RELATÓRIO

GT - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Santo André

Agosto de 2018

Sumário

1 Introdução

O presente relatório é um dos resultados das atividades do Grupo de Trabalho - Política de Segurança da Informação (PoSIC), que também elaborou as minutas da Política e das normas de segurança da informação. Este GT é vinculado ao Comitê Estratégico de Tecnologia da Informação e Comunicação (CETIC) da UFABC, e foi instituído em 02 de março de 2017 pela Portaria da Reitoria nº 118, publicada no Boletim de Serviço nº 632 de 03 de março de 2017, e prorrogado pela Portaria da Reitoria nº 292 de 23 de agosto de 2017, publicada no Boletim de Serviço nº 678 em 25 de agosto de 2017. As metas do GT serão detalhadas em uma seção específica deste relatório.

Com a assinatura do Decreto nº 3505, de 13 de junho de 2000, o Governo Federal começou a disciplinar as ações de Segurança da Informação para os órgãos da APF, através de diretrizes gerais, além de criar o Comitê Gestor de Segurança da Informação. Desde então, surgiram cada vez mais esforços para estruturar esta área, dentre eles, a criação do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional (DSIC/GSI/PR) pelo Decreto nº 5772, de 2006.

De acordo com a Instrução Normativa nº 1 do GSI/PR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na APF, o DSIC é o órgão responsável por planejar e coordenar as atividades de SIC, além de estabelecer normas, definindo os requisitos metodológicos para implementação da Gestão de SIC na Administração Pública Federal. Outro papel importante é o de orientar a condução da Política de Segurança da Informação e Comunicações.

Com a finalidade de orientar os órgãos federais na criação de suas próprias políticas de SIC, o DSIC sistematizou regras claras consubstanciadas em três instruções normativas e 21 normas complementares, sendo que todas elas têm respaldo das melhores práticas em SIC, e a principal referência é a NBR ISO/IEC 27001:2006 e a NBR ISO/IEC 27002:2005.

São contempladas nas normas complementares, informações de grande relevância para a UFABC, como a gestão de riscos de segurança da informação, credenciamento de segurança para tratamento e classificação da informação e time de resposta aos incidentes de redes. Tais normas regulamentam a adoção de práticas de segurança da informação envolvendo ações, diretrizes, princípios, definições, competências técnicas e responsabilidades.

Segundo o guia ao Gestor em Segurança da Informação e Comunicações, criado pelo GSI em parceria com a Secretaria Executiva e o DSIC, a PoSIC é um documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta ou indireta, com o objetivo de fornecer suporte administrativo, diretrizes e critérios suficientes à implementação da SIC. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação de uma organização. Assim, deve ser entendida como uma declaração formal dos órgãos e entidades federais, acerca de seu compromisso com a proteção das informações sob sua custódia, devendo ser cumprida por todos os agentes públicos e colaboradores.

Um dos principais objetivos da PoSIC é instruir o processo de gestão da segurança da informação e as competências para a proteção dos ativos de informação. É importante esclarecer que, de acordo com a Norma Complementar nº 04 da Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República (NC 04/IN01/DSIC/GSI/PR), os ativos de informação são: “Os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso”;

Além disso, uma estrutura gerencial é recomendada para assegurar que os controles de segurança da informação atendam aos requisitos da organização de forma integrada aos processos relevantes.

Entre outras tarefas, a gestão de segurança da informação e comunicação (SIC) deve aprovar as suas metodologias e processos, além de promover a conscientização de segurança e gerenciar as informações recebidas do monitoramento de incidentes de segurança.

Os principais incidentes são:

- Vazamento de informações sigilosas;
- Invasão de sistemas e banco de dados;
- Negação de serviço a sites e infraestrutura que comportam a informação;
- Comprometimento/alteração de arquivos ou sistemas por ações de vírus ou pessoas;
- Uso de software ilegal;
- Acesso físico ou lógico não autorizado;
- Outros;

Entre as ameaças internas mais comuns, podemos citar à modificação ou furto de informações confidenciais para ganho pessoal, o roubo de segredos comerciais ou informações de clientes e também a sabotagem de dados de sistemas ou da rede de uma organização.

Uma pesquisa desenvolvida por uma empresa norte americana de segurança, a *IS Decisions*, aponta que ocorrem 2500 violações internas de segurança todos os dias nos EUA. Isso demonstra que as ameaças internas são umas das principais preocupações de segurança das informações no mundo. Em 2015, segundo uma pesquisa da ISC², 54% dos chefes de segurança da informação entrevistados nos Estados Unidos consideravam-se preocupados com as ameaças causadas por empregados internos. Outra pesquisa, da empresa Forrester, revela que 36% das violações decorrem do uso inadvertido de dados por funcionários descuidados. Além disso, 52% dos funcionários não veem riscos de segurança ao compartilhar *logins* de trabalho.

Esses dados revelam que os controles de segurança da informação devem alcançar também o domínio humano, além do tecnológico. Para isso, as normas de segurança devem ser disseminadas internamente, de forma constante. As diretrizes de segurança da informação devem ser

divulgadas a todo corpo de funcionários e aplicadas sem restrição, incluindo a alta administração e todos os funcionários da área de TI, através da Política de Segurança da Informação.

No contexto atual de ameaças, as instituições públicas ou privadas que ainda não possuem uma estratégia de segurança da informação consolidada para gerenciar os seus riscos estão sujeitas a grandes prejuízos financeiros, impactos legais e danos à sua imagem.

2 Justificativa

Em um levantamento realizado pelo NTI em julho de 2014, foi constatado que, embora a UFABC tenha elaborado e publicado a Política de Segurança da Informação e Comunicações em 2013, a grande maioria dos servidores técnico-administrativos (97%) nunca conheceu o seu teor. De acordo com o relatório da Audin de 2013 (item 3.2.1), foi constatada falha na elaboração e implantação da PoSIC institucionalizada. Conforme foi descrito no seu relatório, essa falha impede o estabelecimento e a implementação das diretrizes de Segurança da Informação e Comunicações com vistas a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, o que deixa a UFABC vulnerável aos riscos inerentes à utilização e contratação de serviços de TI. Outras falhas apresentadas foram: ausência de responsabilização do usuário pela custódia dos recursos de TI e ausência de diretrizes para o tratamento das informações (produção, classificação, transporte, armazenamento e descarte). Dentre as recomendações da Audin para a área de SIC destacamos:

1) Implementar processo de Gestão de Riscos de segurança da informação no setor de TI, de forma integrada e alinhada à alta administração, utilizando métodos quantitativos e qualitativos para avaliar regularmente a probabilidade e o impacto de um determinado risco, conforme normas e legislação vigentes (item T - 3.2.1, AUDIN, 2013);

2) Instituir uma área de Segurança da Informação e Comunicações de TI, nomeando-se um gestor com perfil adequado com a composição de respectiva equipe voltada às atribuições da área. (item Q - 3.2.1, AUDIN, 2013); e

3) Estabelecer o efetivo gerenciamento da segurança da informação baseado nas boas práticas com observância do disposto na Instrução Normativa nº 01/2008 do Gabinete de Segurança Institucional da Presidência da República e da Norma Complementar 03/IN01/DSIC/GSIPR. (item S - 3.2.1 AUDIN, 2013).

