1. OBJETIVO

Regula os requisitos técnicos e obrigatórios de segurança e confidencialidade para o acesso, tratamento, armazenamento e divulgação de dados pessoais e sensíveis dos colaboradores, fornecedores e demais partes interessadas.

2. APLICAÇÃO

É aplicável obrigatoriamente a qualquer operação de tratamento de dados pessoais que tenham sido coletados, ou de alguma forma, tratados pela Engeman, podendo estes dados serem coletados em meio físico ou digital.

3. DOCUMENTOS RELACIONADOS

PG.SG.04- Controle de Não Conformidade e Ações Corretivas;
IT- 171- Gerenciamento de Riscos;
IT-172- Tratamento e Investigação de Denúncias e Reclamações;
FORM. 106 - Relatório de Ação Corretiva – RAC

4. DEFINIÇÃO

DADOS PESSOAIS: Quaisquer informações que possam levar a identificação de uma pessoa natural, de maneira direta ou indireta (identificada ou identificável);

DADOS SENSÍVEIS: São aqueles que, se expostos ou compartilhados, podem causar impacto para a vida pessoal e/ou profissional;

INFORMAÇÃO: Consiste em qualquer dado pessoal em qualquer meio, incluindo mas não se limitando à base de dados, documento(s) físico(s), eletrônico(s), magnético(s), digital(is) finalizado(s) ou em desenvolvimento, recurso(s) de informática, informação(es) comercial(is), financeira(s), estatística(s), jurídica(s), técnica(s), relacionada(s) ao(s) negócio(s) ou ao(s) empregado(s) bem como as informação(ões) relacionada(s) à segurança de tecnologia da informação: domínios, mídias, processos, políticas, procedimentos, medidas, recursos de segurança e, em geral, qualquer conhecimento ou comunicação transmitida verbalmente;

INFORMAÇÃO SENSÍVEL: Consiste em informação(es) de Dados Pessoais referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, relativa à saúde ou à vida sexual, dado genético ou biométrico, bem como àquelas Informações que, ainda que sejam públicas, foram classificadas como sendo de uso interno;

TITULAR: Pessoa Física, a quem se referem os dados pessoais;

CONTROLADOR: Pessoa Física ou Jurídica a quem compete as decisões em relação a finalidade e o tratamento de dados pessoais. O controlador deve orientar e monitorar os procedimentos e condições para o tratamento por parte do operador;

OPERADOR: Pessoa Física ou Jurídica que realiza o tratamento de dados pessoais sob às ordens do Controlador;

ENCARREGADO DE DADOS / DPO: Pessoa Física indicada pelo Controlador para ser o canal de comunicação entre o Controlador, os Titulares e a ANPD (ou órgão que a substituir);

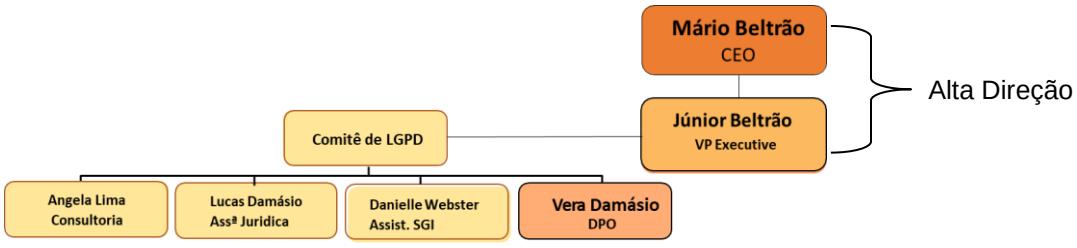
CONFIDENCIALIDADE: Todas as informações, sensíveis ou não, disponibilizadas pela ENGEMAN, acessada(s) ou encontrada(s) nas instalações da Engeman, deve(m) ser mantida(s) no mais absoluto e estrito sigilo, mesmo após o término da relação entre as partes, tendo este sigilo como validade o período de 5 (cinco) anos contados a partir do término da relação contratual. Nenhuma informação(es), sensível(is) ou não, poderá(rão) ser extraídas ou transmitidas de qualquer forma ou meio (eletrônico, mecânico, fotocópia, gravação ou outro meio) das instalações da Engeman, salvo se houver autorização expressa para praticá-los, de modo que se reconhece o dever de confidencialidade das informações e as obrigações relacionadas ao tratamento da(s) informação(es), sensível(is) ou não.

