAGAS FILHO DE AMPARO À PESQUISA DO ESTADO DO RIO DE JANEIRO

ATO DO PRESIDENTE

PORTARIA FAPERJ/PR Nº655 DE 08 DE AGOSTO DE 2023.

INSTITUI O MANUAL DE PROCEDIMENTOS REGULATÓRIOS DE SEGURANÇA DA INFORMAÇÃO DA FUNDAÇÃO CARLOS CHAGAS FILHO DE AMPARO À PESQUISA DO ESTADO DO RIO DE JANEIRO - FAPERJ.

O **PRESIDENTE DA FUNDAÇÃO CARLOS CHAGAS FILHO DE AMPARO À PESQUISA DO ESTADO DO RIO DE JANEIRO - FAPERJ**, no uso de suas atribuições legais, estatutárias e regimentais, e ainda conforme Processo n° SEI-260003/016942/2022;
CONSIDERANDO:

- a Lei n.º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e sua regulamentação pelo Decreto n.º 43.597, de 17 de maio de 2012;

- a Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

- a Portaria PRODERJ/PRE n.º 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, em especial o art. 11, do Anexo B, que trata de ações de governança voltadas à segurança da informação e à proteção de dados;

- o art. 9º da Instrução Normativa/PRE n.º 02, de 28 de abril de 2022, que regulamenta os Procedimentos de Segurança da Informação em Soluções de Tecnologia da Informação e Comunicação - TIC a serem adotados pelos órgãos e entidades integrantes da Administração Direta e Indireta do Poder Executivo do Estado do Rio de Janeiro;

- a Portaria PRODERJ/PRE nº 968, de 05 de Agosto de 2022, que institui o Manual de Procedimentos Regulatórios de Segurança da Informação a ser adotado por todas as repartições, técnicas e administrativas, no âmbito do Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ;

- a necessidade de promover o aperfeiçoamento das boas práticas da área de segurança da informação, estimular e fortalecer essa cultura no Estado; e

- a necessidade de estabelecer conceitos e diretrizes de segurança da informação para implantar e manter processos e ações para gerenciar as ameaças aos recursos de tecnologia da informação e comunicação.

RESOLVE:

Art. 1º - Instituir, na forma desta Portaria e do seu Anexo Único, o Manual de Procedimentos Regulatórios de Segurança da Informação, a ser adotado por todos os setores da Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro - FAPERJ, com a finalidade de contribuir para o aprimoramento da segurança da informação no âmbito da Administração Pública Estadual.

Parágrafo Único. Para os fins do disposto neste instrumento, a segurança da informação abrange:

I - segurança cibernética;

II - defesa cibernética;

III - segurança física;

IV - proteção de dados organizacionais;

V - proteção de dados pessoais; e

VI - ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 2º - Para os fins desta Portaria, o seu Anexo Único dispõe todo procedimento a ser adotado pela Fundação no tocante a segurança da Informação.

Art. 3º - O Anexo Único desta Portaria apresenta o Manual de Procedimentos Regulatórios de Segurança da Informação a ser adotado e cumprido no âmbito da FAPERJ, bem como as penalidades aplicáveis em razão do seu descumprimento.

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

Rio de Janeiro, 08 de agosto de 2023

JERSON LIMA DA SILVA
Presidente

ANEXO ÚNICO
MANUAL DE PROCEDIMENTOS REGULATÓRIOS DE SEGURANÇA DA INFORMAÇÃO - Versão 1.0
FAPERJ
MANUAL DE PROCEDIMENTOS REGULATÓRIOS DE SEGURANÇA DA INFORMAÇÃO
FUNDAÇÃO CARLOS CHAGAS FILHO DE AMPARO À PESQUISA DO ESTADO DO RIO DE JANEIRO - FAPERJ
Presidente
Jerson Lima da Silva
Diretora de Administração e Finanças
Maria Cláudia Ferreira de Souza
Diretor de Tecnologia
Aquilino Senra Martinez
Diretora Científica
Eliete Buskela
1 APRESENTAÇÃO
1.1 No tocante a informação pode-se dizer que constitui um ativo valioso e de extrema importância para a preservação de um órgão e necessita ser convenientemente protegida, independentemente de sua natureza ou 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 a FAPERJ.
1.4 É diretriz que toda informação de propriedade da FAPERJ ou 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;
1.5.4 Autenticidade: confirmar a identidade de quem se diz ser.
1.6 A instituição deste manual é uma declaração formal acerca do compromisso com a proteção, o controle e o monitoramento das informações processadas, armazenadas, transmitidas ou custodiadas pela FAPERJ, que sejam de sua propriedade ou estejam sob a sua guarda.
1.7 O documento apresenta diretrizes para orientar as 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 foram baseadas nas recomendações das publicações da família de normas NBR ISO/IEC 27000.

2. OBJETIVO

2.1 O presente manual tem por objetivo a definição das diretrizes e documentos complementares que viabilizem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações críticas, com a finalidade de garantir a continuidade e a confiabilidade das operações de tecnologia da informação da FAPERJ no que tange a segurança da informação.

3 ABRANGÊNCIA E DIVULGAÇÃO

3.1 Este manual deverá ser adotado e cumprido por todos os servidores e colaboradores da FAPERJ, e suas disposições alcançam a servidores, consultores, pesquisadores, bolsistas, dirigentes, empregados, estagiários, pessoal terceirizado, prestadores de serviços e visitantes desta Fundação.
3.2 As normas de referência, normas complementares e os documentos que integram a estrutura deste Manual deverão estar disponíveis no site institucional da FAPERJ.