Além disso, a respeito da obrigatoriedade da aplicação das normas de segurança da informação na Administração Pública Federal, o Acordão nº 1233/2012 do TCU descreve o seguinte:

9.8.2. Em atenção a Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas

normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II (subitem II.8);

2.1 Alinhamento Estratégico com o PDI e o PDTI

No capítulo 8, “Universidade com Tecnologia da Informação e Comunicação”, no subcapítulo 8.4, “outros serviços do NTI”, o PDI aponta em seu item “Segurança de Sistemas” a responsabilidade do NTI pela segurança interna e externa de sistemas de informação da UFABC e pela aplicação da Política de Segurança da Informação e Comunicações para garantir a proteção dos dados e acessos aos sistemas relacionados aos aspectos de integridade, disponibilidade e confidencialidade, quando esta última for necessária. Além disso, de acordo com o PDI, “deverá ser incentivada uma cultura de segurança em que todos tenham consciência da sua responsabilidade em relação aos ativos de informação”. (PDI UFABC 2013-2022 p. 116).

Além disso, a criação de uma área dedicada à Segurança da Informação e Comunicações na UFABC foi prevista no PDTI 2016/2017 (Plano de Investimentos, pág. 42 e Plano de Metas e Ações pág. 51);

3 Objetivo do GT

O objetivo deste GT é atualizar a Política de Segurança da Informação e Comunicações da UFABC (PoSIC UFABC).

3.1 Objetivos específicos:

- Estudar ações que contemplem a metodologia de gestão de segurança da informação e comunicações recomendada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) em sua norma complementar nº 02 IN01/DSIC/GSIPR de maneira que seja aderente aos objetivos descritos no Plano de Desenvolvimento Institucional da UFABC (PDI UFABC 2013-2022);
- Desenvolver normas para regulamentar os diversos serviços de Tecnologia da Informação, operacionais ou de gestão, tais como controle de acesso, desenvolvimento e manutenção de sistemas, uso de computadores pessoais, acesso a internet, entre outros, para substituir a Resolução nº 12 do CONSUNI, que data de 09 de outubro de 2008 . Esta resolução foi considerada obsoleta pelo GT.
- Estudar a criação de controles internos que assegurem a integridade, a disponibilidade e a confidencialidade das informações, esta última, somente nos casos previstos na legislação, incluindo a Lei de Acesso a Informação (LAI);
- Discutir métodos para mapear os processos mais críticos com relação à segurança de informações, comunicações e dados e definir os níveis de exposição às ameaças internas e externas, bem como definir o impacto de um ou vários incidentes causados por essas ameaças;

- Estudar as diversas metodologias de avaliação de riscos envolvendo a segurança das informações, comunicações e dados da UFABC;

4 Metodologia

O GT foi estruturado para viabilizar a participação de todas as áreas da UFABC com a finalidade de estabelecer um processo transversal de reflexão e debate e que permeasse as principais estruturas do fluxo de gestão da informação envolvendo todo o seu ciclo de proteção.

Para garantir que o processo de criação fosse mais dinâmico e efetivo, o GT foi dividido em 2 (dois) subgrupos, descritos a seguir:

Grupo 1 - Comissão Executiva

Grupo responsável pela criação da minuta da PoSIC e das normas temáticas de segurança da informação e comunicações;

4.1 Membros da Comissão Executiva:

- Lucas Trombeta
- Prof. João Henrique Kleinschmidt
- Paulo Victor Fernandes Silva
- Profª Luana Sucupira Pedroza.
- Fábio Senigália
- Rafael Rondina
- Cristiano de Noronha Lopes

4.2 Principais atividades desenvolvidas pela Comissão Executiva:

- Pesquisa de políticas e normas de outras universidades federais;
- Pesquisa em guias de boas práticas do Tribunal de Contas da União (TCU) e do Sistema de Administração dos Recursos de Tecnologia da Informação do Ministério do Planejamento (SISP/MPDT), entre outros;
- Pesquisa de normas complementares do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e do seu Departamento de Segurança das Informações e Comunicações (DSIC);
- Análise crítica de documentos produzidos na UFABC que tratam de temas ligados à segurança da informação e comunicações;
- Revisão de regras e diretrizes propostas pela Comissão Consultiva.

Grupo 2 - Comissão Consultiva

Grupo opinativo responsável pela avaliação dos controles decorrentes das novas regras impostas pelas normas temáticas de segurança e pela própria PoSIC;

4.3 Membros Comissão Consultiva:

- Eneyas Dutra Barbosa
- Alessandra de Castilho
- César Augusto Moreira Guarido
- Gabriel Oblasser dos Santos (suplente)
- Célia Dias do Nascimento
- Walkyria Elissa Machado Rocha (suplente)
- Gesialdo Silva do Nascimento
- Thais Rodriguez de Toledo
- Carlos Spinetti Moda (suplente)
- Enio Rodrigues Vieira
- Conrado Emilio Gomes
- Henrique de Abreu Piccolo
- Vinicius Nunes Zorzetti
- Robson Luiz Mioto de Carvalho
- Silas Leite de Oliveira (suplente)

4.4 Principais atividades desenvolvidas pela Comissão Consultiva:

- Participação em consultas técnicas e em rodas de conversas;
- Avaliação técnica e validação das mudanças decorrentes da aplicação das normas temáticas;
- Proposição de regras para as minutas das normas complementares;
- Elaboração de minutas de normas pertinentes a sua área de atuação;