5. SISTEMÁTICA

Os principais responsáveis no tratamento de dados pessoais, de acordo com a LGPD são: o titular, o controlador, o operador e o encarregado. De acordo com a LGPD, os dados devem ser tratados das seguintes formas:

- Mediante o consentimento do titular;
- Para cumprimento de obrigações legais;
- Quando necessário para a execução de contrato ou de procedimentos contratuais preliminares;
- Para o exercício regular de direito em processo judicial, administrativo ou arbitral;
- Para atendimento de interesses legítimos do Controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos dados pessoais;
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde, serviços de saúde ou por entidades/autoridades sanitárias;
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

5.1 ORGANOGRAMA DO COMITÊ



5.2 ATRIBUIÇÕES DO COMITÊ

SGI	Elaborar, revisar e melhorar a documentação necessária para a adequação à LGPD; Conscientizar e promover o cumprimento do Código de Conduta e Ética; Promover a identificação, análise e definição dos procedimentos de controle da LGPD; Incentivar o uso do canal de denúncia; Compartilhar exemplos de boa conduta; Participa da elaboração do Relatório de Impacto Dados (RIPD); Receber, analisar e encaminhar qualquer denúncia, irregularidades e infrações relacionadas a LGPD.
Consultoria de Gestão	Orientar na estruturação, implantação, manutenção e melhoria da LGPD; Participar da identificação, análise e definição dos procedimentos de controle da LGPD; Participar da análise e definição de ação para ocorrências do canal de denúncias relacionadas a LGPD; Participar do monitoramento, avaliação e melhoria da gestão de LGPD; Apoiar a análise de riscos e definição do planejamento do sistema de LGPD; Apoiar na elaboração do Relatório de Impacto de Impacto de Dados - RIPD
Assessoria Jurídica	Apoiar na análise de documentos e práticas da LGPD; Apoiar juridicamente a investigação preliminar quando da possível ocorrência de atos lesivos ou descumprimento de qualquer requisito do Sistema de Gestão e da LGPD.
Encarregado de Dados	Representar a empresa junto à ANPD e titulares de dados; Capacitar profissionais que lidam com dados pessoais; Garantir o cumprimento das políticas de segurança da informação e proteção de dados; Monitorar atividades de tratamento de dados e conformidade com a LGPD; Elaboração do Relatório de Impacto Dados (RIPD); Atuar na redução de riscos relacionados à privacidade; Acompanhar o cumprimento, pelos fornecedores, das cláusulas contratuais de segurança da informação.

A função do comitê é avaliada continuamente, na ocasião das reuniões de análise crítica, a fim de garantir o gerenciamento e controle dos riscos

Os Integrantes do Comitê afirmam seu comprometimento através do Termo de confidencialidade.

5.2.1 MANDATO DO COMITÊ

Devido a dimensão da Engeman, não é necessário definir tempo para o mandato dos membros do comitê de LGPD. Após a instalação, os membros poderão ser destituídos do cargo nos casos abaixo:

- Não observância das diretrizes deste programa;
- Comportamento incompatível às atribuições da função;
- Encerramento de vínculo com a Engeman, empregatício ou comercial, no caso de membro externo;
- Renúncia formal do membro.

Neste caso, um novo membro será designado pela Diretoria e deverá ser aprovado pelo Comitê em reunião extraordinária.

5.3 RECURSOS MATERIAIS

5.3.1 CANAL OUVIDORIA

O comitê tem a disposição um canal para recebimento das denúncias e feedback aos denunciantes:

a) 0800 008 3050
b) http://www.contatoconfidencial.com.br/engeman

5.3.2 INFRAESTRUTURA

O comitê de LGPD utiliza os mesmos meios disponibilizados para o sistema de gestão integrado da Engeman: computadores, salas de reunião, linha telefônica e internet.

É expressamente proibido utilizar o tratamento para fins discriminatórios ilícitos, abusivos ou que comprometa a liberdade, privacidade ou o livre desenvolvimento da personalidade da pessoa natural, sendo passivo de medidas administrativas, conforme o Programa de Integridade.

