

Relatório AUDIN nº 2021009

Ação de Auditoria: Monitoramento do Plano de Providências Permanente – Núcleo de Tecnologia da Informação (NTI).

1. INTRODUÇÃO

O Plano de Providências Permanente – PPP, como instrumento que consolida as medidas a serem tomadas pela área auditada, deverá conter todas as recomendações feitas pelos órgãos de controles interno, externo e Auditoria Interna, acompanhadas das providências assumidas pela gestão para implementar as recomendações ou, se for o caso, acompanhadas das justificativas para sua não adoção.

É de responsabilidade do gestor garantir a implementação das providências por ele assumidas, assim como manter atualizado esse instrumento, na medida em que tais providências forem se efetivando.

Para apoiar o gestor na revisão do Plano de Providências Permanente, cabe à Auditoria Interna realizar de forma contínua o monitoramento da execução desse plano, buscando auxiliá-lo na resolução das questões pertinentes, assim como na identificação tempestiva das informações relevantes que impactaram a gestão, seja como avanços conquistados ou retrocessos necessários diante de fatos ou situações ocorridos.

O monitoramento visa garantir efetividade às ações de avaliação e/ou consultoria, proporcionando melhoria à gestão da UFABC bem como permitir a detecção e atuação tempestiva em eventos ocorridos que necessitem de aprofundamento e/ou orientação ao gestor para melhoria de processos internos.

Por fim, serve como base para contabilização de benefícios advindos do acatamento e implementação das recomendações feitas pela Auditoria Interna.

2. VISÃO GERAL DO OBJETO DE AUDITORIA

Trata-se de avaliação das recomendações e providências constante do PPP da área, cujo objeto é o Relatório de Auditoria nº 2018005, que apresentou os resultados

da avaliação de diretivas e controles quanto à gestão da segurança da Tecnologia da Informação e Comunicação na UFABC.

Ao final dos trabalhos, foram identificadas 4 constatações e 4 recomendações. Ressalte-se que para uma constatação é possível a sugestão de uma ou mais ações necessárias para mitigação e/ou saneamento da impropriedade encontrada.

Após as diversas rodadas de verificação quanto à adoção das providências pactuadas, iniciamos o ano de 2020 com 08 recomendações sendo acompanhadas.

Esclarecemos que a partir deste ano, o reporte ao Núcleo de Tecnologia da Informação dará por meio de relatórios e não mais de comunicação via e-mail.

3. DA METODOLOGIA DO MONITORAMENTO

A Auditoria Interna - Audin da Universidade Federal do ABC - UFABC realiza o monitoramento da implementação das recomendações e/ou determinações emitidas pelos órgãos de controles (Audin, TCU e CGU) por meio do envio de formulários eletrônicos de monitoramento, via e-mail institucional, os quais são preenchidos pela gestão¹ e devolvidos à Audin, também via e-mail institucional. O gestor, por sua vez, responde a recomendação e encaminha a situação atual da recomendação com a documentação comprobatória, se for o caso.

A Audin, com base nas respostas e documentação comprobatória, realiza análise crítica sobre o *status* em que a recomendação se encontra, podendo classificá-la nos seguintes *status*:

- Implementada: quando forem apresentados documentos ou for verificado que a recomendação foi realmente atendida.
- Parcialmente Implementada: quando a gestão iniciou as ações que atendem a recomendação, porém, ainda faltam procedimentos para que a recomendação seja integralmente atendida.
- Não implementada: quando se constatar que nada foi feito e não houver previsão para o atendimento da recomendação. Ou ainda, quando o gestor entender que a providência adotada foi suficiente para atendimento à

¹A responsabilidade pelas informações prestadas é do servidor/gestor respondente do formulário. Uma vez que o servidor público possui fé pública, todas as respostas são consideradas verídicas até nova verificação *in loco*.

recomendação. Nesse caso, a depender do conteúdo, a Audin poderá considerar que tal ação não foi adequada e atribuir o risco quanto a não implementação ao gestor responsável.

- Baixada/Cancelada: ocorre em razão de mudanças nas condições observadas, caracterizando a perda do objeto.

As análises são registradas em planilhas eletrônicas e os papéis de trabalho devidamente arquivados.

