Auditoria Interna

AUDITORIA DE CONFORMIDADE

Relatório de Auditoria nº 05/2017

PROGRAMA DE AUDITORIA: 08/2017

MACROPROCESSO: 09. Gestão de Tecnologia da Informação

PROCESSO: 09.01 Governança e Segurança em TI

SUBPROCESSO: 09.01.03. Segurança da Informação

UJ: 153010 - Centro Federal de Educação Tecnológica Celso Suckow da Fonseca

SETOR: Departamento de Tecnologia da Informação (DTINF)

Érica Gomes Rocha da Silva

20/10/2017

SUMÁRIO

1. INTRODUÇÃO

Esse relatório tem como objetivo apresentar os resultados da auditoria relativa à análise da regularidade das atividades da Instituição referentes à Segurança da Informação, realizada de maio a julho de 2017. A Auditoria Interna, ao longo dos trabalhos, reportou-se ao Departamento de Tecnologia da Informação (DTINF), vinculado à Diretoria de Gestão Estratégica (DIGES), por esse departamento ser o responsável pelas atividades de Segurança da Informação no âmbito do Cefet/RJ.

1.1 SITUAÇÃO A SER AVERIGUADA

Analisar a regularidade das atividades da Instituição relativas à Segurança da Informação.

1.2 ESCOPO DA AUDITORIA

Observar a conformidade das atividades da Instituição relativas à Segurança da Informação, através da avaliação de sua Política de Segurança da Informação e Comunicações (POSIC).

2. RESULTADO: CONSTATAÇÃO

2.1 AUSÊNCIA DE POSIC NO ÂMBITO DO CEFET/RJ

2.1.1 CONTEXTO DA AUDITORIA

Com o propósito de analisar as atividades da Instituição voltadas à Segurança da Informação, inicialmente questionou-se a existência da POSIC na reunião de abertura dos trabalhos. De maneira complementar, foi emitida a SA n° 08_01.2017, solicitando a disponibilização da POSIC e encaminhadas outras Solicitações de Auditoria requerendo informações relevantes relacionadas à Segurança da Informação.

Devido ao escopo da presente auditoria, não foi aplicável a adoção de universo amostral, assim como critério de seleção da amostra e sua respectiva constituição e tamanho. A seguir é apresentado o quadro com os achados de auditoria, suas possíveis causas e efeitos.

Quadro 1 – Achado de Auditoria: Ausência de POSIC no âmbito do Cefet/RJ

ACHADO	POSSÍVEL CAUSA	POSSÍVEL EFEITO
Não há POSIC aprovada e formalizada. O Grupo de Trabalho encontra-se em	Não atendimento da legislação aplicável à elaboração da POSIC.	Ausência de normativos que regulamentem e controlem as atividades de Segurança da Informação

processo de formação, segundo Memorando n° 27/2017/DTINF.		no âmbito do Cefet/RJ.

2.1.2 MANIFESTAÇÃO DO GESTOR

Na reunião de abertura dos trabalhos e através do Memorando n° 27/2017/DTINF, emitido em 12/05/2017, a gestora do DTINF, afirmou que a Instituição não possui POSIC formalizada, existindo apenas um rascunho da política em questão.

2.1.3 RECOMENDAÇÕES

- Elaborar a Política de Segurança da Informação e Comunicações, conforme orienta a Norma Complementar nº 03/IN01/DSIC/GSIPR[1].
- Constituir Grupo de Trabalho, de acordo com a recomendação da Norma Complementar nº 03/IN01/DSIC/GSIPR.

2.2 FALTA DE DISSEMINAÇÃO DA CULTURA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA INSTITUIÇÃO

2.2.1 CONTEXTO DA AUDITORIA

Foi emitida SA nº 08_02/2017, questionando se existe promoção da cultura de segurança da informação e a forma como ela é realizada. Posteriormente, foi emitida SA nº 08_03/2017, requerendo a apresentação dos instrumentos utilizados para promover a cultura de segurança da informação no DTINF. O quadro 2 traz o achado de auditoria, possíveis causas e efeitos.

Quadro 2 – Achado de Auditoria: Falta de disseminação da cultura da segurança da informação e comunicações na instituição

ACHADO	POSSÍVEL CAUSA	POSSÍVEL EFEITO
Ausência de disseminação da cultura da Segurança da Informação no Cefet/RJ como um todo.	Não atendimento da legislação aplicável à segurança da informação.	Vulnerabilidades causadas pelo uso inadequado das ferramentas de TI pela comunidade no âmbito da Instituição.