4 CONCEITOS E DEFINIÇÕES

4.1 Alta Administração - É o quadro diretivo da Fundação, com legitimidade para representá-lo, na forma dos seus diretores e presidente;
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 no Data Center da FAPERJ;
4.7 Colaborador - Servidor, colaborador, pesquisador externo ou qualquer pessoa que preste serviços à FAPERJ, por qualquer meio de contratação;
4.8 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;
4.9 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;
4.10 Conformidade - Aderência a um padrão previamente estabelecido e aceito como ideal;
4.11 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;
4.12 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;
4.13 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 e backups, entre outros;
4.14 Criticidade - Nível de crise (ou impacto) que pode advir da divulgação ou uso indevido da informação;
4.15 Dado Anonimizado - Técnica de desassociação das informações que inviabiliza de maneira irreversível a identificação direta do titular de dados pessoais;
4.16 Dado Pseudonimizado - Tratamento por meio do qual um dado perde 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;
4.17 Dados Pessoais - informação relacionada à pessoa natural identificada (diretamente) ou identificável (indiretamente);
4.18 Dados Pessoais Sensíveis - 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;
4.19 Defesa Cibernética - Ações realizadas no espaço cibernético para fins de proteção dos ativos de informação de interesse do Estado, bem como para a obtenção de dados para a produção de conhecimento de inteligência;
4.20 Desvio de Segurança da Informação - É um resultado não previsto ou indesejado em um procedimento. É um desvio no procedimento operacional;
4.21 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;
4.22 Dispositivos móveis - Qualquer equipamento ou acessório portátil, capaz de se conectar à internet e ou armazenar dados, tais como: smartphone, tablet, notebook, netbook, PDA, pendrive, CD/DVD, HD externo e assemelhados;
4.23 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;
4.24 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 exigidas para a execução da sua atividade;
4.25 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;
4.26 Integridade - A integridade da informação está relacionada à sua fidedignidade. Assegurar a integridade da informação, portanto, significa garantir que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional;
4.27 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;
4.28 Portarias - Possuem função de complementar e detalhar os procedimentos e instruções de segurança descritos neste Manual. As Portarias são subordinadas a este Manual e à legislação vigente;
4.29 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;
4.30 Perímetro - Delimitação da área física ou lógica de uma instalação onde são aplicadas proteções contra acessos indevidos;
4.31 Plano de continuidade de operações - Processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção;
4.32 Procedimentos Operacionais - Ações padronizadas a serem implementadas no âmbito do órgão, baseadas nas instruções deste documento, bem como nas normas complementares, para fins de implementação de um sistema de controle e de segurança da informação;
4.33 Risco - Resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento e o impacto resultante;
4.34 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;
4.35 Segurança física - Adoção de medidas por meio de pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas;
4.36 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;
4.37 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 Manual, normas complementares, procedimentos operacionais e outros que se façam necessários para o atendimento às diretrizes aqui estabelecidas.
5.2 Os procedimentos operacionais serão elaborados posteriormente, conforme a necessidade ou determinação explícita neste Manual, para descrever métodos e tecnologias a serem aplicados no atendimento às disposições normativas.
5.3 As normas complementares, assim como os procedimentos operacionais, deverão ser elaboradas e implantadas gradualmente, após a aprovação e implantação deste Manual. Estes documentos devem ser revisados no mínimo, anualmente, ou quando novas normas ou legislações o demandarem.

6 APROVAÇÃO

6.1 Este manual é aprovado pela Presidência da FAPERJ e ciência do Conselho Superior da FAPERJ, divulgado através dos meios de comunicação institucional, formalizando o compromisso da FAPERJ com a Segurança da Informação.

7 RESPONSABILIDADES

7.1 Introdução
7.1.1 É responsabilidade de cada colaborador, independentemente da atividade, cargo ou função, observar e cumprir o estabelecido neste manual.
7.1.2 É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades cotidianas na FAPERJ.
7.2 Comissão de Segurança da Informação
7.2.1 É responsabilidade da Comissão:
7.2.1.1 Discutir e aprovar as proposições de normas de Segurança da Informação;
7.2.1.2 Acompanhar a implantação dos projetos de Segurança da Informação no âmbito da FAPERJ;
7.2.1.3 Apoiar e fazer a revisão periódica deste Manual, buscando o alinhamento com o Planejamento Estratégico da FAPERJ;
7.2.1.4 Apoiar todas as ações que permitam a FAPERJ fazer cumprir esse Manual;
7.2.1.5 Apoiar todas as ações que permitam a FAPERJ atender às exigências legais, normas e resoluções nos aspectos relativos à Segurança da Informação.
7.2.1.6 Para maior detalhamento sobre a Comissão de Segurança da Informação, consulte o item 10 deste documento.
7.2.1.7 Elaborar planos de ação específicos para a implementação deste Manual na FAPERJ;
7.2.1.8 Elaborar e executar planos de auditoria com base neste Manual e normas complementares;
7.2.1.9 Elaborar e implantar o Planejamento Estratégico de Segurança da Informação, seguindo as melhores práticas do mercado;
7.2.1.10 Receber e controlar incidentes de segurança da informação;
7.2.1.11 Elaborar e gerenciar projetos de Segurança da Informação, definindo recursos e funções para a execução deles;
7.2.1.12 Elaborar, atualizar e dar visibilidade à alta administração do mapa de risco da FAPERJ conforme Apêndice B;
7.2.1.13 Gerenciar o cumprimento e assegurar a conformidade da FAPERJ com este Manual e normas complementares;
7.2.1.14 Colaborar com a diretoria da FAPERJ na elaboração dos procedimentos operacionais que eventualmente se façam necessários;
7.2.1.15 O rol apresentado não é taxativo, podendo a Comissão atuar nos demais casos que for solicitada e entender pertinente.
7.3 AI - ASSESSORIA DE INFORMÁTICA
7.3.1 Operar a plataforma para prevenção, detecção e reação a incidentes de segurança;
7.3.2 Responder aos incidentes de segurança detectados;
7.3.3 Corrigir as vulnerabilidades nos ativos tecnológicos da FAPERJ;
7.3.4 Manter atualizado, com as últimas correções de segurança, todo o parque de ativos sob sua responsabilidade;
7.3.5 Monitorar os serviços de Segurança da Informação e gerar relatórios periódicos destes equipamentos;
7.3.6 Implementar e monitorar mecanismos de proteção do perímetro;
7.3.7 Implementar mecanismos de proteção (segurança lógica) nas plataformas tecnológicas (bancos de dados, sistemas operacionais, redes, armazenamento, nuvem etc.) e físicas sob a sua responsabilidade;
7.3.8 Controlar de forma segura as credenciais de acesso sob sua custódia;
7.3.9 Garantir a Segurança a Informação sempre que houver uma manutenção no ambiente que possa impactar a disponibilidade de ativos;
7.3.10 Cumprir e garantir o cumprimento de seus colaboradores a este Manual e suas normas complementares.
7.3.11 Garantir a implantação de segurança no processo e no código dos sistemas desenvolvidos;
7.3.12 Garantir a atualização dos códigos desenvolvidos bem como seus frameworks, visando a remoção de vulnerabilidades que venham a ser descobertas;
7.3.13 Garantir a devida segregação dos ambientes de desenvolvimento, homologação e produção;
7.3.14 Garantir a Segurança da Informação para qualquer alteração que necessite ser realizada em produção;
7.3.15 Apoiar e contribuir, em sua área de atuação, para a melhoria das ações de Segurança da Informação na FAPERJ;
7.3.16 Gerenciar as credenciais de acesso dos colaboradores e eventuais alterações;
7.3.17 Receber e tratar a ocorrência de incidentes de Segurança da Informação através do e- mail: seguranca.assinf@faperj.br.
7.3.18 Reportar a ocorrência de incidentes de Segurança da Informação à Presidência da FAPERJ e a Comissão Permanente de Segurança da Informação;
7.4 Departamento de Recursos Humanos
7.4.1 Informar à Assessoria de Informática as atividades de inclusão, exclusão, alteração da base de dados cadastrais de colaboradores no âmbito da FAPERJ;
7.4.2 Manter atualizado os dados cadastrais dos colaboradores no âmbito da FAPERJ;
7.4.3 Auxiliar na divulgação aos colaboradores sobre este manual de Segurança da Informação da FAPERJ, bem como suas normas complementares;
7.4.4 Auxiliar e orientar a todos colaboradores no cumprimento deste manual e suas normas complementares.
7.5 Controlador
7.5.1 Dentro do escopo deste manual, a FAPERJ 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 os procedimentos de segurança Informação e proteção de dados pessoais dos serviços, sistemas ou sites sob sua responsabilidade;
7.5.2.5 Definir a periodicidade de 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 e este manual da Segurança da Informação.
7.5.3 Uma norma poderá detalhar as responsabilidades do controlador da informação, bem como mapear os sistemas, ativos e serviços com os seus respectivos gestores da informação.
7.6 Operador
7.6.1 Dentro do escopo deste manual, a FAPERJ é o responsável pelo tratamento e custódia das informações de outros órgãos 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.
7.7 Usuários em geral
7.7.1 Reportar a ocorrência de Incidentes de Segurança da Informação através do e-mail seguranca.assinf@faperj.br;
7.7.2 Apoiar e sugerir, em sua área de atuação, as ações de Segurança da Informação;
7.7.3 Cumprir este manual e suas normas complementares.