O resultado é apresentado nesse relatório, que traz uma visão geral da quantidade de recomendações monitoradas, bem como a classificação quanto ao atendimento.

Quando da realização de nova auditoria *in loco* da área/subárea/assunto auditado, considera-se o último formulário de monitoramento como base inicial para os trabalhos de auditoria, verificando-se, assim, se as recomendações foram de fato atendidas ou não, sendo que todas as recomendações reiteradas passam a ser acompanhadas pelo novo relatório.

4. DO MONITORAMENTO DAS RECOMENDAÇÕES DA AUDIN

A seguir apresentamos um histórico das recomendações e providências que estão em monitoramento.

CONSTATAÇÃO: 4.1.1 (01) – Fragilidades na Política de Segurança da Informação e Comunicação – POSIC da UFABC e normas correlatas.

RECOMENDAÇÃO: Certificar-se de que as novas políticas e normas mencionadas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC.

PROVIDÊNCIAS INFORMADAS: *Como mencionado anteriormente, as estruturas básicas de SIC estão estabelecidas, mas tem seu trabalho prejudicado devido à pandemia de COVID-19, está programada para a última reunião do CETIC a nomeação da ETRISI, equipe de respostas a incidentes de segurança da informação, que será responsável por tratar diretamente os casos relativos a violações de SIC de TIC na UFABC. Em paralelo a isso, é necessário que o CSIC se reúna para organizar uma proposta de orçamento separada para as ações de SIC, conforme preconiza a legislação, esta atividade só será possível quando do retorno das atividades presenciais. Item previsto no Planejamento Estratégico da área. Com ID-064 - Instituir área de Segurança de Informação e Comunicação de TI na UFABC - Promover a efetivação da Segurança da Informação na UFABC*

ANÁLISE DA AUDIN: Providência parcialmente atendida. Tendo em vista a informação de que novas ações serão adotadas após o retorno das atividades presenciais, realizaremos novo monitoramento em 31/03/2022.

CONSTATAÇÃO: 4.1.5 (02) - Fragilidade na aderência às orientações da NBR ISO/IEC 27002 – Gestão da Segurança da Informação.

RECOMENDAÇÃO: Certificar-se de que as novas políticas e normas mencionadas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC.

PROVIDÊNCIAS INFORMADAS: *Item previsto no Planejamento Estratégico da área. Com ID-063 - Implantação da POSIC - Promover a efetivação da Segurança da Informação na UFABC. Objetivo específico: Estabelecer efetivo gerenciamento da segurança da informação baseado nas boas práticas definidas pelo Cobit 4.1 e NBR ISO/IEC 27002*

Evidências: Planejamento estratégico do NTI (necessária uma conta da UFABC para acesso)

https://docs.google.com/spreadsheets/d/1emRkucyzi1mE8j9PEjM_iilx4joAH4ZbodmRKFDL18/edit?usp=sharing

ANÁLISE DA AUDIN: Segundo consta do arquivo disponibilizado, 30% do que se pretende realizar já foi concluído. Todavia, não existem evidências sobre as ações efetivamente implementadas. Desta forma, prorrogamos o prazo para novo monitoramento que será realizado em 31/03/2022.

CONSTATAÇÃO: 4.1.9 (03) – Falhas na Comunicação e divulgação da SIC pelo NTI.

RECOMENDAÇÃO: Certificar-se de realizar um plano de trabalho, com seu devido cronograma para implantação do conjunto das ações mencionadas e que elas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC.

PROVIDÊNCIAS INFORMADAS: *Os trabalhos envolvendo o desenvolvimento de novas normas e políticas de SIC, incluindo o plano de comunicações, ficou sendo responsabilidade do Comitê de Segurança da Informação e Comunicação do CETIC. Ficou alinhado com a Administração Central que os trabalhos desta comissão ficariam suspensos até o retorno as atividades presenciais, dada a dificuldade de reunir seus membros nas ferramentas disponibilizadas para os trabalhos remotos para a comunidade.*

Evidências:

1. Nomeia o Presidente do CSIC e seu substituto: PORTARIA DA REITORIA Nº 058, DE 14 DE MARÇO DE 2019.

https://www.ufabc.edu.br/images/stories/comunicare/boletimdeservico/boletim_servico_ufabc_826.pdf

2. Nomeia o CSIC: PORTARIA DA REITORIA Nº 513, DE 13 DE DEZEMBRO DE 2018.

https://www.ufabc.edu.br/images/stories/comunicare/boletimdeservico/boletim_servico_ufabc_803.pdf

ANÁLISE DA AUDIN: Providência parcialmente atendida. Tendo em vista a informação de que novas ações serão adotadas após o retorno das atividades presenciais, realizaremos novo monitoramento em 31/03/2022.