2.2.2 MANIFESTAÇÃO DO GESTOR

[1] Estabelece diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

Em resposta à SA nº 08_02/2017, o DTINF emitiu, em 12/05/2017, o Memorando n° 27/2017/DTINF, em que afirmou o seguinte:

"No âmbito do departamento de tecnologia da informação essa cultura é promovida, havendo constante orientação quanto à segurança da informação. Quanto à promoção externa, está será contemplada pelas ações de divulgação da política."

O DTINF emitiu, em 03/07/2017, o Memorando n° 32/2017/DTINF, em resposta à SA nº 08_03/2017, apresentando a seguinte manifestação:

"No âmbito do departamento de tecnologia da informação essa cultura é promovida, havendo constante orientação quanto à segurança da informação".

2.2.3 COMENTÁRIOS À MANIFESTAÇÃO

A área auditada não mencionou, no respectivo memorando de resposta, quais são os instrumentos utilizados para promover essa cultura no DTINF.

2.2.4 RECOMENDAÇÃO

- Adotar instrumentos que promovam periodicamente a cultura de segurança da informação em toda a Instituição.

2.3 INEXISTÊNCIA DE DOCUMENTO QUE TRATE DA SEGURANÇA CIBERNÉTICA (SegCiber)

2.3.1 CONTEXTO DA AUDITORIA

Foi emitida SA nº 08_02/2017, questionando se existe documento formalizado relativo à Segurança Cibernética (SegCiber). O achado de auditoria, possível causa e efeito, estão expostos no Quadro 3.

Quadro 3 – Achado de Auditoria: Inexistência de documento que trate da Segurança Cibernética (SegCiber)

ACHADO	POSSÍVEL CAUSA	POSSÍVEL EFEITO
Não há documento formalizado que trate da Segurança Cibernética (SegCiber) no Cefet/RJ.	Não atendimento da legislação aplicável à segurança da informação, em especial, à Segurança Cibernética (SegCiber).	Ausência de regulamentação e controle sobre as atividades de Segurança da Informação no âmbito do Cefet/RJ.

2.3.2 MANIFESTAÇÃO DO GESTOR

Com o Memorando n° 27/2017/DTINF, emitido em 12/05/2017, a gestora respondeu à SA nº 08_02/2017, informando que ainda não há documento formalizado relativo à Segurança Cibernética (SegCiber).

2.3.3 RECOMENDAÇÃO

- Normatizar e promover as atividades referentes à Segurança Cibernética na Instituição, em observância à Norma Complementar nº 03/IN01/DSIC/GSIPR.

2.4 AUSÊNCIA DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (GRSIC).

2.4.1 CONTEXTO DA AUDITORIA

Foi emitida SA nº 08_02/2017, questionando se há previsão para implantação da Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) no Cefet/RJ. O Quadro 4 exibe o achado de auditoria, com possível causa e efeito.

Quadro 4 – Achado de Auditoria: Ausência de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC).

ACHADO	POSSÍVEL CAUSA	POSSÍVEL EFEITO
Ainda não teve início a implantação da Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC).	Não atendimento da legislação aplicável à segurança da informação, em especial, à GRSIC.	Carência de mecanismos que controlem os riscos associados à Segurança da Informação e Comunicações no Cefet/RJ.

2.4.2 MANIFESTAÇÃO DO GESTOR

Em resposta à SA nº 08_02/2017, a gestora do DTINF emitiu, em 12/05/2017, o Memorando n° 27/2017/DTINF, em que afirmou existir uma previsão para implantar a (GRSIC), acrescentando que a adoção da GRSIC se seguirá à implantação da gestão de riscos na Instituição.

2.4.3 RECOMENDAÇÃO

- Aplicar a GRSIC de forma sistemática, conforme preceitua a Norma Complementar nº 04/IN01/DSIC/GSIPR[2].

[2] Estipula diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.

2.5 CONTROLES DE ACESSO INFORMAIS

2.5.1 CONTEXTO DA AUDITORIA

Foi emitida a SA nº 08_02/2017, arguindo se existem controles de acesso relativos à segurança da informação e comunicações, e se esses foram aprovados pelo CODIR. De maneira adicional, foi encamindada a SA nº 08_03/2017, requerendo os documentos utilizados para regulamentação dos controles de acesso e os responsáveis pelos referidos controles. O Quadro 5 traz o achado de auditoria, possível causa e efeito.

Quadro 5 – Achado de Auditoria: Controles de acesso informais.

ACHADO	POSSÍVEL CAUSA	POSSÍVEL EFEITO
Existência de controles de acesso sem documento que promova sua formalização e permita a aprovação pelo CODIR.	Não atendimento da legislação aplicável à segurança da informação, principalmente, em relação aos controles de acesso.	Ausência de normatização e consolidação das atividades voltadas ao controle de acesso na Instituição.