8 DIRETRIZES

8.1 Gestão de ativos
Os ativos disponibilizados pela FAPERJ deverão estar aderentes às melhores práticas de segurança da informação, devendo sofrer, sempre que possível adaptações de segurança (hardening) visando mitigar riscos e tornar o ativo mais resiliente no enfrentamento a tentativas de ataque.
8.1.1 Classificação da Informação quanto ao acesso
8.1.1.1 Toda informação armazenada ou mantida deverá ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade e tendo por parâmetro 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**. Caberá a Comissão de Gestão de Documentos a classificação dos documentos.
8.1.1.2 Caberá a Comissão de Classificação de Documentos realizar a classificação quanto ao grau de sigilo.
8.1.1.3 Qualquer dúvida quanto a classificação de documentos será encaminhado para Parecer da Comissão de Gestão de Documentos e posterior deliberação sobre o acesso pela Presidência da FAPERJ.
8.1.1.4 Não poderão ser incluídos no SEI-RJ documentos que possuam informações classificáveis nos níveis de sigilo estabelecido nos art. 23 e 24 da Lei Federal nº 12.527/2011 e no art. 26 do Decreto nº 46.475/2018, a saber: ultrassecreto, secreto e reservado.
8.1.1.5 A informação será **PÚBLICA** quando não estiver classificada em grau RESERVADO, SECRETO, ULTRASSECRETO ou PESSOAL.
8.1.1.5.1 O acesso à informação PÚBLICA é livre e não há restrição para divulgação, resguardadas as informações de divulgação obrigatória constantes dos art. 8º e 9º, do Decreto nº 46.475/2018.
8.1.1.6 A informação será **RESERVADA** quando não for desejável que ela se torne conhecida por pessoas de fora da organização, sendo habitualmente compartilhada corporativamente (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.
8.1.1.6.1 Tem competência para a atribuição do grau RESERVADO, qualquer servidor que exerça cargo de comando, direção ou chefia (art. 30, III, Decreto nº 46.475/2018).
8.1.1.6.2 A restrição de caráter RESERVADO terá duração máxima de 5 anos (art. 29, III, Decreto nº 46.475/2018), podendo ser anualmente reavaliada a sua condição.
8.1.1.7 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.
8.1.1.7.1 A manipulação de documentos classificados como SECRETOS devem observar as orientações referentes a não exposição pública (ex: permanecer sobre mesas e locais de acesso público, impressoras, copiadoras, etc.), garantindo a confidencialidade dos mesmos.
8.1.1.7.2 Documentos SECRETOS não devem ser expostos à visualização ou acesso público de nenhuma forma.
8.1.1.8 A informação será **ULTRASSECRETA**, 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.
8.1.1.8.1 Só devem ter acesso às informações ULTRASSECRETAS pessoas devidamente autorizadas pela respectiva autoridade que assim classificou a informação, independentemente do cargo ocupado.
8.1.1.9 O pedido de acesso à informação de caráter RESERVADO, SECRETO ou ULTRASSECRETO se dará nos termos dos art. 12 ao 20, ou do §7º do art. 29, todos do Decreto nº 46.475/2018, resguardada a possibilidade de recurso em caso de negativa de autorização de acesso, na forma dos art. 21 ao 25.
8.1.1.10 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.
8.1.1.10.1 As informações de natureza **PESSOAL**, por exigência da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), de-