CONSTATAÇÃO: 4.1.13 (04) – Ausência de estrutura e recursos de SIC na UFABC
RECOMENDAÇÃO: Certificar-se de que as novas Políticas e Normas mencionadas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC e, certificar-se ainda que, a criação da devida estrutura organizacional proposta seja devidamente efetivada.
PROVIDÊNCIAS INFORMADAS: <i>Como mencionado anteriormente, as estruturas básicas de SIC estão estabelecidas, mas tem seu trabalho prejudicado devido à pandemia de COVID-19, está programada para a última reunião do CETIC a nomeação da ETRISI, equipe de respostas a incidentes de segurança da informação, que será responsável por tratar diretamente os casos relativos a violações de SIC de TIC na UFABC. Em paralelo a isso, é necessário que o CSIC se reúna para organizar uma proposta de orçamento separada para as ações de SIC, conforme preconiza a legislação, esta atividade só será possível quando do retorno as atividades presenciais. Item previsto no Planejamento Estratégico da área. Com ID-064 - Instituir área de Segurança de Informação e Comunicação de TI na UFABC - Promover a efetivação da Segurança da Informação na UFABC</i>
ANÁLISE DA AUDIN: Providência parcialmente atendida. Tendo em vista a informação de que novas ações serão adotadas após o retorno das atividades presenciais, realizaremos novo monitoramento em 31/03/2022.

Após o detalhamento das 04 recomendações em monitoramento, temos a seguinte situação:

IMPLEMENTADA	NÃO IMPLEMENTADA	BAIXADA POR PERDA DE OBJETO	EM MONITORAMENTO
0	4	0	4

5. DO MONITORAMENTO DAS RECOMENDAÇÕES DOS ÓRGÃOS DE CONTROLE (CGU E TCU).

Inexistem recomendações da CGU ou do TCU emitidas diretamente ao NTI

6. DA CONTABILIZAÇÃO DE BENEFÍCIOS

Em observância à Instrução Normativa nº 10 da Controladoria Geral da União, de 28 de abril de 2020, constatou-se ainda que, em virtude do trabalho desenvolvido por esta Auditoria Interna, para o período 2020/2021 não houve a comprovação quanto ao atendimento das recomendações propostas em Relatório de Auditoria, tendo em vista a suspensão das atividades presenciais desde março/2020 em razão da pandemia do novo coronavírus.

Para conhecimento, os benefícios advindos da adoção de novos controles podem ser dispostos da seguinte forma:

Tipos de benefício	Classes de benefício		Quantidade e/ou valores
Financeiro (valores monetários)	Gastos indevidos evitados		-
	Valores recuperados		-
Não financeiro (outras unidades de mensuração que não monetárias)	Missão, visão, resultados	Transversal	-
		Estratégica	-
		Tático-operacional	-
	Pessoas, estruturas e processos internos	Transversal	-
		Estratégica	-
		Tático-operacional	-

Fonte: Levantamento do Relatório e das respostas da Unidade monitorada.

7. ENCAMINHAMENTOS

Encaminha-se o relatório final:

À Coordenação do NTI para conhecimento e providências.

Ao Reitor como parte integrante da consolidação do monitoramento de todas as recomendações constantes do PPP da UFABC.

À Controladoria-Geral da União em atendimento à IN 05/20021.

Santo André, 03 de novembro de 2.021.

À apreciação superior,



Gilberto da Silva Gusmão
Economista



Márcia Aparecida Costa
Assistente Adm.

De acordo. Encaminhe-se, conforme o proposto.



Rosana de Carvalho Dias
Auditora chefe