Universidade Federal Fluminense

RELATÓRIO DE AUDITORIA

RA Nº 002/2023

Proc. º 23069.191413/2022-19

Junho – 2023

Serviço Público Federal

Poder Executivo

Ministério da Educação

Universidade Federal Fluminense

Conselho de Curadores

Auditoria Técnica

Relatório de Auditoria - RA

Tipo: Auditoria Operacional

Atividade do PAINT 2022: 012 SAUD – Avaliação da infraestrutura de segurança da informação.

Auditoria Interna Governamental[1]

Atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Deve buscar auxiliar as organizações públicas a realizarem seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

Auditoria Operacional[2]

A auditoria operacional é uma atividade que fornece análises objetivas para auxiliar a administração a melhorar seu desempenho e suas operações, reduzir custos, facilitar a tomada de decisões e de medidas corretivas pelas partes responsáveis.

[1] IN SFC nº 03, de 2017

[2] Manual de Orientações Técnicas - CGU

“Aquilo que torna as pessoas vulneráveis também as torna lindas.”

Brené Brown.

RESUMO

Realizamos uma auditoria operacional na Superintendência de Teconologia da Informação – STI, para avaliar a infraestrutura de segurança da informação existente. A origem desse trabalho deve-se à previsão no Plano Anual de Atividades da Auditoria Interna – PAINT 2022 e, conforme demonstrado no Relatório de Atividades de Auditoria Interna de 2022, não foi possível sua conclusão no exercício planejado.

A escolha do tema foi baseada em análise de riscos. Em decorrência da Estratégia Global de Auditoria – EGA, onde determina que em todos os trabalhos de avaliação no exercício de 2022 devam constar análises e testes sobre Termo de Execução Descentralizada - TED, foi questionado à unidade sobre a existência de projetos e/ou programas financiados com recursos de TED.

LISTA DE FIGURAS e ANEXOS

FIGURAS

QUADROS

ANEXOS

LISTA DE SIGLAS E ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

AGU – Advocacia Geral da União

ANPD – Autoridade Nacional de Proteção de Dados

APF - Administração Pública Federal

AT/CUR - Auditoria Técnica/ Conselho de Curadores

CBMERJ – Corpo de Bombeiros Militar do Estado do Rio de Janeiro

CGU – Controladoria Geral da União

CIS – *Center for Internet Security*

CSI – Comitê de Segurança da Informação

CUR - Conselho de Curadores da UFF

CUV - Conselho Universitário da UFF

EGA – Estratégia Global de Auditoria

ETIR – Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

GSI/PR – Gabinete de Segurança Institucional da Presidência da República

IA – Inteligência Artificial

IDUFF – Sistema de Identificação Única da UFF

IFES - Instituição Federal de Ensino Superior

LGPD – Lei Geral de Proteção de Dados Pessoais

MEC – Ministério da Educação

MRC – Matriz de Riscos e Controles

NBR ISO – Normas Brasileiras – Organização Internacional para Padronização

PAINT - Plano Anual de Atividades de Auditoria Interna

PCN – Plano de Continuidade de Negócios

PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação

PDU – Plano de Desenvolvimento da Unidade

PNSI – Política Nacional de Segurança da Informação

PPSI – Programa de Privacidade e Segurança da Informação

PSCIE - Processo de Segurança Contra Incêndio e Emergências

RA - Relatório de Auditoria

RI – Regimento Interno

SA – Solicitação de Auditoria

SGD – Secretaria de Governo Digital

SISP - Sistema de Administração dos Recursos de Tecnologia da Informação

SLA - *Service Level Agreement*

STI – Superintendência de Teconoloda da Informação

TCU – Tribunal de Contas da União

TED – Termo de Execução Descentralizada

UFF – Universidade Federal Fluminense

SUMÁRIO

1. INTRODUÇÃO

A pandemia causada pela covid-19 forçou as organizações a expandir rapidamente o regime de trabalho remoto, o que aumentou a quantidade de acessos externos às redes e o número de incidentes relacionados a ataques cibernéticos, em especial por meio de códigos maliciosos. Para se ter uma ideia, o Brasil foi o quinto país do mundo com maior incidência de ataques de *ransomware* (“sequestro” de dados). Os ataques dispararam em 2020 e aumentaram 90% em 2021 (TCU, 2022).