vem 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.
8.1.1.11 Será instituída normas sobre a guarda, a disponibilização, a circulação e o descarte das informações. Os referidos procedimentos devem resguardar as boas práticas de governança e os princípios inerentes ao quanto disposto neste documento e demais regulamentações.
8.1.1.12 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 da Fundação.
8.1.2 Lei de Acesso à Informação (LAI), Marco Civil e LGPD
8.1.2.1 Normas complementares e procedimentos operacionais deverão ser elaborados para atender aos requisitos da Lei de Acesso à Informação (LAI), Lei nº 12.527, de 18 de novembro de 2011, ao Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, e à Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709, de 14 de agosto de 2018.
8.1.3 Backup e recuperação de dados
8.1.3.1 Os ativos da FAPERJ devem possuir backup com periodicidade definida pelo Controlador;
8.1.3.2 O Controlador deverá, também, definir procedimentos operacionais 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 rede de backup deverão ser devidamente registrados;
8.1.3.6 Sistemas ou serviços que possuam atualização constante deverão ter procedimentos operacionais de backup mais agressiva, a ser definida pelo controlador;
8.1.3.7 A critério do Controlador, poderá ser especificada necessidade de guarda offline
dos backups;
8.1.3.8 Os procedimentos operacionais de 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 datacenter, através de um Plano de Continuidade de Operações (PCO) a ser elaborado pela Assessoria de informática.
8.2 Segurança em Recursos Humanos
8.2.1 Durante a contratação
8.2.1.1 Quando da contratação de qualquer colaborador, o mesmo deverá ter ciência do teor deste Manual, bem como deverá assinar o termo de responsabilidade e de confidencialidade.
8.2.1.2 Caberá a Diretoria responsável comunicar ao Departamento de Recursos Humanos o ingresso, a alteração ou exclusão do colaborador, inclusive quanto ao nível de acesso.
8.2.2 Após a contratação
8.2.2.1 O Departamento de Recursos Humanos, com apoio da Assessoria de Informática, deverá definir os requisitos de segurança necessários para o exercício de cargos e funções de natureza sensível na FAPERJ, assim como o grau de sensibilidade das atividades, cargos e das funções existentes, no intuito de identificar formalmente aqueles que, em razão de suas atribuições, tarefas e responsabilidades, possam acessar informações classificadas.
8.2.2.2 As credenciais de acesso, bem como a custódia de ativos da informação só deverão ser entregues ao(s) contratado(s)/empossado(s) ou qualquer outro colaborador 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 Fica normatizado que pelo DRH com apoio da Assessoria de Informática, o procedimento de desligamento, de interrupção de acesso aos sistemas corporativos e vinculação da FAPERJ ao colaborador desligado, bem como o procedimento de devolução de ativos de informação sob custódia do(s) contratado(s), através da imediata comunicação pela Diretoria Competente.
8.2.3.3 Todos os acessos dos colaboradores desligados deverão ser removidos pelos setores envolvidos, sob coordenação do DRH em conjunto com a Assessoria de Informática, após a imediata comunicação pela Diretoria Competente.
8.2.4 Termo de Responsabilidade e Confidencialidade
8.2.4.1 Todos os colaboradores da FAPERJ deverão assinar o Termo de Responsabilidade e Confidencialidade elaborado pela presente Comissão e gerenciado pelo DRH.
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 aos colaboradores devem ser revistos e auditados pela Assessoria de Informática.
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 Todo serviço de rede não autorizado deverá ser bloqueado ou desabilitado.
8.3.3.5 Todas as transações em rede deverão estar protegidas através de mecanismos de segurança.
8.3.3.6 O acesso a sistemas e aplicações deverá ocorrer sempre através de um procedimento seguro de acesso ao sistema (no mínimo login/senha), projetado para minimizar oportunidades de acessos não autorizados.
8.3.3.7 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.
8.3.3.8 É vedada a utilização de usuário administrador local e unidades de armazenamento USB (pen drives, HDs externos e etc) em estações de trabalho.
8.3.3.8.1 Uma norma complementar poderá ser elaborada sobre a correta utilização de estações de trabalho.
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 risco e não conformidade.
8.3.3.9.2 Usuários genéricos, autorizados pela Assessoria de Informática, devem possuir um único responsável, identificável com matrícula, que será responsabilizado por eventuais incidentes de segurança relacionados a 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 pela FAPERJ, 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 da FAPERJ.
8.3.4 Utilização de senhas
8.3.4.1 Não é permitido o compartilhamento de senhas dentro do âmbito da FAPERJ.
8.3.4.2 As senhas devem ter - no mínimo - 10 caracteres e deve incluir letras maiúsculas e minúsculas, números e símbolos.
8.3.4.3 Não devem ser utilizadas 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.
8.3.4.4 As senhas devem ser alteradas regularmente. Se o colaborador acreditar que sua conta foi comprometida, a senha deve ser alterada imediatamente. As senhas antigas não devem ser reutilizadas.
8.3.4.5 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.
8.3.4.6 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.
8.3.4.7 Não compartilhar senhas com ninguém e não responder a e-mails ou telefonemas solicitando suas credenciais de login. Empresas legítimas nunca solicitarão credenciais de login por meio desses métodos.
8.3.4.8 Não utilizar o e-mail da FAPERJ para cadastrar sites pessoais ou para tratar de assuntos particulares.
8.3.4.9 Sempre que disponível, utilizar autenticação em dois fatores que consiste em algo conhecido (senha) e algo que o colaborador possui (telefone celular, chave física e etc.).
8.3.5 Uso de dispositivos móveis
8.3.5.1 Os procedimentos operacionais para uso de dispositivos móveis na FAPERJ poderão ser regulamentados através de uma 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 Poderá ser estabelecida uma norma complementar com procedimento operacional quanto ao uso, gestão, responsabilidades e controles dos acessos efetuados por usuários (colaboradores, clientes e fornecedores) à rede e ou recursos computacionais da FAPERJ em trabalho remoto, assim considerado aquele realizado fora das suas instalações físicas.
8.3.7 Procedimentos operacionais de logging
8.3.7.1 Os softwares de segurança deverão manter registros sobre os acessos dos usuários para atender a legislação pertinente.
