	Título	Código
	GERENCIAMENTO DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO DE PRESTADORES DE SERVIÇOS	EMAP-PC-96
		Versão
		3
	Data	11/10/2021

Elaborado Por	Aprovado por
Ruan Louzeiro Santos	Thiago Drummond

INDICE

1.0 OBJETIVO.....	1
2.0 DOCUMENTOS DE REFERÊNCIA	1
3.0 DEFINIÇÕES	2
4.0 RESPONSABILIDADES.....	3
5.0 DESCRIÇÃO DO PROCEDIMENTO	3
6.0 ANEXOS.....	6
7.0 REGISTROS.....	6
8.0 HISTÓRICO DE REVISÃO	7

1.0 OBJETIVO

Este procedimento é parte da Política de Segurança da Informação da EMAP e visa orientar a empresa sobre como gerenciar requisitos de segurança da informação de prestadores de serviços da EMAP.

2.0 DOCUMENTOS DE REFERÊNCIA

- Lei Nº 13.709, de 14 De agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)
- Decreto nº 9.637 de 26 e dezembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.
- Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2021 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

- Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021 - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
- Instrução Normativa GSI nº 1, de 4 de abril de 2019 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação – Requisitos
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação
- Ato Declaratório Executivo Coana / Cotec nº 2, de 26 de setembro de 2003 - Especifica os requisitos técnicos, formais e prazos para implantação de sistema informatizado de controle aduaneiro domiciliar e de recintos alfandegados ou autorizados a operar com mercadorias sob controle aduaneiro
- ISPS Code - CÓDIGO INTERNACIONAL PARA A PROTEÇÃO DE NAVIOS E INSTALAÇÕES PORTUÁRIAS

3.0 DEFINIÇÕES

- **SEGURANÇA DA INFORMAÇÃO:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações.
- **EMPREGADOS:** todo aquele que por força de lei, faz parte do quadro de funcionários efetivos da EMAP, sendo em regime permanente ou temporário.
- **SETORES:** todas as áreas da estrutura organizacional da EMAP.
- **PRESTADORES DE SERVIÇOS:** todo e qualquer funcionário de empresa contratada pela EMAP que utiliza um ou mais ativos de informação de propriedade da EMAP, ou sob sua responsabilidade, para realização de suas atividades.
- **GESTOR DE PRESTADORES DE SERVIÇOS:** Empregado da EMAP responsável por supervisionar as atividades realizadas pelos prestadores de serviços em seu setor.
- **FISCAL DE CONTRATO:** Empregado da EMAP responsável por fiscalizar os contratos que envolvem fornecimento de prestadores de serviços e gerenciar toda a documentação e dados pessoais desses trabalhadores.

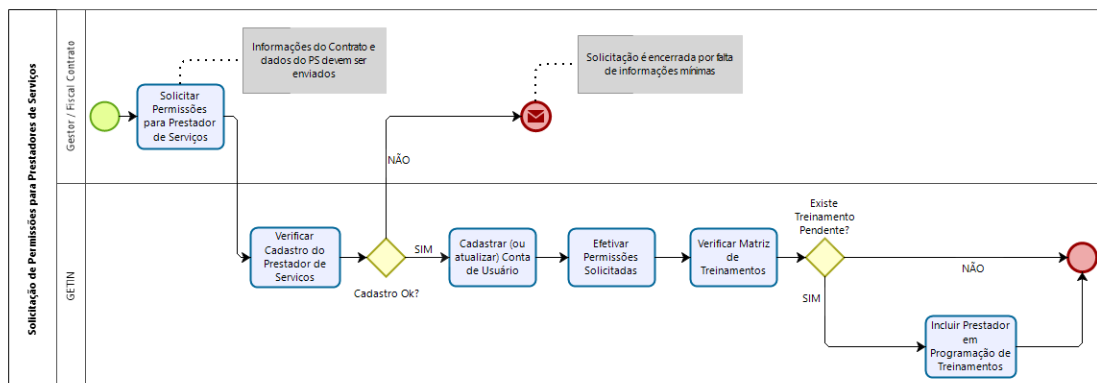
- **TREINAMENTO INTERNO:** Treinamento desenvolvido por pessoal da própria empresa, dentro ou fora do local de trabalho.
- **AVALIAÇÃO DE EFICÁCIA:** forma de avaliar a eficácia do treinamento.

