Centro de Tecnologia da Informação e Comunicação - CTIC

Parecer técnico sobre o relatório do TCU

Idelvandro Fonseca

31 de jul de 2023

1 Introdução

Nota: Este documento utiliza a classificação TLP (*Traffic Light Protocol*), padrão global para facilitar o compartilhamento mais amplo de informações potencialmente sensíveis e a colaboração mais efetiva.

Classificação: **TLP:AMBER**: Divulgação limitada, destinatários só podem comparilhá-la para aqueles que necessitam saber (*need-to-know basis*) dentro de sua própria organização e com seus clientes.

Conforme item 6.16 presente no Plano Diretor de Tecnologia da Informação e Comunicação 2022/2024, o Departamento de Segurança da Informação - DESI, hierarquicamente ligado ao CTIC através da Divisão de Redes e Serviços de Internet, é o setor responsável por:

1. Contribuir com a elaboração e atualização do Sistema de Gestão de Segurança da Informação (SGSI) e da Política de Segurança da Informação e Comunicação (PoSIC) e acordo com normas técnicas vigentes;
2. Promover implementação, análise crítica, monitoramento e constante melhoria do SGCI e PoSIC;
3. Realizar o tratamento de incidentes de segurança da informação e gestão de vulnerabilidades nos serviços de TIC providos pelo CTIC;
4. Promover a gestão de conformidade no contexto dos serviços de TIC da Unifesspa.

Dentro das atribuições do Departamento, encontram-se as ações de SIC executadas no âmbito institucional, como:

- Coordenar equipe de resposta e tratamento de incidentes em redes – ETIR;
- Gerência, configuração e monitoramento dos *appliances firewall next-generation* da sede e dos Campi fora de sede (Rondon, Xinguara, São Félix, Santana);
- Gerência, configuração e monitoramento do software *endpoint* Kaspersky Antivírus;
- Gestão dos incidentes de segurança reportados pelo CAIS (Centro de Atendimento a Incidentes de Segurança) – RNP, através da ferramenta SGIS.

2

Análise dos *feedbacks*

O Departamento de Segurança da Informação apresenta este relatório dando ciência ao **Relatório Individual de *Feedback*** entregue pelo TCU, com observações, análises e respostas da avaliação feita pelo órgão. O TCU avaliou as medidas básicas dos seguintes controles:

- Inventário e controle de ativos corporativos;
- Inventário e controle de ativos de *software*;
- Gestão contínua de vulnerabilidade;
- Conscientização sobre segurança e treinamento de competências;
- Gestão de respostas a incitantes;

Pretende-se com este relatório apresentar uma avaliação e perspectivas futuras para os itens avaliados, com o objetivo de melhorá-los.

2.1 INVENTÁRIO E CONTROLE DE ATIVOS CORPORATIVOS

Os controles dos ativos são realizados com os equipamentos e *softwares* disponíveis na Instituição. Todos os ativos são cadastrados e monitorados de maneira automatizada por ferramentas livres e gatilhos são configurados para que em caso de perda de conexão a equipe seja informada.

Os dispositivos móveis e de IoT (*Internet of Things*) não constam em nossos controles, o segundo por não ser tão frequente ficou fora do radar da equipe. Os celulares e computares portáteis, apesar de não terem cadastro, tem suas atividades registradas em nosso *firewall*, pois para o acesso desses dispositivos na rede é necessário a utilização de usuário e senha cadastrados em nossas bases de dados.

Para futuras ações de melhoria, esta equipe carece de capital humano e recursos para aquisição de ferramentas modernas e que tratem de forma adequadas todos os dispositivos conectados na nossa rede de dados.

2.2 INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

A UNIFESSPA utiliza controlador de domínio para todos os computadores institucionais, com isso, se tem a lista de *softwares* instalados, com suas versões, ultimas atualizações e etc. Para que todo o parque fique *compliance* sem que versões diferentes dos mesmos *softwares* sejam instalados, se faz uso de *Group Policy Object* - GPO, que nada mais é do que é um conjunto de configurações que permite personalizar

recursos dos usuários e dos computadores em ambientes *Windows*.

A Universidade por utilizar esse mecanismo tem controle de tudo que é instalado nos computadores institucionais, não permitindo que *softwares* não homologados sejam inseridos na rede sem a autorização do setor de TI. Para que outros controles sejam realizados, nos faltam capital humano e recursos financeiros para que novas soluções automatizadas sejam adquiridas e implementadas.