8.3.7.2 Os sistemas gerenciadores de bancos de dados, os principais servidores, serviços e ativos 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 (de acordo com o art. 13, caput, da Lei 12.965/2014), os logs deverão ser mantidos pelo período mínimo de um ano, sempre respeitando as restrições e determinações da LGPD.
8.4 Criptografia e Chaves Criptográficas
8.4.1 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.
8.4.2 A Assessoria de Informática deverá definir 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, a armazenagem, o arquivamento, a recuperação, a distribuição, a retirada e a destruição das chaves, considerando a geração de registro e auditoria das atividades relacionadas com o gerenciamento das mesmas. Assim como quando o processo de codificação se mostrar necessário para resguardar a privacidade e proteção dos dados pessoais.
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 possibilitem 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
8.6.1 Entrada e saída de pessoas
8.6.1.1 A movimentação de pessoal nos ambientes da FAPERJ, deverá ser monitorada, para serem utilizados em caso de incidentes de segurança cuja investigação e resolução possam ser feitas com o auxílio destes instrumentos. Uma norma poderá ser elaborada para a segurança física e do ambiente, incluindo o controle de acesso físico.
8.6.1.2 Os colaboradores deverão utilizar crachá em local de fácil visualização em todas as dependências da FAPERJ.
8.6.1.3 Os visitantes deverão ser acompanhados durante o todo o período em que permanecerem dentro da FAPERJ, pretendendo-se assim evitar que circulem em locais de acesso restrito.
8.6.2 Entrada e saída de equipamentos
8.6.2.1 É extremamente importante o registro da tramitação de equipamentos 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 institucionais só poderão sair da FAPERJ mediante a apresentação da autorização de saída de material assinada pelo Chefe de Departamento e posterior comunicação ao Gestor de Bens Móveis.
8.6.3 Proteção de instalações e equipamentos críticos de infraestrutura
8.6.3.1 Poderá ser elaborada norma complementar regulamentando a proteção a instalações e equipamentos considerados críticos.
8.7 Comunicação segura
8.7.1 Segurança dos serviços de rede
8.7.1.1 A rede da FAPERJ deve ser segmentada em VLANS, separando ambientes computacionais de acordo com a sua característica e finalidade com controle de acesso seguro por funcionalidade;
8.7.1.2 A rede deve ser monitorada pela Assessoria de Informática e pela operadora de telefonia provedora dos links, 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 poderá ser estabelecida para formalizar e documentar a segmentação da rede da FAPERJ.
8.7.2 Transferência de informações
8.7.2.1 Todo o envio e recebimento de documentos classificados, em meios físicos e em meios digitais, deve ser exclusivo para pessoas de acesso autorizado às informações conforme definição do controlador.
8.7.2.2 Quando utilizados meios digitais, a comunicação deverá ser criptografada, sempre que possível. Quando não for possível a utilização de criptografia, esse desvio de segurança da informação deverá ser informado à Assessoria de Informática e ser contabilizado no mapa de risco.
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 durante seu processo de especificação.
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 envolvidas no processo e pela Assessoria de Informática.
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, definido pela Assessoria de Informática, 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 poderá ser elaborada para aquisição, desenvolvimento e manutenção de sistemas de informação.
8.8.2 Processamento correto nas aplicações
8.8.2.1 A Assessoria de Informática deverá disponibilizar 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 A Assessoria de Informática, deverá elaborar e manter um manual de boas práticas para a construção de códigos seguros.
8.8.3.5 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 e pelo colaborador especializado.
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 e Parceiros, elaborado pela Assessoria de Informática e entregue ao fornecedor pela área contratante.
8.9.2 Cláusulas de segurança na contratação
8.9.2.1 Os contratos 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. Esses requisitos de segurança da informação e proteção de dados pessoais, definidos pela Assessoria de Informática, deverão constar de todo contrato.
8.9.3 Computação em Nuvem (Cloud Computing)
8.9.3.1 A contratação de serviço em nuvem deverá atender aos requisitos deste manual, das normas complementares e das demais normas da legislação brasileiras, quanto a confidencialidade e propriedade, bem como a localização dos dados armazenados, que devem observar as orientações a partir da sua classificação conforme os itens 5.3 e 5.4 da Instrução Normativa nº 14/IN01/DSIC/SCS/GSIPR, que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, bem como Instrução Normativa Nº 5, do Gabinete de Segurança Institucional da Presidência da República, publicada no Diário Oficial em 31/08/2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
8.9.3.2 A empresa contratada deverá assegurar que segue os padrões das normas nacionais e internacionais de segurança em computação na nuvem, através de certificações emitidas por estas entidades.
8.10 Gestão de incidentes de segurança da informação
8.10.1 A Assessoria de Informática deve estabelecer um processo para resposta a incidentes de forma a assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação sob responsabilidade da FAPERJ;
8.10.2 Todos os incidentes de segurança da informação ocorridos no âmbito da FAPERJ deverão ser imediatamente comunicados à Assessoria de Informática através do e-mail seguranca.assinf@faperj.br.
8.11 Orientações ao colaborador em geral
8.11.1 Uso aceitável dos ativos
8.11.1.1 Apenas os equipamentos e software disponibilizados e/ou homologados pela FAPERJ podem ser instalados e conectados à rede da FAPERJ;
8.11.1.2 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;
8.11.1.3 Os ativos da FAPERJ são destinados às atividades laborais, sendo vedado o uso para fins que não sejam do interesse da FAPERJ ou da administração pública;
8.11.1.4 Todo o resultado do trabalho efetuado com os ativos da FAPERJ é propriedade do Governo do Estado do Rio de Janeiro.
8.11.2 Cuidados cotidianos
8.11.2.1 Nenhuma informação classificada como secreta, ultrassecreta ou pessoal deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.
8.11.2.2 Na utilização de impressoras coletivas, o colaborador deverá recolher o documento impresso imediatamente.
8.11.2.3 Monitores deverão ser bloqueados sempre que não estiverem em uso. Para realizar este bloqueio de maneira rápida, basta pres-