4.0 RESPONSABILIDADES

- É responsabilidade de todos os empregados e prestadores de serviços proteger as informações e relatar qualquer situação que represente desvio ou violação de segurança das mesmas, bem como atender às recomendações pertinentes constantes na Política de Segurança da Informação da EMAP.
- É responsabilidade dos fiscais de contratos (ou gestores dos prestadores de serviços da EMAP) informar à GETIN todas informações dos prestadores de serviços necessárias para análise dos requisitos de segurança da informação.
- É responsabilidade dos prestadores de serviços realizar todos os treinamentos relacionados à segurança da informação indicados pela GETIN.
- É responsabilidade da GETIN avaliar todos os requisitos de segurança da informação dos prestadores de serviços, gerenciar as permissões das suas contas de usuários e necessidades de treinamentos em procedimentos relacionados ao escopo da segurança da informação.

5.0 DESCRIÇÃO DO PROCEDIMENTO

Esse procedimento é aplicável aos fiscais de contratos (e gestores dos setores da empresa) e empregados da GETIN.



5.1 SOLICITAR PERMISSÕES

O fiscal do contrato (ou o gestor do setor responsável pelo contrato) deverá abrir um chamado junto à Central de Serviços da GETIN solicitando permissões de acesso para o prestador de serviços vinculado ao contrato sob sua fiscalização / gestão.

Todas as informações desse prestador de serviços listadas abaixo deverão ser informadas na solicitação.

- Nome completo
- Sexo
- CPF
- Empresa contratada
- Número do Contrato
- Setor (operacional ou administrativo)
- Função a desempenhar
- Lotação
- Gerência Responsável

Mesmo que um prestador de serviços já possua uma conta de usuário e esteja apenas mudando de função, o chamado com as informações necessárias à análise deverá ser enviado, obrigatoriamente.

É de responsabilidade do fiscal do contrato manter cópia de documentos e informações atualizadas dos prestadores de serviços, conforme requisitos do Termo de Referência que originou o contrato de prestação de serviços.

5.2 VERIFICAR CADASTRO

A GETIN deverá manter um cadastro dos prestadores de serviços com as informações enviadas pelos fiscais de contrato / gestores com objetivo de gerenciar os treinamentos de segurança da informação indicados. Para isso, deverá utilizar o do REGISTRO ANUAL DE TREINAMENTOS - ANEXO I (EMAP-RSGSI-20)

Ao receber as informações do prestador de serviços, as mesmas deverão ser verificadas e o cadastro de prestadores de serviços atualizado.

A informação de data de cadastro deve ser preenchida sempre que um novo prestador de serviços for incluído. Caso seja apenas atualizado dados, essa data NÃO deverá ser alterada.

Caso estejam faltando informações necessárias à análise, o chamado será encerrado e o fiscal do contrato / gestor poderá abrir um novo chamado quando estiver de posse de todas as informações necessárias.

Se as informações estiverem corretas, o cadastro da conta de usuário do prestador de serviços será realizado (ou atualizado, caso já exista).

5.3 EFETIVAR PERMISSÕES SOLICITADAS

Para que não haja impacto nas atividades operacionais e administrativas que dependem desses prestadores de serviços, o prestador de serviços com as informações corretas terá as permissões em sua conta de acesso concedidas, mesmo que exista algum treinamento indicado pela GETIN pendente.

5.4 VERIFICAR MATRIZ DE TREINAMENTOS

A GETIN também deve gerenciar a necessidade e realização de treinamentos em procedimentos relacionados ao escopo da segurança da informação pelos prestadores de serviços. Para isso, deve elaborar um PLANO ANUAL DE TREINAMENTOS - ANEXO II (EMAP-RSGSI-19).

O controle da realização dos treinamentos dos prestadores de serviços será feito através do REGISTRO ANUAL DE TREINAMENTOS.

Deve-se consultar o Registro Anual de Treinamentos para verificar se o prestador de serviços já realizou todos os treinamentos necessários ao desempenho da função. Caso haja necessidade de treinamentos, a GETIN deverá incluir o registro do treinamento observando a coluna NOVO / RECICAGEM ANUAL, informando NOVO se é um novo prestador de serviços que está realizando os treinamentos pela primeira vez ou RECICAGEM ANUAL se é um treinamento anual de reciclagem.