Nos últimos anos o Governo vem utilizando cada vez mais a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão.

Nesse contexto, as instituições federais coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais.

As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor (TCU, 2020)

O presente trabalho apresenta os resultados da auditoria operacional realizada na Superintendência de Tecnologia da Informação – STI com o foco na avaliação da infraestrutura de segurança da informação, com o objetivo de avaliar a atual capacidade da instituição em evitar e mitigar os eventos de riscos passíveis de ocorrer na operação dos diversos sistemas da UFF.

1.1 Metodologia

Para o planejamento e execução desta auditoria, foi elaborado matriz de riscos e controles – MRC, para identificação dos riscos mais relevantes nos

processos de segurança da informação da STI e seus respectivos controles internos.

Para responder as *questões de auditoria* foram utilizadas diversas técnicas de auditoria, tais como:

- ✓ Visitas técnicas;
- ✓ Levantamento e análise da legislação aplicada;
- ✓ Reuniões com os gestores da STI;
- ✓ Emissão de Solicitação de Auditoria – SA;
- ✓ Análise documental;
- ✓ Registro fotográfico;
- ✓ Avaliação de controles internos;
- ✓ Identificação e avaliação de riscos (*BowTie*);
- ✓ Elaboração de planilhas eletrônicas para análise dos dados.

1.2 Limitações e restrições

Devido a falta de experiência da equipe em auditorias operacionais de sistemas de informação o escopo do trabalho foi reduzido. Não analisamos os riscos de segurança da informação inerentes aos periféricos. Não avaliamos o PDTIC-UFF em função de ação, sobre esse objeto, prevista no PAINT.

Apesar de tecer considerações pontuais sobre determinados processos de informação, não foi contemplado, neste trabalho, a avaliação dos impactos da LGPD nos sistemas de informação da UFF.

1.3 Unidade auditada

A Superintendência de Tecnologia da Informação – STI está situada no *Campus* da Praia Vermelha, São Domingos – Niterói. O *Data Center* está localizado no Campus Valonguinho, Centro – Niterói.

A unidade informou que seu Regimento Interno está em fase final de elaboração para a aprovação pelo Conselho Universitário – CUV. Foi enviada minuta que consta como finalidade:

> " [...] assessorar a Universidade, o Reitor e os órgãos competentes em assuntos relacionados às políticas, diretrizes e supervisão dos recursos e das atividades internas de tecnologia da informação, comunicação de dados e de voz no âmbito da Universidade Federal Fluminense.

A estrutura organizacional da unidade configura-se da seguinte maneira, conforme a Portaria 65.098/2019 – UFF:

- Coordenação Técnica - CTE/STI
  - Divisão de Suporte à Rede - DSRE/CTE
  - Divisão de Telefonia - DTEL/CTE
- Coordenação de Desenvolvimentos de Sistemas - CDS/STI
  - Divisão de Qualidade de Dados e Sistemas - DQDS/CDS
  - Divisão de Exibição - DEX/CTV
- Gerência Operacional Financeira da STI - GOF/STI
- Gerência de Desenvolvimento de Novas Tecnologias - GDTN/STI
- Gerência de Governança e Segurança da Informação - GGSI/STI
- Gerência de Relacionamento Externo - GRE/STI

1.4 Visão geral do objeto de auditoria

A Política nacional de Segurança da Informação – PNSI[3], abrange a segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais.

O Programa de Privacidade e Segurança da Informação - PPSI[4], define segurança da informação como ações que objetivam viabilizar e assegurar a:

- ✓ ***Disponibilidade*** - Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem éde direito;
- ✓ ***Integridade*** - Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos

[3] Decreto 10.641/2021 que altera o Decreto 9.637/2018.