2.5.2 MANIFESTAÇÃO DO GESTOR

Por intermédio do Memorando n° 27/2017/DTINF, emitido em 12/05/2017, a área auditada manifestou-se em relação à SA nº 08_02/2017 da seguinte forma:

"Já existem controles de acesso, pois estes são boas práticas de segurança da informação. No entanto, os mesmos são definidos pelas áreas responsáveis por cada informação, e não pelo CODIR".

Por outro lado, no Memorando n° 32/201/DTINF, emitido em 03/07/2017, como resposta à SA nº 08_03/2017, a gestora do DTINF informou que ainda não há formalização dos controles de acesso na entidade.

2.5.3 RECOMENDAÇÃO

- Regulamentar e promover os controles de acesso no Cefet/RJ, com base na Norma Complementar nº 07/IN01/DSIC/GSIPR[3].

2.6 AUSÊNCIA DE INDICAÇÃO FORMAL DOS RESPONSÁVEIS PELAS ATIVIDADES DE SEGURANÇA DA INFORMAÇÃO

2.6.1 CONTEXTO DA AUDITORIA

[3] Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Foi emitida a SA nº 08_02/2017, perguntando se foi designado um gestor de Segurança da Informação e Comunicação (SIC), e se esse gestor tem como uma das atribuições a implementação dos procedimentos relativos ao uso de recursos criptográficos. Também foi questionado se foram designados gestores de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR). O Quadro 6 apresenta o achado de auditoria, sua possível causa e efeito.

Quadro 6 – Achado de Auditoria: Falta de indicação formal dos responsáveis pelas atividades de segurança da informação.

ACHADO	CAUSA	EFEITO
O Cefet/RJ não indicou formalmente os responsáveis pelas atividades de segurança da informação.	Não atendimento da legislação aplicável à segurança da informação.	Dificuldade na atribuição de responsabilidades aos gestores designados.

2.6.2 MANIFESTAÇÃO DO GESTOR

Em resposta à SA nº 08_02/2017, em relação ao questionamento sobre a designação do um gestor de Segurança da Informação e Comunicação (SIC), a gestora do DTINF emitiu em 12/05/2017, o Memorando n° 27/2017/DTINF, apresentando o seguinte posicionamento:

"Há uma seção de segurança da informação (SEGUR) que é responsável pela emissão de normas e procedimentos referentes à segurança da informação em TI. Essa seção, por ser estratégica, está sendo realocada para a divisão de estratégia e governança em TI (DIGTI)".

No que se refere à designação de gestores de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), a gestora do DTINF, ainda no Memorando n° 27/2017/DTINF, manifestou-se conforme exposto abaixo:

"As equipes de resposta e tratamento de incidentes são definidas apenas em caso de necessidade, por motivo de quantitativo de pessoal. Além disso, a ocorrência de incidentes de segurança não é frequente o suficiente para manter uma equipe permanentemente definida para lidar com os mesmos. O chefe da SEGUR fará as vezes de gestor da ETIR, caso ocorram incidentes".

2.6.3 RECOMENDAÇÃO

- Designar formalmente os gestores relacionados às atividades de segurança da informação.

3. ANÁLISE DA AUDITORIA INTERNA

No decorrer da presente auditoria, constatou-se que as atividades de segurança da informação no âmbito do Cefet/RJ ainda não estão formalizadas. Identificou-se a inexistência da Política de Segurança da Informação e dos demais normativos necessários à efetiva implementação dessas atividades na Instituição. Além disso, verificou-se que a Instituição ainda não atende às normas emanadas pelo Gabinete de Segurança Institucional da

Presidência da República (GSIPR), em consonância com o documento Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018[4]. É importante destacar que, conforme o Memorando n° 27/2017/DTINF, os servidores que atuam na SIC realizam capacitações; contudo, foi verificado que a entidade ainda não cumpre todos os requisitos elencados na Norma Complementar nº 17/IN01/DSIC/GSIPR[5].

4. CONCLUSÃO

A análise de auditoria detectou as seguintes constatações: (i) ausência de POSIC no âmbito do Cefet/RJ; (ii) falta de disseminação da cultura da Segurança da Informação e Comunicações na Instituição; (iii) inexistência de documento que trate da Segurança Cibernética (SegCiber); (iv) ausência de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC); (v) controles de acesso informais; e (vi) ausência de indicação formal dos responsáveis pelas atividades de segurança da informação. Com relação à avaliação dos controles internos, foi observado que a maioria dos controles avaliados não existe, enquanto que os demais são fracos. Assim, a maturidade dos controles internos relativos à Segurança da Informação encontra-se em nível inicial, por apresentar formalização precária e carência de controles formalizados.

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO

_____

ÉRICA GOMES ROCHA DA SILVA
Contadora

De acordo:

_____

LUCIANA SALES MARQUES BISSOL
Auditora-Chefe

[4] Versão 1.0 (página 51).
[5] Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).