1. OBJETIVO

Orientar e estabelecer as atividades de análise e monitoramento de incidentes em processos e controles, contribuindo para a melhoria do ambiente de controle e conformidade da companhia.

2. ABRANGÊNCIA

Este padrão aplica-se à Gerência Executiva de Conformidade.

3. DESCRIÇÃO

As atividades descritas nesse processo têm como objetivo realizar o monitoramento e a análise dos incidentes em processos e controles, buscando as causas dos incidentes e de suas materializações, quando ocorrerem, correlacionando aos riscos e processos, identificando lacunas e possibilidades de melhorias nos aspectos de conformidade e controles internos. Possibilitam, assim, a formação de uma base de dados de suporte para estudos de elaboração ou revisão do ambiente de conformidade da Companhia.

3.1. Requisitos do Processo

A identificação das causas dos incidentes e sua prevenção e/ou ações de detecção tempestiva, correlacionando com riscos no desenho e avaliação de processos, bem como medidas de respostas a riscos, inclusive através de controles internos, deve ocorrer de forma articulada com as demais áreas da companhia e com a participação dos gestores de processos.

A proposição de melhorias deve ocorrer de forma articulada nos processos afetados, a partir de informações de incidentes reportados pela Auditoria Interna, Auditoria Externa e área de Integridade Corporativa.

A criação e a manutenção de uma base de dados para registro dos incidentes correlacionando com os respectivos processos, riscos e atividades de controles ou ações de conformidade, deverá

ocorrer de forma articulada com as demais áreas da CONFORMIDADE e/ou companhia.

3.2. Fluxo de Atividades

Analisar Incidentes de Controle_Fluxo.xlsx

3.3. Detalhamento das Atividades do Processo

3.3.1. Comunicar incidentes de controle

As áreas de Auditoria Interna e Integridade Corporativa informam, mensalmente, a relação com a descrição das não conformidades apuradas.

No reporte disponibilizado para CONF/IMIC/AM, deve constar a forma de apuração do incidente (número do relatório de auditoria, da apuração especial ou da apuração), descrição detalhada do incidente, processo, risco, criticidade e unidade em que ocorreu o incidente e a data de emissão do relatório que reportou o fato.

Adicionalmente, os incidentes constantes nos relatórios finais emitidos pelo TCU e pela CGU, direcionados à Companhia, são identificados e acrescidos ao escopo de análise pela CONF/IMIC/AM.

Por fim, os pontos levantados anualmente na Certificação de Controles Internos sobre Relatórios Financeiros - SOx (SAD e CCI de acordo com o padrão PP-1PBR-00520 - COORDENAR CERTIFICAÇÃO DE CONTROLES INTERNOS) são contemplados na análise de incidentes do período correspondente.

3.3.2. Definir escopo da análise

Cabe a CONF/IMIC/AM definir o escopo de análise e avaliação dos incidentes recebidos, os quais tem como base os seguintes aspectos de relevância:

· Incidentes com criticidade Alta e Muito Alta;
· Incidentes envolvendo riscos empresariais classificados com severidade Muito Alta ou Alta para a Companhia;
· Incidentes envolvendo riscos de Fraude/Corrupção/Salvaguarda de Ativos (FCPA);
· Sumário Agregado de Deficiências (SAD);
· Incidentes informados na Carta de Controles Internos (CCI) elaborada anualmente pelos auditores independentes.
· Incidentes relatados pelo TCU ou pela CGU;

3.3.3. Analisar incidentes

3.3.3.1. Realizar primeira fase da análise

A CONF/IMIC/AM realiza a primeira fase da análise dos registros reportados, constantes no banco de dados de incidentes, validando os processos, unidades da Companhia, riscos e valores envolvidos (quando possível), bem como diagnosticando causas e propondo ações. Em seguida, cabe à CONF/CI uma segunda fase da análise dos incidentes, descritas no item a seguir.

3.3.3.2. Validar o entendimento/diagnóstico dos incidentes

A CONF/CI deve validar a primeira fase da análise realizada pela CONF/IMIC/AM, propondo mudanças, quando couber.