[4] PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023

dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital;

- ✓ ***Confidencialidade*** - Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento;
- ✓ ***Autenticidade*** - Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

Na UFF, a Coordenação de Infraestrutura, Conectividade e Segurança da Informação é responsável pela coordenação das áreas de infraestrutura de TI da STI e por questões relacionadas à Segurança da Informação. Subdivide-se nas seguintes áreas: (i) Divisão de redes; (ii) Divisão de suporte técnico; e (iii) Divisão de telefonia.

2 – RESULTADOS

Apresentamos a seguir os resultados das avaliações sobre os controles internos da gestão que tratam do framework da segurança da informação utilizado pela UFF.

2.1 Estrutura de Segurança da Informação

Segundo a NBRISO/IEC 27005 – Gestão de riscos de segurança da informação, existem dois tipos de ativos na instituição:

- ✓ Ativos primários:
  - Processos e atividades;
  - Informação.
- ✓ Ativos de suporte (sobre os quais os elementos primários se apoiam).
  - *Hardware;*
  - *Software;*

- Rede;
- Instalações físicas;
- Recursos humanos;
- Estrutura da organização.

A estrutura de suporte da STI é composta por (Anexo II):

- ✓ Servidores;
  - E-mail, Filtro de *Spam*;
  - *Backup;*
  - Banco de dados (desenvolvimento e produção);
  - SQL, *Docker;*
  - *Storage* e *Data Domain.*
- ✓ *Firewall;*
- ✓ Robô de fita;
- ✓ *Hubs, Switches;*
- ✓ *Data Center (*sala segura);
- ✓ Instalações; e
- ✓ Recursos humanos.

A STI opera a plataforma SIMON de gerenciamento eventos e incidentes de monitoramento e também "...executa automações através da base de conhecimento acionável, topologia automática e auto recuperação de um ambiente ou equipamento" (Ofício nº 16/2023/STI/UFF).

Ainda, segundo a gestão, a ferramenta é responsável por observar 451 itens de configurações, entre servidores, switches, firewalls, etc.

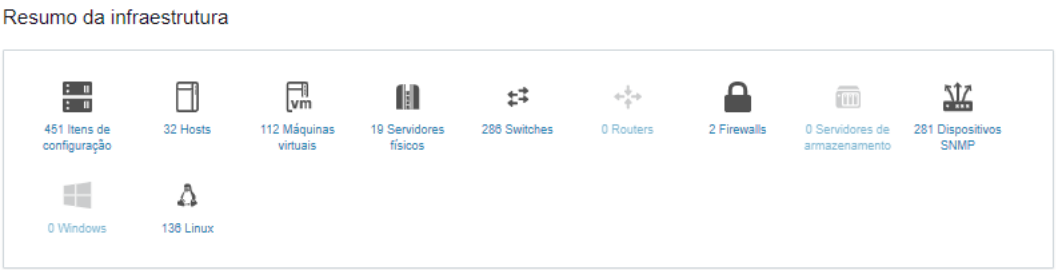

Figura 1 - Infraestrutura base para monitoramento SIMON

2.2 Identificação do objetivo-chave

O Comitê de Segurança da Informação - CSI, instituído pela Portaria 68.302 de 5/01/2022, até o momento da elaboração deste relatório, somente havia se reunido duas vezes em 2022, sem no entanto, produzir os resultados pretendidos pela Política de Segurança da Informação.

O CSI é responsável por conduzir o alinhamento das ações de Segurança da Informação para o alcance dos objetivos estratégicos da instituição em conformidade com a legislação vigente, devendo atuar, para alinhamento da UFF à LGPD, na definição, normatização e monitoramento interno dos seguintes temas: (i) Estratégias de backup e recuperação de incidentes de segurança; (ii) Políticas de autenticação e controle de acesso; (iii) Definição de ferramentas de prevenção contra ameaças; (iv) Segurança e acesso ao ambiente físico de TI; (v) Atualização de sistemas e *softwares*; e (vi) Conscientização de segurança para os servidores.