5 Referencia normativa para a estrutura gerencial de segurança da informação

A estrutura organizacional de segurança da informação é preconizada por diversas normas federais e por normativos técnicos internacionais, descritos no quadro a seguir:

"Convém que a coordenação da segurança da informação envolva a cooperação e a colaboração de gerentes, usuários, administradores, desenvolvedores, auditores, pessoal de segurança e especialistas com habilidades nas áreas de seguro, questões legais, recursos humanos, TI e gestão de riscos" (Controle 6.1.2, **Coordenação da segurança da informação** - ABNT NBR ISO/IEC 27002:2005).
"Convém que todas as responsabilidades pela segurança da informação, estejam claramente definidas." (Controle 6.1.3, **Atribuição de responsabilidades para a segurança da informação** - ABNT NBR ISO/IEC 27002:2005).
"É recomendável que na estrutura da instituição exista uma área responsável pela segurança de informações, a qual deve iniciar o processo de elaboração da política de segurança de informações, bem como coordenar sua implantação, aprová-la e revisá-la, além de designar

funções de segurança". (item 1.4, **Quem são os responsáveis por elaborar a PSI?** - Guia de Boas Práticas em Segurança da Informação - TCU, 4ª edição, 2012).
"Nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002". (item 9.15.12.1. **Acordão TCU 1233/2012**).
"Criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002". (item 9.15.12.2. **Acordão TCU 1233/2012**).
"Implementar processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 - Gestão de riscos de segurança da informação" (item 9.15.12.3 **Acordão TCU 1233/2012**).
"Definir a estrutura para a Gestão da Segurança da Informação e Comunicações". (item 5.3.7.1 **Competências e Responsabilidades -** Norma Complementar nº 03/IN01/DSIC/GSIPR de 30 de junho de 2009).
"Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do órgão ou entidade da APF". (item 5.3.7.4 **Competências e Responsabilidades -** Norma Complementar nº 03/IN01/DSIC/GSIPR 30 de junho de 2009).
"O processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações". (item 5.2. **Princípios e Diretrizes -** Norma Complementar nº 04/IN01/DSIC/GSIPR de 15 de Fevereiro de 2013).
"Os Gestores de Segurança da Informação e Comunicações, no âmbito de suas atribuições, são responsáveis pela coordenação da Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos e entidades da APF, direta e indireta". (item 7.2 **Responsabilidades -** Norma Complementar nº 04/IN01/DSIC/GSIPR de 15 de Fevereiro de 2013).
"De acordo com as necessidades de cada órgão ou entidade, os Gestores de Segurança da Informação e Comunicações poderão indicar responsáveis pelo gerenciamento de atividades (...)". (item 7.3 **Responsabilidades -** Norma Complementar nº 04/IN01/DSIC/GSIPR de 15de Fevereiro de 2013).
"Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete: III - propor programa orçamentário específico para as ações de segurança da informação e comunicações; IV **- nomear Gestor de Segurança da Informação e Comunicações**; V - instituir e implementar **equipe de tratamento e resposta a incidentes em redes computacionais**; VI **- instituir Comitê de Segurança da Informação e Comunicações**; (art. 5º - Instrução Normativa 01/2008 GSI/PR)".

6 Desenvolvimento

O GT foi dividido em duas fases:

1ª fase: Atualização da PoSIC;

2ª fase: Desenvolvimento das normas complementares à PoSIC (Normas Temáticas);

A primeira fase foi iniciada em 03 de março de 2017. Neste período, o GT revisou a PoSIC e propôs novas diretrizes baseadas nos resultados das discussões. A Comissão Executiva se reuniu em treze oportunidades e realizou duas consultas aos órgãos de controle da UFABC em relação aos aspectos legais da PoSIC, sendo a primeira consulta à Corregedoria Seccional da UFABC e a segunda à Procuradoria Federal da UFABC. A consulta questionou a autonomia da Equipe de Tratamento a Incidentes de Redes e Segurança da Informação para a realização de procedimentos de análise forense. Isso porque alguns procedimentos requerem privilégios administrativos, os quais inclui examinar os registros de atividades de qualquer servidor armazenados em logs.

6.1 1º Fase

6.1.1 Estruturação

Na primeira fase, os temas da PoSIC foram divididos em 12 eixos de discussão, descritos a seguir, objetivando dar maior celeridade ao processo de atualização:

1. Competências e responsabilidades
2. Tratamento de incidentes de segurança e ETIR
3. Gestão de riscos e vulnerabilidades
4. Auditoria, conformidade e penalidades
5. Aquisição e desenvolvimento de sistemas
6. Controle de acesso
7. Uso de e-mail
8. Acesso a Internet e rede wireless
9. Gestão da continuidade dos negócios
10. Tratamento das informações
11. Uso dos recursos corporativos e pessoais
12. Redes Sociais

6.1.2 Eixo Competências e Responsabilidades

O CETIC deve apoiar às ações de Segurança da Informação e Comunicações na UFABC demonstrando o seu comprometimento e o conhecimento das responsabilidades inerentes. Em outras palavras, a criação de uma estrutura organizacional de segurança da informação deve seguir a topologia “*top-down”* a qual o CETIC deve tomar as iniciativas dessas ações. No entanto, vale

ressaltar que o cenário ideal inclui a existência do Comitê de Segurança da Informação e Comunicações (CSIC) composta por gestores das áreas de TIC, e também por especialistas em questões legais, segurança física, recursos humanos, gestão de riscos, entre outros. Algumas universidades federais já adotaram esta prática, a exemplo das universidades federais de Itajubá (UNIFEI), Santa Catarina (UFSC), Mato Grosso (UFMT), Santa Maria (UFSM), Rio Grande do Sul (UFRGS), Pernambuco (UFPE) e Pelotas (UFPEL).

