Nota N°: 10/2018

Destino: Núcleo de Tecnologia da Informação (NTI)

Assunto: Avaliação do Plano de Providências do NTI, quanto ao Relatório de Auditoria - RA n° 2018005 – Ação de Auditoria nº 05 – PAINT 2018 – Gestão da Segurança da Informação e Comunicação da UFABC.

A presente Nota avalia as providências quanto à ação de auditoria relativa ao assunto supracitado, emanadas pelo **Núcleo de Tecnologia da Informação (NTI)** em seu Plano de Providências Permanente – PPP encaminhado em 04/12/2018 à Auditoria Interna - AUDIN.

1. CONSTATAÇÕES

1.1. Constatação 1: Fragilidades na Política de Segurança da Informação e Comunicação - POSIC da UFABC e normas internas correlatas.

1.1.1. Providências informadas pela área:

> 1.b Providências a serem implementadas: divulgação da nova PoSIC 2018; Criação de Workshop´s sobre a Posic; criação do Time de Resposta a Incidentes de Segurança da Informação; Criação de procedimentos para a notificação e o registro de incidentes de segurança.

1.1.2. Prazo de atendimento: 01/12/2019.

1.1.3. Análise da AUDIN: Parcialmente Acatada. Em que pese as providências relatadas, cabe observar que algumas das fragilidades também evidenciadas no rol na constatação 1 (item 4.1.1 do RA) não foram totalmente abordadas nas providências apontadas, a exemplo das evidências de n°s 1, 4 e 5, que dizem respeito a "Não há uniformização entre unidades de tratamento seguro de acesso às informações", a "Ausência de Plano de Continuidade de Negócios – PCN formalizado" e a "Fragilidade no processo de controle de acessos", respectivamente. Já a evidência n° 2 ("Falta de clareza de procedimentos, supervisão e interação quanto ao encaminhamento de

ocorrências de incidentes de segurança da informação"), há providência para formulação de procedimento de interação (fluxo de informação) de incidentes entre atores internos, porém, não restou claro se a área tratará tal falha quando da composição do Time de Resposta a Incidentes de Segurança da Informação. No mais, as providências propostas pela área serão monitoradas na data indicada pela área, entretanto, em função da extensão do prazo informado, **a AUDIN adotará data intermediária de 05/08/2019 para solicitação de posicionamento sobre andamento da referida providência.**

1.2. Constatação 2: Fragilidade na aderência às orientações da NBR ISO/IEC 27002 – Gestão da Segurança da Informação.

1.2.1. Providências informadas pela área:

> 2.b Providências a serem implementadas: Nomeação do Gestor de Segurança da Informação; Colocar em prática processos de Gestão de conformidade de Segurança da Informação; Colocar em prática processo de Gestão de Riscos;

1.2.2. Prazo de atendimento: 01/12/2019.

1.2.3. Análise da AUDIN: Acatada. As providências propostas pela área serão monitoradas na data indicada, entretanto, em função da extensão do prazo informado, **a AUDIN adotará data intermediária de 05/08/2019 para solicitação de posicionamento sobre andamento da referida providência.**

1.3. Constatação 3: Falhas na Comunicação e Divulgação da SIC pelo NTI.

1.3.1. Providências informadas pela área:

> 3.b Providências a serem implementadas: O NTI estuda melhorar a sua comunicação por meio de ações como palestras, boletins, entre outros. Este estudo ocorre em paralelo à criação de um escritório de Governança de TIC, responsável por esta gestão e que atualmente está em fase beta de implantação;

1.3.2. Prazo de atendimento: 01/12/2019.

1.3.3. Análise da AUDIN: Acatada. As providências propostas pela área serão monitoradas na data indicada, entretanto, em função da extensão do prazo informado,

a AUDIN adotará data intermediária de 05/08/2019 para solicitação de posicionamento sobre andamento da referida providência.

1.4. Constatação 4: Ausência de estrutura e recursos de SIC na UFABC.

1.4.1. Providências informadas pela área:

> 4.b Providências a serem implementadas: Criação do Comitê de Segurança da Informação e Comunicação para tratar de políticas, normas e assuntos orçamentários; Criação de divisão de Governança de TIC o qual será responsável pela gestão de riscos e conformidade de segurança da informação. Criação de Equipe de tratamento a incidentes de segurança da informação.

1.4.2. Prazo de atendimento: 01/07/2020.

1.4.3. Análise da AUDIN: Acatada. As providências propostas pela área serão monitoradas na data indicada, entretanto, em função da extensão do prazo informado, **a AUDIN adotará data intermediária de 25/11/2019 para solicitação de posicionamento sobre andamento da referida providência.**

2. ENCAMINHAMENTO

Encaminhamos a Nota Final de Auditoria - NFA nº 10/2018 ao Núcleo de Tecnologia da Informação - NTI, para ciência da avaliação realizada pela AUDIN do Plano de Providências Permanente – PPP referente ao Relatório de Auditoria nº 2018005, cuja implementação será monitorada nos prazos informados.

Por fim, cabe salientar que a Auditoria Interna da UFABC, na sua missão de agregar valor à gestão, tem buscado o aprimoramento de seus processos e serviços objetivando a excelência no controle interno como instrumento de gestão governamental. Para tanto, baseia sua atuação em reconhecidas práticas internacionais aplicáveis à auditoria interna, a exemplo *The Professional Practices Framework*, assim como da observância de regras internacionais do auditor interno, denominadas PA - *Practice Advisory* do IIA – *Institute of Internal Auditors,* dentre as quais se destaca:

> [...]a responsabilidade da administração é tomar decisões acerca da ação apropriada a ser adotada relativamente às observações e recomendações significativas dos trabalhos de auditoria. A alta administração pode decidir-se a assumir o risco de não corrigir a condição relatada devido a considerações devidamente justificadas[...] (PA/IIA nº. 2060-1, Orange Book, p.154.).

Dessa forma, finaliza-se esta ação, transferindo-a ao Monitoramento das Ações de Auditoria.

Santo André, 19 de dezembro de 2018.

Gebel Eduardo Mendonça Barbosa
Administrador

De acordo. Encaminhe-se conforme proposto.

Patrícia Alves Moreira
Gerente da Auditoria Interna - em substituição.