Foi identificado e selecionado pela equipe de auditoria como um objetivo-chave da unidade, garantir a segurança da Informação necessária para a manutenção e disponibilidade dos serviços à sociedade e o sigilo dos dados da organização e do cidadão.

2.3 Identificação de Riscos

O Tribunal de Contas da União – TCU recomenda a utilização do Framework do CIS[5] para definição de controles para combater os principais riscos de segurança cibernéticos (Anexo II). O CIS define 18 controles críticos, considerados pelo TCU como imprescindíveis e urgentes para as organizações (quadro 1).

[5] *Center for Internet Security (CIS*), organização independente e sem fins lucrativos.

Controles críticos de Segurança Cibernética - CIS	
1	Inventário e controle de ativos corporativos
2	Inventário e controle de ativos de software
3	Proteção de dados
4	Configuração segura de ativos corporativos e software
5	Gestão de contas
6	Gestão de controles de acesso
7	Gestão contínua de vulnerabilidades
8	Gestão de registros (logs) de auditoria
9	Proteção de e-mail e navegador da web
10	Defesa contra malware
11	Recuperação de dados
12	Gestão de infraestrutura de rede
13	Monitoramento e defesa de rede
14	Conscientização sobre segurança e treinamento de competências
15	Gestão de provedores de serviço
16	Segurança de aplicações de software
17	Gestão de respostas a incidentes
18	Teste de invasão

Fonte: CIS Controls® Version 8 (tradução livre).

Quadro 1- Controles CIS v 8

A gestão da STI informou não haver mapeamento do processo de segurança da informação. Não foi demonstrado haver um processo estruturado de identificação e análise de riscos em segurança da informação e comunicação que possa sugerir a existência de uma gestão de riscos na unidade.

Foram identificados e analisados os principais eventos de riscos suscetíveis de impactar, criticamente, o objetivo-chave:

a) Dano físico – incêndio, destruição de equipamento ou mídia;
b) Paralisação de serviços essenciais – falta de luz, falha na climatização;
c) Comprometimento da informação – alterações em *hardware/software*;
d) Ações não autorizadas – processamento ilegal de dados.

Utilizamos o diagrama *BowTie* para identificar e analisar os riscos selecionados.

a) Dano físico – incêndio , falta de suprimento de energia, etc. (figura 3).