6.1.2.1 Situação Atual

- Segundo o Art. 8º da atual PoSIC, o Núcleo de Tecnologia da Informação (NTI) atua como Gestor de Segurança da Informação e Comunicações (GSIC). Entretanto, de acordo com o art. 5º, inciso IV da Instrução Normativa nº 01/2008 do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), é impositivo que o gestor de SIC seja um servidor público nominalmente designado pela autoridade do órgão;
- Segundo o Art. 9º da atual PoSIC, o Comitê Estratégico de Tecnologia da Informação e Comunicação (CETIC) atua como Comitê de Segurança da Informação e Comunicações (CSIC). Além disso, atualmente, o Presidente do CETIC é o Vice Reitor da UFABC. No entanto, de acordo com o art. 7º, Inciso IV da Instrução Normativa nº 01/2008 GSI/PR, é impositivo que o gestor de SIC seja o Coordenador do Comitê de SIC.
- Atualmente não há regimento interno do CSIC;
- Não há programa orçamentário específico para as ações de Segurança da Informação e Comunicações, como sugerido pelo artigo 5º, Inciso III da Instrução Normativa 01/2008 GSI/PR;
- Não há Equipe de Tratamento a Incidentes de Segurança da Informação e Comunicações (ETIR), segundo sugere o art. 5º, Inciso V da Instrução Normativa nº 01/2008 do GSI/PR e a própria PoSIC em seu art.º 10;
- Não há divisão de Segurança da Informação o qual está em desacordo com o item 3.2.1.q do relatório de Auditoria de Gestão de Tecnologia da Informação de 2013. (Audin, 2013).

6.1.2.2 Recomendações do GT PoSIC para a criação da área de Segurança da Informação e Comunicações

O CETIC deve definir quem será o responsável pela área de segurança da informação e comunicações da UFABC que deverá atuar de forma alinhada às diretrizes estratégicas. A inexistência de uma área de segurança da informação é considerada uma falha grave do ponto de vista legal e deve ser pautada no planejamento estratégico.

O GT levantou as principais responsabilidades que a área de gestão da segurança da informação deve assumir:

Promover a cultura de segurança da informação e comunicações na instituição.
Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de

segurança.
Propor recursos necessários às ações de segurança da informação e comunicações no âmbito da UFABC.
Coordenar a divisão de Segurança da Informação, o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento a Incidentes de Redes (ETIR)
Propor a criação e atualização de normas relativas à Segurança da Informação e Comunicações
Capacitar todos os envolvidos com a auditoria de conformidade nas legislações vigentes relacionadas à Segurança da Informação.
Estabelecer a Metodologia de Gestão de Riscos de TIC mais apropriada ao negócio
Alinhar a Gestão de Riscos de TIC aos objetivos de negócio.
Acompanhar a mitigação e transferência dos riscos de TIC.
Gerenciar o controle de acesso e os planos de continuidade de negócio
Promover ações de conscientização e capacitação sobre SIC para todos os usuários
Criar estatísticas sobre resposta a incidentes de SIC.
Prevenir a ocorrência de novos incidentes de SIC.
Divulgar ações de SIC.

A criação da divisão de SIC deverá seguir o rito da Portaria da Reitoria n° 205/2016 que define as diretrizes para a criação de novas áreas administrativas na UFABC.

6.1.2.3 ETIR

Minimamente, uma estrutura de SIC deve compor também uma Equipe de Tratamento a Incidentes em Redes Computacionais (ETIR), mundialmente conhecida como CSIRT® (Computer Security Incident Response Team). Essa equipe possui a responsabilidade de receber, analisar e responder às notificações de incidentes e atividades relacionadas à segurança em redes de computadores;

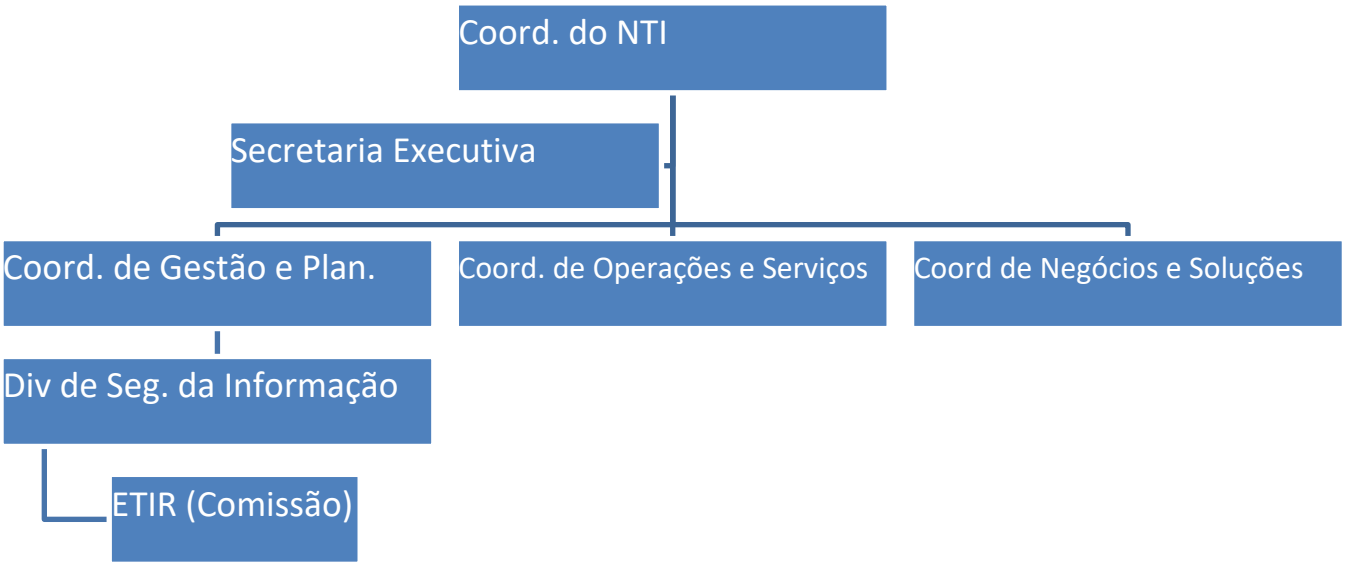
O CETIC deve instituir a ETIR dentro da nova estrutura de segurança da informação conforme preconiza a norma complementar nº 05 IN01/DSIC/GSI. Esta equipe deve ser composta por especialistas das áreas de TIC e segurança da informação com o objetivo principal de responder aos incidentes de segurança em redes computacionais. Será necessário formalizar em ato administrativo a formação dessa nova equipe, detalhando a sua missão, visão, valores, serviços oferecidos, organograma, escopo e autonomia.

O GT entende que a UFABC não possui recursos financeiros e humanos suficientes para a criação de uma nova equipe com este nível de especialização. A contratação de novos funcionários e o deslocamento de pessoal para a nova área é atualmente inviável, além de gerar ônus com a alocação de uma nova sala e a aquisição de material permanente. Como solução, o GT recomenda a criação de uma comissão interna composta, a princípio, por membros do NTI e indicados pela sua

Coordenação. Desta forma, não será mais necessário o deslocamento de servidores das suas funções originais, que dedicarão apenas parte do seu tempo às atividades de resposta a incidentes e demais atividades anuídas em ato administrativo, sem que isso prejudique a suas atividades.