sionar simultaneamente as teclas “Windows + L”.
8.11.3 Transferência de informações
8.11.3.1 Todo envio de documentos classificados em meio físico ou em meio digital deverá ser somente para os colaboradores que possuam direito a ter acesso às informações conforme definição do Controlador.
8.11.3.2 Quando utilizado meios digitais, a comunicação deverá ser, sempre que possível, criptografada. Quando não for possível a utilização de criptografia, esse desvio deverá ser informado e ser contabilizado no mapa de risco.
8.11.4 Acesso à Internet, redes sociais e comunicadores instantâneos
8.11.4.1 É permitida a utilização de Internet dentro da infraestrutura da FAPERJ por padrão. Essa utilização deve servir às funções profissionais e o interesse público, respeitando todas as normas complementares, bem como a legislação em vigor.
8.11.4.2 A utilização de redes sociais deve ser restrita às funções que necessitam destes acessos para atividades profissionais. Esses acessos deverão ser devidamente solicitados pela respectiva diretoria e autorizados pela Assessoria de Informática. Tais acessos são passíveis de auditoria.
8.11.4.3 A utilização de comunicadores instantâneos, (tais como WhatsApp, Messenger, Telegram, Signal entre outros) não são permitidos por padrão nos computadores do FAPERJ. A utilização é permitida para fins profissionais, com autorização da diretoria solicitante e avaliação de risco por parte da Assessoria de Informática.
8.11.4.4 Todos os acessos à Internet são registrados e as atividades podem ser monitoradas visando sempre a melhoria da segurança da informação bem como o cumprimento da legislação existente.
8.11.4.5 Não é permitido o envio ou recebimento (upload e download) de qualquer informação classificada da FAPERJ para redes sociais, comunicadores instantâneos ou qualquer site da Internet.
8.11.4.6 Poderá ser estabelecida norma complementar 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 da FAPERJ, tendo em vista que a Internet tem sido veículo de muitas ações prejudiciais às organizações, gerando danos à imagem, perdas de produtividade, danos aos sistemas e à organização, entre outras consequências.
8.11.5 Conscientização de Segurança da Informação
8.11.5.1 A Assessoria de Informática deverá desenvolver programas de capacitação específicos e campanhas, com apoio do Departamento de Recursos Humanos, para conscientização e divulgação deste Manual, bem como de suas normas complementares, visando a ampliação da cultura organizacional, quanto à importância da Segurança da Informação e seu valor estratégico para o FAPERJ.
8.11.6 Acesso ao correio e a ferramentas de colaboração
8.11.6.1 Poderão ser estabelecidas regras para utilização de correio eletrônico e ferramentas de colaboração providas pela FAPERJ.
8.11.7 Proteção contra códigos maliciosos
8.11.7.1 A Assessoria de Informática deverá estabelecer regras para a proteção dos recursos de Tecnologia da Informação da FAPERJ contra ação de códigos maliciosos e programas impróprios. Uma norma poderá elaborada para regulamentar a proteção contra código malicioso.
8.12 Gestão de riscos
8.12.1 Análise, avaliação e tratamento de riscos
8.12.2 A Assessoria de Informática deverá estabelecer regras para implementar um processo sistêmico de gerenciamento de riscos, que adote uma metodologia de gestão de riscos de Segurança da Informação, contemplando análise e avaliação, tratamento, aceitação e comunicação de riscos.
8.12.3 Gestão de continuidade de operações
8.12.4 A Assessoria de Informática, deverá estabelecer regras e princípios que regulamentem a gestão da continuidade do operações, através de um processo sistêmico para que se construa uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes críticos de segurança e salvaguardar as atividades e a reputação da FAPERJ. Uma norm poderá á ser elaborada para a gestão da continuidade de operações.
8.13 Monitoramento e auditoria
8.13.1 Deverá ser estabelecido, pela Assessoria de Informática, um programa de auditoria do processo de Gestão da Segurança da Informação, visando a verificar o cumprimento deste manual e se os controles implementados estão atendendo eficazmente a conformidade dos requisitos.
8.13.2 Deverá ser estabelecido, pela Assessoria de Informática, um programa de auditoria do processo de Gestão da Segurança da Informação, visando a verificar o cumprimento deste manual e se os controles implementados estão atendendo eficazmente a conformidade dos requisitos.
8.13.3 Deverá ser conduzida uma análise crítica dos resultados da auditoria, com o objetivo de determinar ações preventivas e corretivas para melhoria contínua do processo de Gestão de Segurança da Informação. Um plano de ação deve ser elaborado com base no relatório gerado pela auditoria.
8.13.4 O resultado de auditoria de Segurança da Informação deverá ser caracterizado como informação secreta, quando este puder comprometer a segurança dos processos da FAPERJ.
8.14 Gestão de Indicadores de Segurança
8.16.1 É responsabilidade da Assessoria de Informática elaborar e manter indicadores de Segurança da Informação que permitam avaliar o grau de maturidade da FAPERJ em relação à de exposição a 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 da FAPERJ.
8.15.1.1 A análise crítica deverá ser realizada em intervalos planejados ou qu.ando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia e demonstrar apoio e comprometimento com a Segurança da Informação.
9 DO DESCUMPRIMENTO
9.1 Nos casos em que houver descumprimento deste manual e/ou de suas normas complementares poderão ser adotadas medidas administrativas e/ou judicias cabíveis.
9.2 As ações abaixo descritas, dentre outras, consideram descumprimento:
9.2.1 Uso ilegal de software;
9.2.2 Introdução (intencional ou não) de vírus de informática;
9.2.3 Tentativas de acesso não autorizado a dados e sistemas;
9.2.4 Fotografar dados, compartilhamento de informações ou documentos da FAPERJ classificados como reservado, secreto, ultrassecreto;
9.2.5 A ausência da comunicação pelo colaborador de incidentes.
9.3 Em casos de incidentes de segurança da informação a Assessoria de Informática deverá ser imediatamente comunicada.
9.4 Detectada a autoria de alguma violação das normas previstas neste manual, antes de ser adotada alguma medida prevista no item.
9.5., a Comissão de Segurança da Informação poderá notificar o colaborador para a correção da conduta.
9.6 Toda violação ou desvio será investigado para a determinação das medidas necessárias, visando à correção da falha.
9.7 Em caso de dúvidas quantos aos princípios e responsabilidades descritas neste Manual, o colaborador deve entrar em contato com a Assessoria de Informática;
10 COMISSÃO DE SEGURANÇA DA INFORMAÇÃO
10.1 A Comissão de Segurança da Informação é composta por um representante da Assessoria de Informática, um da Assessoria Jurídica, um do Departamento de Recursos Humanos e dois colaboradores, bem como pelo Encarregado pelo Tratamento de Dados Pessoais do FAPERJ.
10.2 O representante da Assessoria de Informática presidirá a Comissão e que corresponde ao Gestor de Segurança da Informação. Que também será responsável pela mitigação operacional dos incidentes identificados.
10.3 Os representantes dos demais departamentos serão os respectivos chefes ou colaboradores por eles indicados.
10.4 A Comissão se reunirá ordinariamente a cada três meses e, extraordinariamente, a qualquer tempo, quando convocada.
10.5 Suas deliberações necessitam da presença de um quórum mínimo de 70% de seus membros.
10.6 As reuniões da Comissão terão como objetivo a avaliação e o aprimoramento deste manual e a análise das não conformidades de Segurança da Informação, além do encaminhamento das ações a serem adotadas para a correção das não conformidades.
10.7 Deverão constar no Portal da FAPERJ informações sobre a Comissão de Segurança da Informação, suas competências, seus membros e respectivos meios de contato, com destaque para o Gestor de Segurança da Informação, o responsável pelo tratamento e resposta a incidentes.
11 ATUALIZAÇÃO DESTE MANUAL DE SEGURANÇA
11.2 Deverá ser estabelecida a periodicidade mínima de um ano para a revisão deste Manual de Segurança da Informação da FAPERJ, bem como os demais documentos normativos gerados a partir dela, a fim de que não fiquem ultrapassados ou desatualizados.
11.2.1 Sempre que se faça necessário este manual poderá ser revisado independentemente da periodicidade aqui estabelecida.
11.2.2 As alterações feitas deverão ser registradas no campo adequando em Controle do Documento.
12. REFERÊNCIAS LEGAIS E NORMATIVAS(CONFORMIDADE)
12.1 Deverá ser disponibilizada pela Assessoria de Informática, para o conhecimento de todos, uma relação de normas e leis referentes à Segurança da Informação, que estará disponível na página da FAPERJ.
12.2 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 a FAPERJ, entre elas a NBR ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de segurança - Código de prática para controles de segurança da informação.
Apêndice A: Desvio de Procedimento de Segurança da Informação
Caso um colaborador ou um departamento da FAPERJ identifique impedimento ou não possa adotar um ou mais itens deste manual de Segurança da Informação da FAPERJ, deve solicitar justificadamente um Desvio de Segurança de Informações, utilizando o e-mail comissao.seguranca@faperj.br com autorização do chefe imediato;
A Assessoria de Informática deverá analisar, identificar qualitativa e quantitativamente os riscos inerentes ao Desvio de Procedimento de Segurança da Informação. A área solicitante deverá se responsabilizar em mitigar os riscos identificados, com apoio da Assessoria de Informática.
A Assessoria de Informática poderá vetar a solicitação caso identifique um risco grave à segurança da FAPERJ;
A Assessoria de Informática deverá manter os registros dos desvios de segurança da informação autorizados em controle próprio e revisar anualmente estas concessões, visando reduzir o nível de risco da FAPERJ.
Apêndice B: Análise de Risco de Segurança da Informação
É de responsabilidade da Assessoria de Informática manter um mapa de risco atualizado do FAPERJ que contempla os aspectos quantitativos e qualitativos, bem como as ações e projetos para mitigar cada categoria de risco identificado.
A Assessoria de Informática tem como, uma de suas atribuições, manter o nível de risco do FAPERJ o mais baixo possível em consonância com os objetivos estratégicos da autarquia.
Os riscos deverão ser identificados através de:
Auditorias de segurança;
Análises de Vulnerabilidades;
Testes de Invasão;
Desvio de Procedimento de Segurança da Informação;
Incidentes de Segurança;
e-mails enviados ao seguranca.assinf@faperj.br;
Consultoria externa;
Recomendações do CERT.BR, GSI entre outros órgãos governamentais;
A Diretoria deverá ser constantemente informada do nível de risco da FAPERJ pela Assessoria de Informática.
O processo de gestão de riscos em segurança da informação poderão ser detalhado em norma específica.