2.3 GESTÃO CONTÍNUA DE VULNERABILIDADE

Apesar de não ter um processo de gestão de vulnerabilidade formalmente escrito e aprovado, o DESI realiza atividades que visam mitigar possíveis comprometimentos de seus ativos ativos de *hardware* e *software*. São realizadas verificações automatizadas por ferramentas específicas e estas por sua vez, quando possível, realizam ações também automatizadas com a finalidade de corrigir ou alertar os administradores dos sistemas.

Com falta de capital humano, tenta-se suprir esta escassez com ferramentas que possam realizar mais tarefas automáticas como sistemas SIEM - *Security Information and Event Management*, analisando os registros e *logs* de eventos de tudo o que acontece na infraestrutura. Rotinas com *scripts* de atualização de segurança são executados continuamente nos servidores, visando mantê-los mais atualizado possível com os *patchs* de segurança disponibilizados pelos sistemas operacionais.

Outros verificadores de integridade de sistemas são utilizados, como analisadores de imagens e pacotes utilizados nas aplicações. Fontes públicas e privadas sobre ameaças e vulnerabilidades são consultadas, bem como quando notificados CAIS as medidas são tomadas.

2.4 CONSCIENTIZAÇÃO SOBRE SEGURANÇA E TREINAMENTO DE COMPETÊNCIAS

Sobre conscientização e treinamento sobre o tema de cybersegurança, apensar de esforços pontuais como criação de cartilhas e boletins de segurança bimestrais e de um evento voltado para o tema, hoje não é possível realizar essas atividades vide a escassez de capital humano e financeiro dentro da instituição.

Para reforçar o dito acima, apenas um servidor compõe o setor de segurança da informação na instituição, o que sobrecarrega o departamento e enfraquece este tama dentro do órgão.

2.5 GESTÃO DE RESPOSTAS A INCITANTES

A Universidade Federal do Sul e Sudeste do Pará - Unifesspa, através do Comitê de Governança Digital – CGD, instituiu no dia 20 de março de 2018 a criação da Equipe de Tratamento e Resposta a Incidentes em Redes de Computadores – ETIR. Todos os membros que compõem a equipe seguem a recomendação da Norma Complementar 05/IN01/DSIC/GSIPR, que recomenda que a formação da equipe seja composta por: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas da organização com conhecimento técnico comprovado.

Apesar de existir uma equipe de ETIR, estes não tem sua dedicação exclusiva para esta atividade, assim como citado nos outros tópicos a escassez de força de trabalho não permite que todos dediquem-se apenas para esse fim, o que acaba afetando controles como revisão de contatos de interessados, estabelecer responsabilidades, e compor toda cadeia de ações necessárias para uma resposta mais rápida e eficiente.

3 Conclusões

A Unifesspa possui diversos mecanismos de proteção e detecção no âmbito da segurança da informação conforme demonstrado ao longo deste documento, adota-se ainda de maneira parcial alguns dos controles medidos pelo TCU. Mesmo com sua equipe insuficiente o Centro de Tecnologia da Informação - CTIC e o DESI, inovam com soluções de detecção de ameaças, registros de *logs*, *backups*, entre outros, buscando sempre por soluções livres devido a falta de recursos financeiros.

O ano de 2024 reserva novos desafios e perspectivas para o Departamento de Segurança da Informação, com a realizações de ações como *workshop* e *webinar* a serem planejadas, assim como a retomada da divulgação dos boletins de segurança da informação com o intuito da conscientização em SIC.

Novos mecanismos e métodos são constantemente estudados, boas práticas adotadas, sempre em busca do aprimoramento dos processos e melhoria constante.

Emitido em 01/08/2023

RELATÓRIO Nº 984/2023 - DESINF (11.12.15)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 01/08/2023 09:51)
IDELVANDRO JOSE DE MIRANDA FONSECA
CHEFE DE DEPARTAMENTO
2139800

Para verificar a autenticidade deste documento entre em https://sipac.unifesspa.edu.br/documentos/ informando seu número: **984**, ano: **2023**, tipo: **RELATÓRIO**, data de emissão: **01/08/2023** e o código de verificação: **9f0fa5bb2a**