6.1.2.4 Organograma Sugerido para a divisão de SIC e a para a ETIR

A seguir a proposta do GT PoSIC para o organograma que inclui a divisão de segurança da informação e a ETIR:



Neste aspecto, é importante ressaltar que a Divisão de SIC e a ETIR são duas áreas tecnicamente distintas e, portanto, devem possuir equipes dedicadas. A Divisão de SIC será responsável pelos aspectos de gestão de segurança e riscos, enquanto a ETIR desenvolverá atividades mais focadas na solução de problemas na camada operacional.

Outra opção que pode ser estudada pelo CETIC seria a criação de uma área responsável pela Governança de TIC, a qual a divisão de segurança da informação seria integrada. A gestão de riscos e conformidade, inerente a gestão de segurança da informação, é uma das práticas recomendada pelo guia de governança de TIC elaborado pelo SISP em 2015 e integraria a nova área de governança de TIC dentro NTI. Da mesma forma, caso seja acatada esta opção, o NTI deverá estudar os recursos necessários para a criação dessa nova área.

6.1.2.5 Funções de SIC

Após realização de pesquisa das normas ABNT NBR ISO IEC 27001 e ISO 27002, da legislação pertinente ao assunto e dos normativos de segurança da informação, o GT listou de forma detalhada quais devem ser as funções e atividades desempenhadas pela nova divisão de segurança da informação e comunicações, e também as funções da ETIR. Além disso, o GT estabeleceu a necessidade mínima e a ideal de recursos humanos. Este quadro consta em outro documento denominado “Funções de SIC”.

6.1.3 Eixo Tratamento de Incidentes de Segurança

O tratamento de Incidentes de Segurança deve seguir um fluxo que deve conter no mínimo as atividades de recebimento, avaliação, tratamento e aprendizado. Outras atividades podem ser incorporadas e desenvolvidas pela Equipe de Tratamento a Incidente de Redes Computacionais (ETIR) na medida em que for adquirindo maturidade. O processo deve ser mapeado pelos membros indicados a compor a equipe.

A ETIR deve ser responsável pelo tratamento de incidentes de segurança da informação e pela coleta e preservação de evidências digitais, em apoio às investigações administrativas e criminais. A ETIR também deve ter autonomia suficiente para solicitar a custódia temporária de equipamentos para proceder à análise forense computacional, mediante termo assinado, para aferir o "modus operandi", a causa e o autor de um determinado incidente de segurança, desde que haja equipamentos disponíveis em estoque para a imediata substituição. Para isso, é necessário que a equipe tenha amparo legal para preceder desta forma, atuando junto às comissões investigativas. Além disso, a capacitação da equipe deve ser uma das principais metas.

O ato administrativo de criação da ETIR também deve nomear os responsáveis pelo encaminhamento de denúncias externas e internas.

A ETIR deve ter a prerrogativa de solicitar o bloqueio temporário de acesso à rede ou sistemas de informação por medida preventiva quando ocorrerem incidentes de segurança, visando minimizar o impacto à UFABC, sempre com a ciência do usuário.

6.1.3.1 Estatísticas de Incidentes de SIC

De acordo com o levantamento realizado entre 2015 e 2016, o GT identificou a ocorrência de 9648 incidentes de SIC, sendo que 98% dos casos foram de vírus com severidade alta ou crítica. Estes vírus foram tratados pelo software de proteção de *endpoint*, popularmente conhecido como software antivírus, que hoje em dia engloba outras funções de segurança, como a prevenção de intrusões locais, *antispam*, *firewall* local, entre outros. Neste levantamento, não foram considerados os registros de bloqueios automáticos do *firewall de borda* que previne a rede contra ataques externos. Deste total, 234 incidentes foram reportados como *spam* ou tentativa de *phishing,* e encaminhados ao e-mail abuse@ufabc.edu.br. Além disso, 31 incidentes necessitaram intervenção dos servidores das divisões de redes, data center e suporte do NTI para investigar a causa e restaurar o ambiente. As categorias de ataques que mais se repetiram foram:

- Pichação de Site;
- *Infecção por Botnets*;
- Mineração de *Bitcoins;*
- *Spams;*
- Perda de dados (não intencional);

- Ataque de negação de Serviço;

Com relação aos vírus detectados, 68% dos casos tiveram como alvo a Prograd e 29% a Proap no período mencionado.

6.1.4 Eixo Gestão de Riscos

A PoSIC de 2013 faz menção à gestão de riscos de TIC apenas no planejamento estratégico, sendo tratada com enfoque de alto nível para as aquisições de TI. O Plano Diretor de Tecnologia da Informação faz uso da metodologia de priorização de problemas GUT e da conhecida metodologia de análise de gestão, a análise SWOT, que inclui a análise dos pontos fortes, fraquezas, oportunidades e ameaças do ambiente de TIC da UFABC, mas não detalha as vulnerabilidades técnicas.

O processo de Gestão de Riscos de Tecnologia da Informação e Comunicação, que inclui a avaliação de controles de segurança da informação, foi consolidado e validado pelo escritório de processos do NTI. No entanto, para iniciar a sua execução é necessária a criação de uma estrutura gerencial para os riscos. A alta administração deve nomear um Gestor de Riscos com as atribuições previstas na norma complementar nº 04/DSIC/GSI/PR, ou incluir nas atribuições do Gestor de Segurança da Informação.

Na PoSIC, o GT incluiu novas diretrizes que norteiam a escolha de uma metodologia de gestão de riscos aderente às normas complementares do DSIC e à ISO 27005:2008. Além disso, o GT recomenda que as áreas avaliem o custo benefício da adoção de controles para o tratamento do risco, com apoio do Gestor de Riscos.

6.1.5 Eixo Gestão da Continuidade do Negócio

A UFABC nunca elaborou um plano de continuidade de negócios, apesar de ter sido previsto na PoSIC de 2013. O GT considera importante identificar a criticidade dos ativos de informação, sendo recomendado que o Gestor de Segurança da Informação defina os critérios de priorização e impacto. Além disso, o GT recomenda a formalização de uma política de backup (cópia de segurança) que defina periodicidade, prioridades na guarda de dados e tecnologia empregada. O NTI aguarda o processo de contratação de solução de armazenamento para definir esta política.