Id: 2500232

FUNDAÇÃO UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
DIRETORIA DE ADMINISTRAÇÃO FINANCEIRA

ATOS DO DIRETOR EM EXERCÍCIO
DE 04/08/2023

PORTARIA UERJ/DAF/SEI Nº 96/2023- DESIGNA o servidor **ANTONIO WILSON DE SOUSA**, matrícula 37509-7, como responsável pelo acompanhamento e fiscalização do Termo de Autorização de Uso do imóvel de propriedade da UERJ, situado na Rua Carolina Machado, nº 478-B, Madureira, Rio de Janeiro/RJ, em substituição à servidora Telma Ferreira Farias Teles Costa, matrícula nº 35523-0, a contar de 1º/08/2023. Processo SEI-260007/031004/2022.

PORTARIA UERJ/DAF/SEI Nº 97/2023- DESIGNA o servidor **CARLOS ALEXANDRE GOMES DOS SANTOS**, matrícula 37195-5, como responsável pelo acompanhamento e fiscalização do Termo de Autorização de Uso do imóvel de propriedade da UERJ, situado na Rua Barra do Rocha, nº 120 - Alameda dos Pavões, nº 137 - 2º andar, Pavuna, Rio de Janeiro/RJ, em substituição à servidora Telma Ferreira Farias Teles Costa, matrícula nº 35523-0, a contar de 1º/08/2023. Processo SEI-260007/005341/2022.

Id: 2500027

SECRETARIA DE ESTADO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO
FUNDAÇÃO UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO

ATO DO DIRETOR EM EXERCÍCIO

PORTARIA UERJ/DAF Nº 97 DE 04 DE AGOSTO DE 2023

DESIGNA DE SERVIDOR NA FORMA QUE MENCIONA.

O DIRETOR DE ADMINISTRAÇÃO FINANCEIRA, EM EXERCÍCIO, no uso das atribuições que lhe foram conferidas pela Portaria UERJ/Reitoria nº 633/2023, de 26/07/2023, diante do artigo 67, da Lei 8.666/1993 e conforme processo SEI-260007/005341/2022,

RESOLVE:

Art. 1º - DESIGNAR o servidor Carlos Alexandre Gomes dos Santos, matrícula 37195-5, ID 4460061-5, como responsável pelo acompanhamento e fiscalização do Termo de Autorização de Uso nº 003/2023, do imóvel de propriedade da UERJ, situado na situado na Rua Barra do Rocha, nº 120 - Alameda dos Pavões nº 137 -, 2º andar, Pavuna, Município do Rio de Janeiro/RJ, em substituição à servidora Telma Ferreira Farias Teles Costa, matrícula 35523-0, ID 4404476-3, a contar de 1º/08/2023.

Art. 2º - Esta Portaria entrará em vigor na data de sua publicação, revogadas as disposições em contrário.

Rio de Janeiro, 04 de agosto de 2023

ARY PEREIRA DE MIRANDA
Diretor de Administração Financeira em Exercício

Id: 2500025

FUNDAÇÃO UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO

DESPACHOS DO REITOR EM EXERCÍCIO
DE 03.08.2023

PROCESSO Nº SEI-260007/033071/2023 - HOMOLOGO o afastamento integral remunerado pelo Procad, por tratar-se de estudo de interesse desta Administração Pública, do Profº MARCOS ANDRÉ GLEIZER, matr. nº 30.884-1, para realizar estágio de pesquisa na Universidade de Paris 1, Phanteon-Sorbone, França, no período de 01/10/2023 a 31/01/2024, com ônus Capes PrInt.

PROCESSO Nº SEI-260007/036640/2023 - HOMOLOGO o afastamento integral remunerado pelo Procad da Profª VÂNIA MORALES SIERRA, matr. nº 34.630-4, para atuar como professor visitante na Universitè Saint Denis - Paris VIII, França, no período de 01/10/2023 a 31/12/2023, com ônus Capes PrInt.

PROCESSO Nº SEI-260007/032994/2023 - HOMOLOGO a licença sabática, por tratar-se de estudo de interesse desta Administração Pública, do Profº JOSÉ EDUARDO LEON SZWAKO, matr. nº 38.825-6, para realizar atividades de pesquisa na Escuela de Política y Gobierno, Universidad Nacional de San Martin, Buenos Aires, Argentina, no período de 01/10/2023 a 31/12/2023, com ônus Capes PrInt.

PROCESSO Nº SEI-260007/034015/2023 - HOMOLOGO a licença sabática, por tratar-se de estudo de interesse desta Administração Pública, do Profº MARCO ANTÔNIO DOS SANTOS CASA NOVA, Profº 31.798-2, para realizar atividades de pesquisa na Augustana Hochschule, Neuendettelsau, na Alemanha, no período de 01/10/2023 a 31/01/2024,com ônus Capes PrInt.

Id: 2500200

FUNDAÇÃO UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
SUPERINTENDÊNCIA DE GESTÃO DE PESSOAS

ATOS DA SUPERINTENDENTE
DE 08.08.2023

PORTARIA UERJ/SGP Nº SEI-1023/2023 - APOSENTA PAULO GOMES, matr. nº 04.911-4, ID Funcional 25448544, Professor Associado, nível 1, com 20 horas semanais, de acordo com o artigo 3º da Emenda Constitucional nº 47/2005, c/c artigo 2º da Emenda Constitucional Estadual nº 90/2021 - Processo nº SEI-260007/018799/2023.