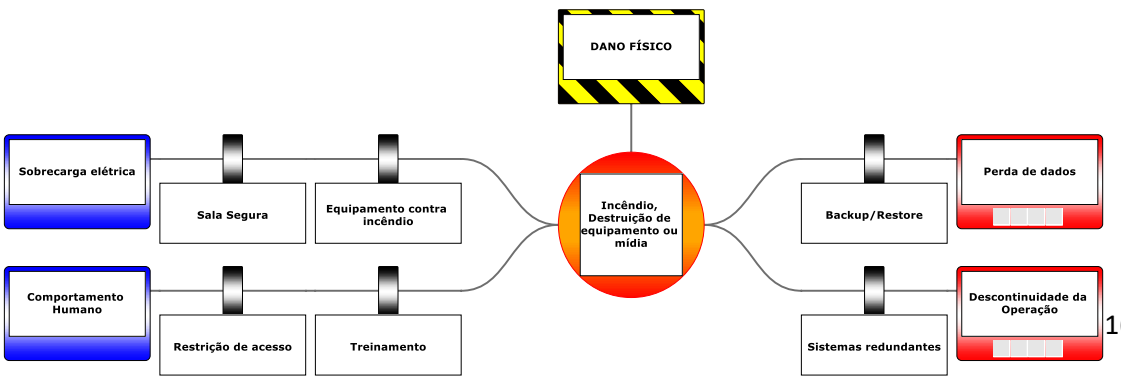

Figura 2- Risco de Danos - Incêndio

1. O *Data Center* está localizado no *Campus* do Valonguinho em um ambiente controlado (sala segura). O prédio não tem certificado do Corpo de Bombeiros do RJ.
    a. Existência de detector de fumaça com alarme ambiente. Não há aviso remoto;
    b. Identificamos equipamentos de combate a incêndios. Não há equipe treinada para combate a incêndios.
    c. As fitas de backup são armazenadas em cofre no mesmo prédio e andar do *Data Center.*

b) Paralisação de serviços essenciais – falta de luz, falha na climatização (figura 4).

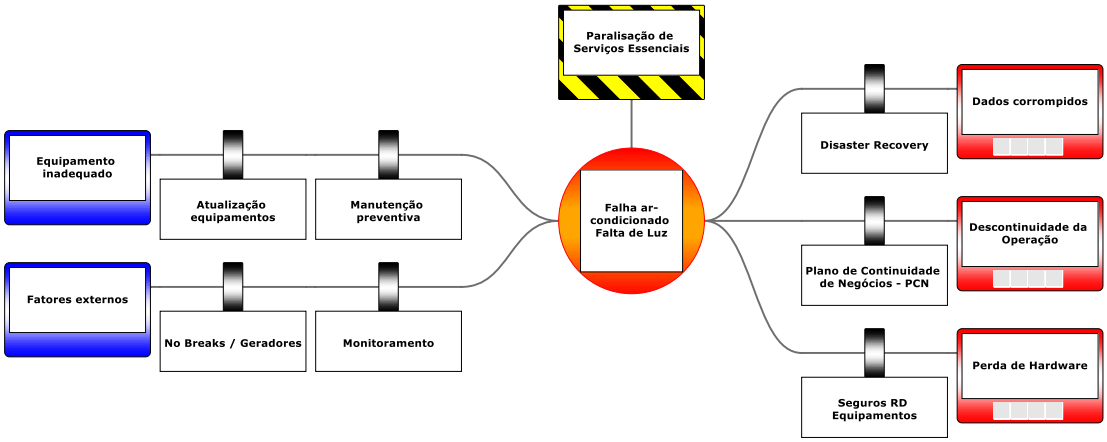

Figura 3 ´Riscos de paralisação de servisços essenciais

1. O *Data Center*, em caso de falta de energia, tem alimentação alternativa por gerador;
2. O *Data Center* possui equipamentos de climatização do tipo *Split.* Em visita técnica constatamos diferencial de temperatura nas salas do *Data Center.* De acordo com NBR14565:2013, a temperatura e a umidade devem estar, em todos os pontos, controlados precisamente;
3. A gestão informou que não são realizados testes para desastres;
4. Não existe um Plano de Continuidade de Negócios – PCN.

c) Comprometimento da informação – pode ser causado por modificações em hardware/software, erros durante o uso de sistemas, repúdio de ações, furto de equipamento (figura 5).