O operador deve informar ao titular, antes de efetuar o tratamento, as finalidades da ação, os dados recolhidos, e a finalidade dos dados recebidos e a forma de proteção e acesso dos mesmos.

O Encarregado de dados deverá ser acionado sempre que houver necessidade para esclarecimento de dúvidas ou sobre suposto desvio no tratamento dos dados. Seu trabalho, basicamente, é garantir que a empresa esteja operando dentro dos requisitos legais e de modo a atender os princípios impostos pela lei e em conformidade com a LGPD.

O titular dos dados, caso necessite, terá acesso ao encarregado de dados através do e-mail: encarregadodedados@engeman.net. Poderá utilizá-lo para obtenção de informações relativos aos seus dados, assim como fazer sugestões e reclamações, em consonância com artigo 41 da Lei n° 13.709/2018.

Qualquer parte interessada interna ou externa que identificar possível descumprimento da LGDP, poderá realizar o registro através dos canais de ouvidoria da Engeman e /ou do Encarregado de dados.

Ao receber a reclamação, o encarregado de dados deverá proceder com as tratativas e devidas medidas cabíveis para a resolução do descumprimento da LGPD.

O encarregado deverá emitir o RAC- Relatório de Ação Corretiva (FORM.106), conforme PG.SG.04 e iniciar a investigação conforme IT-172- Tratamento e Investigação de Denúncias e Reclamações, solicitar documentação aos setores envolvidos e tomar as ações corretivas definidas no RAC.

Caso um titular revogue seu consentimento, o encarregado de dados, ao receber a solicitação, tomará as providências para resolver a demanda, podendo delegar a tarefa a um colaborador específico, e se certificar que ela foi feita, prestando todos os esclarecimentos ao titular ou autoridade nacional que tenha solicitado alguma informação.

O prazo para resposta às solicitações dos titulares é de dez dias úteis após o recebimento da solicitação.

5.4 Durante o armazenamento de Dados Pessoais, a Engeman respeitará, no mínimo, os seguintes padrões de segurança:

(a) Os acessos aos Dados Pessoais deverão ser revisados periodicamente;

(b) O tratamento dos DADOS deverão ser monitorados por meio de gerenciamento detalhado dos acessos, contendo a identidade do colaborador ou responsável pelo acesso designado pela Engeman;

(c) Utilização de meios para proteção dos dados em armazenado;

(d) Manter o gerenciamento dos Dados Pessoais atualizados, sejam eles processados, transmitidos pelos sistemas ou armazenados.

5.5 A Engeman manterá o registro das seguintes informações:

a) Papéis e responsabilidades definidos e atribuídos. Esse registro deverá ser revisado e atualizado sempre que houver mudança na rotina de trabalho, ou no surgimento de um novo cargo;
a) Registro dos compartilhamentos e/ou transferências a terceiros, incluindo toda a documentação envolvida (Ex: Portal, plano de saúde etc);
b) Registro do consentimento para tratamento dos Dados de forma confidencial e integra;
c) Levantamento dos Dados Pessoais tratados e as respectivas medidas de controle;
d) Capacidade de restaurar a disponibilidade e o acesso aos DADOS de forma rápida em caso de incidente físico ou técnico; e
e) Existência de processo de verificação contínua de medidas técnicas e organizacionais relativas à segurança do TRATAMENTO de DADOS;

A Engeman manterá sigilo em relação aos DADOS que não forem manifestamente públicos, ao TRATAMENTO dos dados pessoais e dos dados pessoais sensíveis, bem como em relação ao resultado do tratamento em virtude dos contratos firmados, garantindo que todas as pessoas autorizadas a realizarem tais atividades estejam comprometidas ao dever de confidencialidade, e serão devidamente instruídas e capacitadas para o referido tratamento.

5.6 DIREITOS DO TITULAR

O Titular dos dados poderá requerer seus direitos, mediante a solicitações através dos canais de comunicação informados no item 6, desde que não haja a necessidade de manutenção destes dados em virtude de obrigação legal ou regulatória (emissão de documentos trabalhistas por exemplo).