6.1.6 Eixo Auditoria e Conformidade

O GT achou adequado remover da PoSIC de 2013 a diretriz que previa a criação de uma comissão de auditoria interna para a avaliação da conformidade de segurança da informação. A responsabilidade deste processo deve ser do Gestor de Segurança da Informação. As não-conformidades relativas ao descumprimento de legislações, normas e procedimentos devem ser identificadas e tratadas como riscos de segurança da informação. Sempre que possível, a avaliação de conformidade deve ser suportada por sistemas automatizados de detecção de logs, vulnerabilidades e controle de ativos.

6.1.7 Eixo Tratamento da Informação

Algumas diretrizes sobre o tratamento da informação foram incluídas na nova minuta da PoSIC para esclarecer o seu objetivo e referenciar a legislação atual, além de explicar a importância de se proteger as informações de acordo com o seu nível de sensibilidade e criticidade. Entendemos que as informações sigilosas devem possuir proteção adequada fornecida pelo NTI. No entanto, cada usuário permanece responsável pelo seu compartilhamento ou guarda, já que é o proprietário ou custodiante da informação.

O GT discutiu amplamente o uso de contas de e-mails e serviços de TIC que armazenam dados fora do território brasileiro. O uso destes serviços, fornecidos pela empresa Google, por exemplo, viola o decreto 8.135 de novembro de 2013, que dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. De forma resumida, este decreto restringe o uso de serviços de nuvem computacional em território estrangeiro para o armazenamento de dados.

O GT também discutiu o uso sustentável da pasta compartilhada na rede da UFABC, dada à capacidade limitada de armazenamento eletrônico na UFABC. Mesmo assim, o GT incluiu regras preconizadas pelo CONARQ sobre a temporalidade de guarda de arquivos, de acordo com a sua resolução nº 40/2014. Também foram considerados os procedimentos para a salvaguarda de documentos sigilosos e classificados, dada pela Lei de Acesso a Informação (Lei 12.527/2011).

6.1.8 Eixo controle de acesso

A PoSIC de 2013 contempla o controle de acesso físico e lógico de forma incipiente. O GT incluiu diretrizes que definem o objetivo do controle de acesso, requisitos para a concessão de acesso e critérios para a concessão de privilégio de acesso. Foram ainda discutidas outras possibilidades de diretrizes referentes ao controle de acesso: autenticação a rede sem fio, gestão de identidade e acesso, procedimentos para proteção de documentos eletrônicos, gerenciamento de senhas e registros de auditoria (logs), procedimentos para privilégios de acesso, entre outras questões que foram incluídas nas minutas das normas complementares à PoSIC.

6.1.9 Eixo Aquisição e Desenvolvimento de Sistemas

Com o uso intensificado de softwares e hardwares específicos para prover níveis de segurança adequados às informações, novas formas de ataques também foram elaboradas para transpor essa barreira. Atualmente, o foco concentra-se na exploração de vulnerabilidades nas aplicações desenvolvidas para o ambiente online, uma vez que muitas não implementam as boas práticas de codificação, ou não foram objeto de um processo de desenvolvimento suportado por testes que validem os controles aplicados.

Grande parte dessas vulnerabilidades de segurança ocorrem em consequência de falhas que podem ser introduzidas durante o ciclo de desenvolvimento de um sistema.

A norma complementar nº. 16/IN01/DSIC/GSIPR fornece diretrizes para o desenvolvimento e obtenção de software nos órgãos da administração pública federal. A norma recomenda que os requisitos de segurança devem ser definidos logo no início de qualquer projeto de desenvolvimento de software. O GT verificou que essa e outras recomendações já são observadas pela equipe de desenvolvimento do NTI, mas esses procedimentos ainda estão sendo formalizados. Diretrizes que promovem as boas práticas para o desenvolvimento seguro de softwares e sistemas foram incluídas na minuta da atualização da PoSIC.

6.1.10 Eixo uso de E-mail, Internet e Recursos de TIC

As diretrizes sobre o uso de ativos de informação expostas na PoSIC de 2013 contemplam em linhas gerais a utilização de e-mail, internet e computadores. Com efeito, durante as reuniões, foram levantadas necessidades específicas em relação ao uso de cada um desses recursos. Em conformidade com essas diretrizes, pode-se ressaltar que a UFABC já possui uma norma de uso de e-mail vigente, um documento separado de sua política de segurança que complementa suas diretrizes. O conteúdo dessa norma de e-mail observa as diretrizes gerais da política e pontua normas e procedimentos de acordo com a capacidade tecnológica do sistema de e-mail, bem como as suas ferramentas de acesso. Porém, deve-se ressaltar que as diretrizes expressas na PoSIC são substratos efetivos para que os membros da comunidade acadêmica consigam nortear o uso dos ativos de informação de forma consciente, de acordo com o seu papel na comunidade.

6.1.11 Eixo Redes Sociais

O GT entende que as diretrizes para as redes sociais estão relacionadas às diretrizes de proteção de ativos de informação, sendo que as regras de predominancia tática e operacional devem ser definidas em uma norma específica. Desta forma, o GT produziu uma minuta contendo as normas para uso seguro das redes sociais em conjunto com a Assessoria de Comunicação e Imprensa (ACI), que corrobora o guia de boas práticas já existente em sua página. Em resumo, as regras tratam da responsabilidade pela criação e gestão de perfis institucionais e da criação de campanhas de conscientização no uso das redes sociais.

6.2 2ª fase

6.2.1 Estruturação

Na segunda fase do GT, que ocorreu entre setembro de 2017 e maio de 2018, a Comissão Executiva se reuniu em sete oportunidades e realizou diversas rodas de conversas com as áreas envolvidas. Além disso, em maio de 2018, foi realizada mais uma consulta a Procuradoria Federal da UFABC.

O GT iniciou o desenvolvimento das minutas das normas temáticas abrangendo os aspectos táticos e operacionais da sua implantação. Neste período, a Comissão Consultiva protagonizou as principais atividades e recebeu a colaboração de servidores do NTI que apresentaram soluções com foco em infraestrutura de redes, suporte técnico e uso de sistemas.