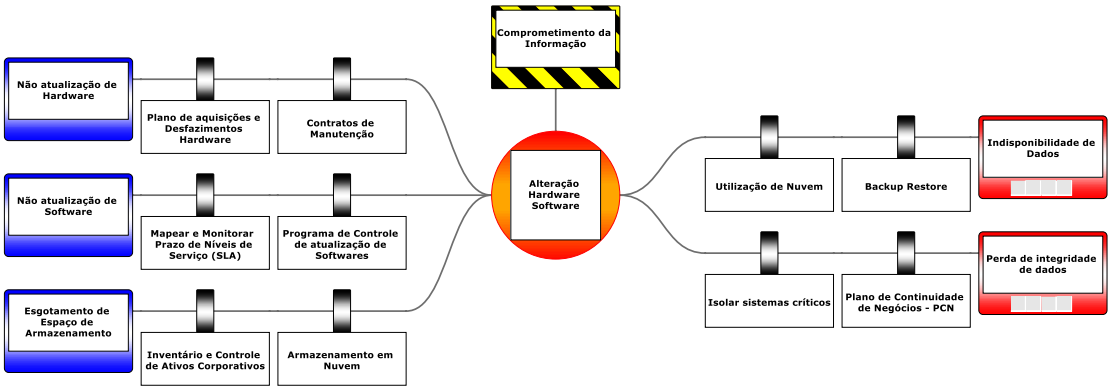

Figura 4- Riscos que comprometem a informação

1. A unidade mantém inventário de ativos de informação, contudo, não identificamos um processo de controle formal e estruturado sobre esses ativos;
2. A UFF mantém, em seus ativos de informação, sistemas legados[6] em aplicações/sistemas de alta criticidade, como:

Sistemas

i. Avaliação de Desempenho, última atualização 2015;
ii. Cadastramento de Ficha Financeira, última atualização 2013;
iii. Controle de Processos, última atualização 2012;
iv. Sistema de Frequência, última atualização 2016;
v. Sistema de Perícia Médica, última atualização 2015;
vi. Cálculo de Horas de Adicional e Extra, última atualização 2015;
vii. Sistema de Controle de Férias, última atualização 2015;
viii. Emissão de Contra-Cheques, última atualização 2015;

Plataformas

ix. FDI: versão 2.0;

[6] Segundo o Gartner, são sistemas de informação baseados em tecnologias ultrapassadas, mas é fundamental para as operações do dia a dia. Contudo, por não receberem atualizações, a manutenção é comprometida.

x. NX: Versão 3.2;

Servidor de e-mail

xi. MTA: Versão postfix: 2.7.1
xii. SMTP1: Versão postfix: 2.6.5
xiii. SMTP2: Versão postfix: 2.5.6
xiv. MailHub2: Versão postfix: 2.6.5

3. Existem câmeras de monitoramento nas salas do *Data Center*. Não há gravação das imagens;
4. Não identificamos normativo interno, obrigatório pela IN nº 5/2021 GSI, sobre uso seguro de computação em nuvem;
5. Dados institucionais são gravados e armazenados no Drive do Google, atual plataforma para e-mails institucionais. A gestão informou que, até a data de 7/4/2023, o volume de dados institucionais armazenado no Google Drive era 2,39 PentaBytes. Não há normativo na UFF sobre o uso e procedimentos de segurança de dados em nuvem, preconizada na IN 05/2021 do GSI;
6. A STI informou ter capacidade de armazenamento (quadro 2), de 214 Terabytes. A Biblioteca de fitas tem estimativa de 8 meses para saturação 100%;
7. Não há, na UFF, uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR, instituída pelo Decreto nº 9.637/2018. Instrução Normativa GSI/PR nº 01/2020 e Instrução Normativa GSI/PR nº 02/2020.

CAPACIDADE DE ARMAZENAMENTO

Tipo	Capacidade (1)	Utilização	Retenção Backup
Tape Library (2)	69 TB	34,8%	Estimado em 364 Dias
Storage:	115 TB	78,0%	
Data Domain:	30 TB	95%	6 meses
	214 TB	34%	

Observação:

(2) Informação de 06/04/2023

(1) Estimado alcançar 100% em 8 mesesInformação retirada no dia 06/04/2023.

Quadro 2 - Capacidade de Armazenamento

d) Ações não autorizadas – brechas de segurança, ataques cibernéticos, comportamento humano (figura 6).