A Engeman garante a realização de avaliações de risco e impacto, bem como o exercício dos seguintes direitos por parte dos TITULARES:

(a) Confirmação da existência de TRATAMENTO;
(b) Acesso aos DADOS;
(c) Correção de DADOS incompletos, inexatos ou desatualizados;

(d) Anonimização, bloqueio ou eliminação de DADOS desnecessários, excessivos ou tratados em desconformidade com a lei;
(e) Portabilidade dos DADOS;
(f) Eliminação dos DADOS tratados com ou sem o consentimento;
(g)Informação sobre entidades públicas e privadas com as quais foi realizado uso compartilhado de DADOS;
(h) Informação sobre a possibilidade de não fornecimento do consentimento e sobre as consequências da negativa;
(i) Revogação do consentimento.

Caso algum TITULAR solicite o exercício de seus direitos descritos acima, e o TRATAMENTO dos DADOS impactar na execução do Contrato entre a Engeman, deverá a parte requerida comunicar tal fato de forma imediata (e, no limite, no dia útil seguinte).

5.7 Incidente

Em caso de incidente, como por exemplo, de acesso indevido, não autorizado, de vazamento ou perda de dados, decorrente de TRATAMENTO, independentemente do motivo que o tenha ocasionado, deverá a Engeman, ou um terceiro, denominado Controlador responsável pelo referido TRATAMENTO, enviar comunicação por escrito para o controlador, certificando-se do recebimento, imediatamente a partir da ciência do incidente, contendo, no mínimo, as seguintes informações:

(i) data e hora do incidente;
(ii) data e hora da ciência pelo CONTROLADOR responsável;
(iii) relação dos tipos de DADOS afetados pelo incidente;
(iv) número de TITULARES afetados;
(v) relação de TITULARES afetados pelo vazamento;
(vi) dados de contato do ENCARREGADO DE DADOS (DPO) ou outra pessoa junto à qual seja possível obter maiores informações sobre o ocorrido;
(vii) descrição das possíveis consequências e riscos do incidente; e
(viii) indicação de medidas que estiverem sendo tomadas para reparar o dano e evitar novos incidentes.

O tratamento do incidente deverá seguir conforme descrito na IT 172- Tratamento e Investigação de Denúncia e reclamação e o registro deverá ser realizado através do RAC- Relatório de Ação Corretiva- FORM. 106, considerando as seguintes medidas:

1. Comunicação à ANPD e ao titular;
2. Avaliação dos riscos e impactos do incidente;
3. Medidas mitigadoras a serem adotadas.

A Engeman, controladora, declara que manterá, durante toda a execução do contrato, no mínimo os padrões de segurança, de privacidade e de proteção de DADOS, aptas a proteger os DADOS pessoais de qualquer forma de tratamento inadequado ou ilícito. Bem como, os demais CONTROLADORES envolvidos também asseguram que utilizam e continuarão utilizando as Melhores Práticas do Mercado em relação à segurança das informações que circulam em seus ambientes físicos e virtuais.

A Engeman assegura que ao término da relação entre CONTROLADORES, será solicitado mediante eventual solicitação do TITULAR, para eliminar, corrigir e/ou bloquear o acesso aos DADOS, em caráter definitivo ou não, que tiverem sido tratados em decorrência do contrato, estendendo-se a eventuais cópias, salvo atendimento a uma base legal que permita a manutenção desses DADOS ou em cumprimento a uma Lei pertinente.

5.8 INFORMAÇÃO

1. Confirmação do tratamento de Dados Pessoais e solicitação de informações sobre a utilização de informações pessoais;

2. Acesso às informações pessoais tratadas pela Engeman;

3. Correção ou atualização de informações pessoais tratadas pela Engeman;

4. Exclusão de Dados Pessoais disponibilizados com base no consentimento, ou coletados em desacordo com as finalidades informadas;

5. Oposição ao processamento de informações pessoais.

5.9.1 RECLAMAÇÃO / PEDIDO DE REVOGAÇÃO

O Titular dos Dados Pessoais poderá realizar uma reclamação relação sobre o uso indevido de algum dado ou solicitar a eliminação dos dados fornecidos a Engeman, em caráter formal, com base nas seguintes situações:

1- Desde que, os dados tenham sido fornecidos de forma irregular e/ou desnecessária para finalidade que justifique a realização do tratamento; ou
2- Quando os Dados tenham sidos fornecidos de forma excessiva em relação ao necessário para alcance da finalidade ou tenham sido tratados em desconformidade com a LGPD;

3- Quando identificado tratamento em desconformidade, ou seja, caso não estejam sendo tratados para finalidades específicas ou o tratamento não seja justificável por nenhuma base legal.