Quando um novo registro é informado, a DATA MÁXIMA PARA REALIZAÇÃO do treinamento é calculada automaticamente, sendo até 45 (quarenta e cinco) dias a partir da data de cadastro, se for um novo prestador de serviços ou a data fim do treinamento informada no plano anual de treinamentos. Nos dois casos o STATUS do treinamento é criado como PENDENTE.

Além desse estado, o treinamento pode estar ATRASADO, caso ultrapasse a data máxima para realização, ou CONCLUÍDO, quando o treinamento já foi realizado.

Caso o prestador de serviços não realize o treinamento no prazo estabelecido, a conta de usuário dele será bloqueada pela GETIN, ficando impedido de utilizar os sistemas de informação e serviços de TI, e o gestor notificado.

5.5 REALIZAÇÃO DE TREINAMENTOS

Após realização dos treinamentos, a GETIN deverá atualizar o Registro Anual de Treinamentos informando data de conclusão. A lista de frequência do treinamento

também deverá ser guardada (em meio digital) de modo a evidenciar a participação no treinamento.

A GETIN também é responsável por verificar a eficácia dos treinamentos. A partir de sessenta dias após a realização do treinamento e por um prazo de dez meses (ou nova realização do mesmo treinamento), o treinamento será considerado EFICAZ, se não ocorrer NENHUM incidente de segurança da informação provocado pelo prestador de serviços (ou relacionado a ele) e NÃO EFICAZ, se acontecer pelo menos um incidente.

Em caso de avaliação não eficaz, o treinamento deverá ser repetido. Além disso, o fiscal do contrato (ou o gestor do setor responsável pelo contrato) poderá analisar a causa e traçar plano de ação.

O controle das Avaliações de Eficácia será feito na planilha de Registro Anual de Treinamento, onde se evidencia a data da avaliação e o percentual de eficácia do treinamento.

6.0 ANEXOS

- [Anexo I: EMAP-RSGSI-20 REGISTRO ANUAL DE TREINAMENTOS](#)
- [Anexo II: EMAP-RSGSI-19 PLANO ANUAL DE TREINAMENTOS](#)

7.0 REGISTROS

Identificação	Local do Arquivo	Armazenamento	Proteção	Disposição e Recuperação	Tempo de Retenção		Descarte
					Tempo	Base legal	
EMAP-RSGSI-19 PLANO ANUAL DE TREINAMENTOS	Servidor de Arquivos	\\arquivos\GEST AO_SGSI\Presta dores\	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica por ano	5 anos	Não há	Deletar
EMAP-RSGSI-20 REGISTRO ANUAL DE TREINAMENTOS	Servidor de Arquivos	\\arquivos\GEST AO_SGSI\Presta dores\	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica por ano	5 anos	Não há	Deletar

Identificação	Local do Arquivo	Armazenamento	Proteção	Disposição e Recuperação	Tempo de Retenção		Descarte
					Tempo	Base legal	
DOSSIÊ PRESTADORES DE SERVIÇOS DA GETIN	Servidor de Arquivos	\\arquivos\GESTAO_SGSI\Presta dores\	Usuário e senha. Acesso restrito à GETIN	Ordem Alfabética	5 anos	Não há	Deletar
CHAMADO COM DE INCLUSÃO / ALTERAÇÃO DE PERMISSÕES DOS PRESTADORES DE SERVIÇOS	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem Cronológica	Permanente	Não há	Não há

8.0 HISTÓRICO DE REVISÃO

Versão	Data	Item	Revisões
0	25/11/2020	3	Inclusão das definições de Gestor de Prestador de Serviços e Fiscal de Contrato
0	25/11/2020	7	Inclusão de novo registro referente ao CHAMADO COM DE INCLUSÃO / ALTERAÇÃO DE PERMISSÕES DOS PRESTADORES DE SERVIÇOS
1	21/12/2020	7	Revisão de tempo de retenção e disposição dos registros
2	11/10/2021	2	Revisão dos documentos de referência
2	11/10/2021	5.2	Inclusão de observação a respeito da <i>Data de Cadastro</i> .
2	11/10/2021	5.4	Inclusão de informações a respeito do controle da realização dos treinamentos e bloqueio de usuários em caso de não realização de treinamento no prazo estipulado.
2	11/10/2021	6.0	Alteração do Anexo I Plano anual de treinamento