Foram produzidas 6 (seis) minutas de normas temáticas para os recursos de TIC, descritas a seguir:

- Norma para uso seguro da Internet e rede sem fio da UFABC
- Conjunto de normas para uso seguro de serviços de rede e tecnologia web
- Norma de utilização segura das redes sociais da UFABC
- Norma para uso seguro de computadores e softwares da UFABC
- Norma para controle de acesso lógico e físico ao ambiente de TIC na UFABC
- Norma para o tratamento seguro da informação eletrônica para as atividades meio da UFABC

Além disso, o GT propôs alterações na norma de uso seguro do correio eletrônico e listas de mails institucionais da UFABC, em vigor através da Portaria da Reitoria nº 471 de 16 de novembro de 2016 e publicada no Boletim de Serviço nº 605 de 18 de Novembro de 2016. As alterações foram realizadas pelos servidores da área de suporte técnico do NTI que diagnosticaram inconsistências operacionais.

As minutas das normas seguem uma estrutura padronizada de organização de conteúdo disponibilizada da seguinte forma:

- Referencial normativo;
- Abrangência da norma;
- Objetivo;
- Glossário;
- Regras para o usuário;
- Regras específicas para o NTI;
- Disposições gerais.

A ordem não é mandatória e a estrutura não é obrigatória, mas ajudou o GT a organizar o desenvolvimento das minutas.

6.3 Referencias técnicas e normativas para as normas temáticas de segurança da UFABC

6.3.1 Norma para o uso seguro da Internet e rede sem fio da UFABC

Para composição desta minuta, o GT teve como base os seguintes documentos:

Norma ABNT ISO IEC 27002 de 2005 - Estabelece o Código de Prática para a Gestão de Segurança da Informação, que tem como objetivo “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização”.

(Item 7.1.3; Uso aceitável dos ativos).

> “Convém que todos os funcionários, fornecedores e terceiros sigam as regras para o uso permitido de informações e de ativos associados aos recursos de processamento da informação, incluindo: a) regras para o uso da internet e do correio eletrônico (ver 10.8)”;

Diretrizes da Política de Segurança da Informação para o uso de ativos de informação - PoSIC 2013 - UFABC.

(item VII; art. 7º; quanto ao uso dos ativos de informação):

> “a) observar a premissa geral de que os recursos computacionais devem ser utilizados de maneira responsável, devendo este uso estar alinhado prioritariamente com os objetivos educacionais, de pesquisa, extensão, administrativos e gerenciais da Universidade”;

Norma Complementar nº 07/IN01/DSIC/GSIPR - Esta norma estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação na Administração Pública Federal.

(Item 5.3; Quanto aos ativos de informação):

> 5.3.7 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso da Internet, do Correio Eletrônico e de Mensagens Instantâneas.

Resolução nº 12 do ConsUni - UFABC - Aprova as Normas de Uso e Políticas Gerais de Segurança da Universidade Federal do ABC (UFABC)

(Capítulo VI, Sessão II artigo nº 33; Normas para o Administrador):

> Cabe ao administrador zelar pelo bom funcionamento da rede observando o seguinte: I - Caso haja necessidade eminente, fazer uso de ferramentas para monitorar a rede da Unidade.
>
> II - Comunicar imediatamente ao NTI a ocorrência de invasões ("hackers", "lammers", "crackers", etc.), tomando as medidas de desconexão da rede e correção das falhas.

> III - Proteger os serviços de rede utilizando ferramentas apropriadas, como "firewall", "Proxy", Sistemas de Detecção de Intrusão, etc,
>
> VIII - Bloquear e notificar ao NTI sobre os serviços que possam comprometer o desempenho da rede ou infringir qualquer item da norma.

Rede Ipê: Política de Uso - Apresenta as condições e políticas de uso aceitável da rede Ipê

(Capítulo 4, Condições de Uso):

> As Organizações Usuárias podem utilizar os Serviços de Redes disponíveis (…), exceto nas seguintes condições: produção ou transmissão de dados ou materiais considerados ilegais, entre outros, por caracterizarem: transgressão dos direito do autor, de proteção à criança e ao meio-ambiente; atentado à privacidade ou promoção à discriminação racial ou religiosa; veiculação de propaganda comercial, política ou religiosa; transmissão de mensagens ou material de propaganda não solicitadas pelo destinatário; uso em atividades estritamente comerciais; atividades que contribuam para ineficiência ou esgotamento dos recursos na rede, sejam eles computacionais, comunicacionais ou humanos; atividades que promovam a corrupção ou destruição de dados de usuários; atividades que interrompam ou prejudiquem a utilização dos Serviços de Rede por outros usuários; interligação ou abrigo em seu espaço de endereçamento de uma terceira instituição sem qualificação obtida através desta Política de Uso.

E por fim,

Norma Complementar nº 07/IN01/DSIC/GSIPR - Esta norma estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação na Administração Pública Federal.

(Item 5.2 Quanto à rede corporativa de computadores):

> 5.2.5 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.

6.3.2 Conjunto de normas para o uso seguro de serviços de rede e tecnologia Web

Para composição desta minuta, o GT teve como base os seguintes documentos:

Norma ABNT ISO IEC 27002 de 2005 - Estabelece o Código de Prática para a Gestão de Segurança da Informação, que tem como objetivo “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização”.

(Item 11.4.2 Autenticação para conexão externa do usuário).

Controle: Convém que métodos apropriados de autenticações sejam usados para controlar acesso de usuários remotos.

(Item 10.6.1 Controles de redes).

Controle: Convém que as redes sejam adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.

b) as responsabilidades e procedimentos sobre o gerenciamento de equipamentos remotos, incluindo equipamentos em áreas de usuários, sejam estabelecidos;

c) os controles especiais sejam estabelecidos para proteção da confidencialidade e integridade dos dados trafegando sobre redes públicas ou sobre as redes sem fio (wireless) e para proteger os sistemas e aplicações a elas conectadas; controles especiais podem também ser requeridos para manter a disponibilidade dos serviços de rede e computadores conectados;

(Item 10.9.3 Informações publicamente disponíveis).

Convém que haja um processo formal de aprovação antes que uma informação seja publicada. Adicionalmente, convém que todo dado de entrada fornecido por fontes externas ao sistema seja verificado e aprovado.

- ✓ E por fim,

Resolução nº 12 do ConsUni - UFABC - Aprova as Normas de Uso e Políticas Gerais de Segurança da Universidade Federal do ABC (UFABC)

(Capítulo VII, artigo 35; Normas para uso de Serviços de Acesso Remoto):

São normas do Serviço de Acesso Remoto: I - Ser aluno, devidamente autorizado pelo professor responsável, ou técnico administrativo da Universidade, devidamente autorizado pelo seu superior hierárquico; II - Cadastrar nome de usuário e senha junto ao NTI;

Além disso, o GT realizou diversas pesquisas em materiais de boas práticas e normas de outras instituições.