6. COMUNICAÇÃO

Para o exercício de seus direitos, o Titular deverá enviar sua solicitação através do canal de ouvidoria ou através do e-mail: encarregadodedados@engeman.net.

O Prazo para resposta é de dez dias úteis após o recebimento da solicitação. É vedada a realização de solicitações diretamente pelo TITULAR, quando menor de idade, de modo que serão tidas como não formuladas as solicitações enviadas em desconformidade com o previsto neste instrumento.

7. MAPEAMENTO DOS DADOS PESSOAIS

Através do FORM.424 - Gestão De Tratamento De Dados – LGPD, estão identificados os dados pessoais que são tratados por cada setor, indicando o documento que contém os dados pessoais; a finalidade; o compartilhamento; o tempo de retenção; o descarte e as medidas de controle.

7.1 – Entradas para o Gestão de Tratamento de Dados

7.1.1 O mapeamento dos dados deve ser realizado na ocorrência das situações abaixo:

- Definição dos processos;
- Início de novos contratos;

7.1.2 Deverá ser analisado criticamente a Gestão de Tratamento de Dados, na ocorrência das situações abaixo:

- Sempre que houver alterações de processos;
- Após a ocorrência;
- Revisão anual das estratégias / plano operacional;
- Reclamações / Denúncias consideradas críticas.

7.2 Método para Identificação

A metodologia utilizada para identificação dos riscos é preconizada da seguinte forma:

1º Passo – Identificação dos Dados e Documentos utilizados no processo:

A identificação dos riscos deve iniciar com a elaboração da relação dos Dados Pessoais a serem tratados. Para cada processo deve ser preenchido uma planilha conforme modelo FORM.424 - Gestão De Tratamento De Dados – LGPD.

2º Passo – Finalidade:

Para cada tratamento dos Dados, deve ser identificado a finalidade para o acesso ao dado.

3º Passo – Meio de armazenamento:

Para cada documento/ Dado Pessoal, deverá ser sinalizado o meio no qual são armazenados, se físicos ou eletrônicos, ou os dois. Deverá ser indicado o tempo para retenção dos dados e a forma de descarte dos mesmos.

4º Passo – Controle:

Nesta etapa, deverá ser indicado se há compartilhamento de dados, seja para conhecimento ou para diligenciamento.

5º Passo – Riscos:

Para cada dado Pessoal / Documento em análise, deverá ser identificado os riscos associados e listados na coluna correspondente, podendo ser identificado vários riscos.

7.3 Análise dos Riscos

Os riscos identificados, devem ser caracterizados quanto ao nível, conforme definições abaixo:

7.3.1 PESO:

Para a definição do Peso do risco, deve ser levado em conta a sua abrangência e reversibilidade, podendo ser pontuada conforme critério dos quadros abaixo:

NÍVEL	CRITÉRIO	EXEMPLO	PONTUAÇÃO
BAIXO	Risco de impacto facilmente reversível	Vazamento de dados internamente	**1**
MÉDIO	Risco de impacto moderado, mas possível de ser revertido	Vazamento de informações como: telefone ou endereço	**2**
ALTO	Risco de impacto irreversível	Vazamento externo de dados bancários de um funcionário	**3**

7.3.2 CRITICIDADE:

No quadro a seguir são apresentados os critérios para pontuação da criticidade, associada ao Riscos:

CRITICIDADE	CRITÉRIO	PONTUAÇÃO
BAIXO	Risco de magnitude desprezível/restrito ao local de ocorrência/totalmente reversível com ações imediatas; Uma Não Conformidade pontual ou potencial ou Causas com efeitos benéficos	**1**
MÉDIO	Risco de magnitude considerável/reversível com ações corretivas; Não Conformidade sistêmica	**2**
ALTO	Risco de grande magnitude/de grande extensão/ consequências muito graves, mesmo com ações corretivas. Não conformidade sistêmica que compromete o cumprimento ou atendimento da LGPD	**3**

As pontuações referentes ao Peso e a Criticidade dos riscos são assinaladas nas colunas correspondentes da planilha.