3.3.3.3. Avaliar a efetividade do ambiente de controles internos e conformidade

A CONF/CI deve realizar a avaliação da efetividade de controles internos porventura existentes para mitigação dos incidentes apontados e revisão das matrizes de controles, bem como a necessidade de realização de ações de conformidade complementares.

3.3.3.4. Interagir com as áreas gestoras

A CONF/CI deve promover a interação com as áreas gestoras, responsáveis pelos processos e controles, na busca de medidas de mitigação, incluindo adequações na matriz de controles internos e/ou adoção de medidas de conformidade aplicáveis e complementares.

3.3.3.5. Avaliar a necessidade e proposição de medidas de mitigação

A CONF/CI, com base nas atividades descritas nos itens 3.3.3.2, 3.3.3.3 e 3.3.3.4, deve propor, quando necessário, medidas de mitigação para os riscos identificados.

As ações de mitigação incluem revisão do desenho do controle ou do processo, criação de novo controle, treinamentos, automatizações, entre outros.

A CONF/CI deve definir, através dos controles porventura avaliados, quais aqueles que devem ser objeto de automatização, seja via CCM (Monitoramento Contínuo de Controles), RPA (*Robotic Process Automation*) ou outra forma de automatização, em face da avaliação de risco e relação custo-benefício;

NOTA 1: A CONF/CI deve atuar na identificação e avaliação, em conjunto com os gestores, de controles internos que mitiguem incidentes que sejam avaliados de risco para a Companhia.

A CONF/CI deve justificar, mediante preenchimento em campo próprio definido na documentação de análise, os casos relevantes para os quais não sejam definidas ação de mitigação, explicitando os motivos para os quais a análise tenha demonstrado não haver necessidade de adoção de medidas adicionais relacionadas ao ambiente de controle.

3.3.4. Atualizar base de incidentes

A CONF/IMIC/AM deve atualizar, periodicamente, a base de incidentes, armazenando em planilha ou plataforma eletrônica, as informações recebidas conforme item 3.3.1 assim como os

resultados das análises descritos no item 3.3.3.

3.3.5. Acompanhar Medidas propostas

A CONF/IMIC/AM periodicamente verifica a realização das ações mitigatórias propostas com o objetivo de garantir o tratamento dado aos riscos descobertos de incidentes passados, posteriormente atualizando a base de incidentes e as plataformas de dados disponibilizados aos públicos de interesse.

NOTA 2: A CONF/IMIC/AM e a CONF/CI, além das demais gerências da CONFORMIDADE que eventualmente precisem atuar no processo, devem identificar, a partir da base de incidentes, as necessidades de treinamentos a serem desenvolvidos ou reforçados pelos gestores de processos e sua força de trabalho, com apoio das áreas de Recursos Humanos e Comunicação sempre que necessário, de forma a aprimorar o ambiente de controle e conformidade e reduzir a probabilidade de reincidência de incidentes.

4. REGISTROS

Identificação	Armazenamento	Proteção	Recuperação	Retenção	Disposição
Registro do incidente no Banco de Dados	Planilha eletrônica	Acesso Pasta de Rede Criptografada NP3, protegida por backup.	Incidentes indexados pela área organizacional, macroprocesso, número da apuração da INC e número da Auditoria em ordem cronológica.	Não se aplica	Não se aplica
Relatório de análise de incidentes	Pasta de Rede e Painel eletrônico	Acesso Pasta de Rede Criptografada NP3, protegida por backup.	Número do Relatório em ordem cronológica	Não se aplica	Não se aplica

5. DEFINIÇÕES

"Não aplicável".

6. REFERÊNCIAS

DI-1PBR-00069 - GESTÃO DO PROGRAMA PETROBRAS DE PREVENÇÃO DA CORRUPÇÃO - PPPC
DI-1PBR-00106 - GERENCIAMENTO DOS RISCOS EMPRESARIAIS DA PETROBRAS
PL-0SPB-00008 - POLÍTICA DE COMPLIANCE
PL-0SPB-00018 - CÓDIGO DE CONDUTA ÉTICA
PP-1PBR-00520 -COORDENAR CERTIFICAÇÃO DE CONTROLES INTERNOS

"Não aplicável".

****ÚLTIMA FOLHA DO PADRÃO****