6.3.3 Norma para controle de acesso lógico e físico ao ambiente de TIC na UFABC

Para composição desta minuta, o GT teve como base os seguintes documentos:

Norma Complementar nº 07/IN01/DSIC/GSIPR - Esta norma estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação na Administração Pública Federal.

(Item 5.3: Quanto aos ativos de informação):

> 5.3.2 Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

(Item 5.2 Quanto à rede corporativa de computadores):

> 5.2.3 Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em cada órgão ou entidade da APF.
>
> 5.2.4 Implementar, sempre que possível, pelo menos um dos mecanismos que contemplam biometria, tokens, smart cards, a fim de autenticar a identidade do usuário da rede.
>
> 5.2.6 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.
>
> 5.2.7 Utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.
>
> 5.2.8 Gravar o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;

Norma ABNT ISO IEC 27002 de 2005 - Estabelece o Código de Prática para a Gestão de Segurança da Informação, que tem como objetivo “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização”.

(Item 11.2 Gerenciamento de acesso do usuário).

11.2.1 Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.

11.2.2 Convém que a concessão e o uso de privilégios sejam restritos e controlados.

11.2.4 Convém que o gestor conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.

6.3.4 Norma de utilização segura das redes sociais da UFABC

Para composição desta minuta, o GT teve como base os seguintes documentos:

Norma Complementar nº 15/IN01/DSIC/GSIPR - Esta norma estabelece diretrizes para o uso seguro das redes sociais na administração pública federal

(Item 5: Princípios e Diretrizes):

5.2 A normatização interna de uso seguro das redes sociais deve estar alinhada tanto à Política de Segurança da Informação e Comunicações (POSIC) quanto aos objetivos estratégicos do órgão ou entidade. Também deve estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais, por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social, a partir da infraestrutura das redes de computadores da APF.

6.3.5 Norma para uso seguro de computadores e softwares da UFABC

Para composição desta minuta, o GT teve como base os seguintes documentos:

Norma ABNT ISO IEC 27002 de 2005 - Estabelece o Código de Prática para a Gestão de Segurança da Informação, que tem como objetivo “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização”.

(Item 10.4 Proteção contra códigos maliciosos e códigos móveis).

10.4.1 Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

(Item 11.5 Controle de acesso ao sistema operacional).

11.5.2 Convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário.

11.5.4 Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado

Resolução nº ConsUni nº 12 - UFABC - Aprova as Normas de Uso e Políticas Gerais de Segurança da Universidade Federal do ABC (UFABC)

(Capítulo IV, artigo 18; Normas para Uso de Computadores da UFABC):

Os diversos computadores pessoais da UFABC e sob responsabilidade dos usuários, conectados ou não rede da UFABC, devem seguir normas de forma a minimizar os problemas com relação à perda de informação e comprometimento das atividades acadêmicas, científicas e administrativas da Universidade

(Capítulo V, Sessão IV artigo nº 30; Das Infrações e penalidade):

São consideradas infrações no uso dos recursos computacionais oferecidos:
I - Fornecer as senhas de acesso a externos, utilizar a senha de outro usuário sem seu consentimento e devida autorização;
II - Utilizar os recursos oferecidos com fins comerciais não autorizados explicitamente;
III - Utilizar software ou procedimentos para conseguir acesso não autorizado a recursos ou informações, ou para degradar o desempenho, ou para colocar fora de operação sistemas computacionais locais ou remotos;
IV - Armazenar arquivos de conteúdo ilegal ou considerados abusivos;

6.3.6 Norma para o tratamento seguro da informação eletrônica para as atividades meio da UFABC

Para composição desta minuta, o GT teve como base os seguintes documentos:

Medida Provisória nº 2.200-2 - Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

(Artigo 10):

§ 1o As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação

aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.

§ 2o O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Lei nº 12.682 - Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.

Art. 3o O processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP - Brasil.

Art. 6o Os registros públicos originais, ainda que digitalizados, deverão ser preservados de acordo com o disposto na legislação pertinente.

Lei nº 12.527 - Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

Art. 6o Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:

I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;

II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e

III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Decreto nº 8.135 - Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos

por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.

§ 4º O armazenamento e a recuperação de dados a que se refere o caput deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal.

Norma Complementar nº 20/IN01/DSIC/GSIPR - Esta norma estabelece diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da administração pública federal

6.1.5 Na fase da produção e recepção de informações, os órgãos e entidades da APF deverão verificar se as informações por eles produzidas ou custodiadas se enquadram em quaisquer hipóteses de sigilo especificadas na Lei 12.527/2011 ou em legislações específicas - tais como aquelas referentes aos sigilos legal, fiscal e bancário, ao segredo industrial ou de justiça (conforme Anexo B) -, a fim de adotar as medidas cabíveis quanto ao seu tratamento.

Norma Complementar nº 14/IN01/DSIC/SCS/GSIPR - Esta norma estabelece diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da administração pública federal

(Artigo 5.2; Sobre tratamento da informação):

5.2.1 Informação sem restrição de acesso: Pode ser tratada, a critério da entidade da APF em ambiente de computação em nuvem (…).
5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem

5.4 Os dados, metadados, informações e conhecimento, produzidos ou custodiados por entidade da APF, referente à Documento com restrição de acesso prevista em legislação, Documento preparatório e Informação Pessoal, devem residir exclusivamente em território brasileiro

Além disso, o GT realizou diversas pesquisas em materiais de boas práticas e normas de outras instituições como fonte de conhecimento.

7 Conclusão

O GT concluiu que a UFABC pode melhorar as questões relacionadas a segurança da informação através de medidas administrativas e através da discussão e

aprovação de uma politica que seja mais esclarecedora e adequada a comunidade acadêmica e suas atividades.

As propostas desse GT referentes à politica de segurança da informação e comunicação e as normas complementares formam, juntamente ao relatório de atividades desse GT, a base sob a qual o CETIC deve discutir o assunto.

Esse relatório possui de forma sintetizada a legislação sob a qual os órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação estão submetidos. E também possui o histórico de consultas a diversos membros dos setores da UFABC, bem como as suas observações enquanto representantes das suas respectivas áreas.