7.4 CÁLCULO DO NÍVEL:

A pontuação do nível do risco é definida através da multiplicação das colunas de Peso e Criticidade.

P * C

7.5 AVALIAÇÃO DOS RISCOS

Na etapa de avaliação dos riscos deve ser considerada a forma em que será tratado o risco identificado.

1. Reduzir: aplicação de um controle para que o risco seja reavaliado como aceitável
2. Evitar: deixar de executar a atividade de risco
3. Transferir: realizar a transferência do risco para outra entidade
4. Aceitar: aceitar o risco como está

7.6 CONTROLES E AÇÕES ADOTADAS

É um conjunto de técnicas que visa mitigar os riscos e tratar afim de evitar que possíveis danos pessoais e/ou a empresa.

7.7 ATENDIMENTO

Após implementação dos controles, deverá ser avaliado o atendimento, se atende, atende parcial ou não atende.

7.8 ANÁLISE DO RISCO RESIDUAL

Após a análise de atendimento dos controles, a análise residual deverá ser realizada, com foco nos controles implementados e a ausência de novas medidas para mitigar os riscos.

7.9 EFICÁCIA DAS MEDIDAS DE CONTROLE

A eficácia dos controles avalia a pertinência e adequação das ações e os objetivos pretendidos para os riscos apontados a fim de identificar mudanças no desempenho esperado.

A eficácia deverá ser apontada na ocasião da Análise Crítica- ARAC, afim de monitorar o atendimento dos controles e o nível dos riscos dos processos, bem como os desvios constatados.

7.9.1 AVALIAÇÃO DA EFICÁCIA DOS CONTROLES

A periodicidade de avaliação da eficácia dos controles, devem ocorrer no máximo semestralmente.

8. GESTÃO DE CONSEQUENCIAS

A Engeman adota as seguintes medidas disciplinares que poderão ser aplicadas no caso de violação de qualquer norma contida neste Programa, no Código de Ética e Conduta Profissional, no Programa de Integridade e na Política de Gestão Integrada visando o seu integral cumprimento por todos os Colaboradores, Gestores e Diretores dependendo do ocorrido.

- **Advertência:** quando colaborador não for reincidente
- **Suspensão:** quando o colaborador for reincidente;
- **Demissão**: quando o colaborador cometer ilícito grave como assédio e suborno.

9. MONITORAMENTO

A Engeman monitora a eficácia do Programa de Privacidade anualmente através do RIPD- Relatório de Impacto à dados Pessoais que será analisado criticamente na ocasião da reunião de análise crítica- ARAC.
Através do RIPD, serão analisadas as informações recebidas através do canal ouvidoria ou solicitações recebidas via e-mail pelo Encarregado de Dados e os indicadores associados.

10. RESPONSABILIDADES

ATIVIDADE	RESPONSABILIDADE				
	Qualquer funcionário	Encarregado de Dados	SGI	Gestores de Unidades e Filiais	Diretoria
Identificar os riscos de suas atividades				X	
Detectar Incidente ou acidentes	X	X	X	X	
Emitir ação corretiva		X			
Realizar a comunicação entre as partes interessadas		X			
Controle das ações		X	X		
Avaliar a eficácia dos controles		X	X		
Inspecionar		X	X		
Coleta e armazenamento dos dados e quais medidas de segurança da informação serão aplicadas ao tratamento	X			X	
Prover recursos necessários para a manutenção e melhoria do Sistema de Gestão, assegurando a confidencialidade, transparência, eficácia e eficiência					X
Comunicar, conscientizar e promover as práticas da Segurança da informação;					X
Assegurar o cumprimento do Código de Conduta e Ética;					X
Aprovar Política do SGI, objetivos e indicadores;					X
Responsável pela comunicação com o poder público e desenvolvimento de políticas					X

11. HISTÓRICOS

Rev.	Data	Alteração
01	27/07/2021	Inclusão dos itens 8 e 9
02	13/08/2021	Inclusão do organograma do Comitê de Privacidade no subitem 5.1; Revisão das atribuições dos membros do comitê de privacidade (item 5.2) Revisão dos itens 5.4 e 5.5 Revisão da sistemática de incidente (item 5.8) Revisão no quadro de responsabilidades (item 10)

12. ASSINATURAS

Elaborado: _____

Aprovado: _____