PORTARIA UERJ/SGP Nº SEI-1024/2023 - APOSENTA SERGIO LUIZ SILVA, matr. nº 07.039-1, ID Funcional 25471538, Professor Associado, nível 1, com 40 horas semanais, pertencente ao regime de trabalho com Dedicação Exclusiva, nos termos da Lei 8.267/2018, de acordo com o artigo 3º da Emenda Constitucional nº 47/2005, c/c artigo 2º da Emenda Constitucional Estadual nº 90/2021 - Processo nº SEI-260007/049876/2022.

PORTARIA UERJ/SGP Nº SEI-1025/2023 - APOSENTA ANA CRISTINA DA MOTA CORDEIRO, matr. nº 34.200-6, ID Funcional 6080448, Professor Associado, nível 1, com 40 horas semanais, pertencente ao regime de trabalho com Dedicação Exclusiva, nos termos da Lei 8.267/2018, de acordo com o artigo 4º da Emenda Constitucional Estadual nº 90/2021 - Processo nº SEI-260007/006267/2023.

PORTARIA UERJ/SGP Nº SEI-1027/2023 - APOSENTA JULIO DE ALBUQUERQUE GONZALEZ, matr. nº 05.882-6, ID: Funcional 25456636, Professor Assistente, nível 4, com 40 horas semanais, pertencente ao regime de trabalho com Dedicação Exclusiva, nos termos da Lei 8.267/2018, de acordo com o artigo 3º da Emenda Constitucional nº 47/2005, c/c artigo 2º da Emenda Constitucional Estadual nº 90/2021 - Processo nº SEI-260007/007838/2023.

PORTARIA UERJ/SGP Nº SEI-1028/2023 - APOSENTA IVONETE FERREIRA DIOGO, matr. nº 33.615-6, ID: Funcional 25812971, Auxiliar Técnico Universitário IV/Serviços Operacionais, com padrão de vencimentos XII, com 40 horas semanais, de acordo com o artigo 6º da Emenda Constitucional nº 41/2003, c/c artigo 2º da Emenda Constitucional Estadual nº 90/2021 - Processo nº SEI-260007/008635/2023.

Id: 2500201

FUNDAÇÃO UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
SUPERINTENDÊNCIA DE GESTÃO DE PESSOAS

DESPACHOS DA SUPERINTENDENTE
DE 08.08.2023

PROCESSO Nº SEI-260007/031782/2023 - DETERMINO a inclusão de LUIZ RENATO MONTONE PERA, Professor Adjunto, matr. nº 41.339-3, no Regime de Dedicação Exclusiva, a contar de 04/08/2023, conforme a Lei Estadual nº 6.328/2012 e o art. 2º, § 6º, da Resolução CONSUN nº 05/2019. Esta publicação torna sem efeito a ocorrida no dia 04/08/2023, pág. 17, coluna 2.

PROCESSO Nº SEI-260007/040351/2023 - AUTORIZO o desligamento de ALESSANDRA DE PAULA SANTOS, matr. nº 38.901-5, a contar de 01/07/2019, considerando a solicitação da servidora docente, do Regime de Dedicação Exclusiva previsto na Lei Estadual nº 6.328/2012 e regulado pelo AEDA nº 052/REITORIA/2012 e pela Resolução CONSUN nº 5/2019.

PROCESSO Nº SEI-260007/047638/2022 - DETERMINO a inclusão de DANIELA DE BARROS MUCCI, Professor Adjunto, matr. nº 41.287-4, ID: 51357968, vínculo 1, no Regime de Dedicação Exclusiva, a contar de 09/03/2023, conforme Lei Estadual nº 6.328/2012 e Art. 2º, § 6º da Resolução do CONSUN nº 05/2019. Esta publicação torna sem efeito a ocorrida no dia 22/03/2023, pág. 40, col. 01.

PROCESSO Nº SEI-260007/033013/2023 - DETERMINO a inclusão de PATRÍCIA ALVES REIS, Professor Adjunto, matr. nº 41.772-5, no Regime de Dedicação Exclusiva previsto na Lei Estadual nº 6.328/2012, regulado por meio da Resolução CONSUN nº 05/2019.

Id: 2500202

FUNDAÇÃO UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
SUPERINTENDÊNCIA DE GESTÃO DE PESSOAS
DEPARTAMENTO DE GESTÃO E ACOMPANHAMENTO FUNCIONAL

DESPACHOS DO DIRETOR
DE 08.08.2023

DEFIRO o Abono de Permanência dos servidores uma vez que os interessados atendem aos requisitos constitucionais:

PROCESSO Nº SEI-260007/030760/2023 - ELIZABETE MARTINS DA ROCHA, matr. nº 33.157-9, ID: 32312970, com validade a contar de 12/07/2023.

PROCESSO Nº SEI-260007/018488/2023 - JUSSARA MENDONCA DOS SANTOS, matr. nº 31.653-9, ID: 32301456, com validade a contar de 27/01/2022.

PROCESSO Nº SEI-260007/013693/2023- CELSO ROBERTO DA SILVA ARAUJO, matr. nº 26.799-7, ID: 25736183, com validade a contar de 20/10/2021.

PROCESSO Nº SEI-260007/015816/2023 - TEREZA CRISTINA BENTO DE FREITAS, matr. nº 35.940-6, ID: 31384978, com validade a contar de 06/03/2023.

PROCESSO Nº SEI-260007/015633/2023 - MARCO ANTONIO SANTORO SALVADOR, matr. nº 34.738-5, ID: 37391550, com validade a contar de 01/01/2022.

PROCESSO Nº SEI-260007/011644/2023 - ANA PAULA MENEZES PEREIRA, matr. nº 32.087-9, ID: 25273876, com validade a contar de 07/07/2023.

PROCESSO Nº SEI-260007/052171/2022 - DALMO DELPHIM RIBEIRO, matr. nº 06.776-9, ID: 25625470, com validade a contar de 02/07/2023.

PROCESSO Nº SEI-260007/021094/2023 - PAULO ROBERTO BENCHIMOL BARBOSA, matr. nº 27.896-0, ID: 3231707-7, com validade a contar de 26/07/2023.

PROCESSO Nº SEI-260007/035975/2023 - MARIA CRISTINA VIEGAS CAMPOS DA RESSURREIÇÃO, matr. nº 33.620-6, ID: 6078036, com validade a contar de 23/12/2022.

Id: 2500203