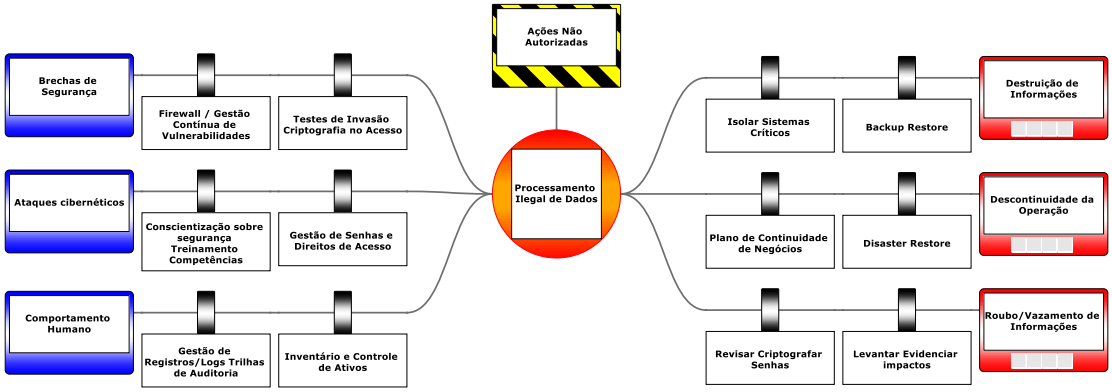

Figura 5 - Riscos de Ações Não Autorizadas

1. A unidade mantém inventário de ativos de informação. Não identificamos um processo formalizado de monitoramento dos ativos de informação da UFF;
2. Não existe uma política, processo, programa, plano ou equivalente com o objetivo de conscientizar a comunidade interna da instituição dos perigos e tratamentos;
3. A STI possui logs e trilhas de auditoria de todos os principais sistemas. Foram testadas as trilhas de auditoria dos sistemas Pergamun, SISBOL, SISAP, Sia-Compras, ID-UFF, SUPERBOL, SEI e CCPD. O sistema SUPERBOL não apresentou transações no

período analisado. Não identificamos uma política/procedimento de gestão de Logs;

4. A STI utiliza uma camada de segurança física utilizando sistema SGCA;
5. A camada de segurança lógica utiliza ferramentas para autenticação e autorização de acesso aos sistemas e para os serviços de *Data Center*. (Freeipa, Keycloak, Ldap, Ability e Smart Card);
6. O acesso físico ao *Data Center* é compartilhado entre vários profissionais da unidade auditada. Esse acesso ocorre através de carteirinha da Universidade (chip com permissão para os profissionais autorizados através do sistema IDUFF);
7. Não identificamos uma política, programa, normativo ou equivalente, que defina os requisitos mínimos para acesso aos sistemas e aplicativos da instituição;
8. A STI utiliza sistema de monitoramento *SIMON* que envia mensagens para os analistas responsáveis em caso de acesso indevido alem de recuperar automáticamente quedas de serviço;
9. A STI utiliza procedimentos de *Backup* constantes em minuta de Política de Backup e Restauração, que estabelece diretrizes para o processo de cópia e armazenamento dos dados, não formalizada;
10. Não constatamos a formalização de um processo/política ou equivalente, sobre a gestão das vulnerabilidades de segurança da informação;
11. A UFF sofreu, nos últimos 3 anos, 28 ataques cibernéticos (quadro 3). Um ataque *DdoS* e os demais *Defacements.* O baixo número se deve, segundo a STI, ao “esforço da equipe em manter os sistemas atualizados e nas análises de vulnerabilidade antes da implantação de plug-ins”.(Ofício nº 16/2023/STI/UFF);
12. A gestão da STI informou que o Comitê de Segurança da Informação - CSI, estava em reformulação, e que, após a efetivação da CSI seria revisada a Política de Segurança da Informação - PSI. Até a data deste relatório, não recebemos essas atualizações.

ATAQUES REGISTRADOS NOS ÚLTIMOS 3 ANOS NA UFF

Item	Data	Aplicação	Categoria
3	15/08/2022	uff.br	DDoS
10	08/06/2021	www.labem.uff.br/novo	Defacements
19	01/06/2020	www.labem.uff.br/novo	Defacements
15	23/09/2020	www.lar.uff.br	Defacements
7	09/06/2022	www.rasi.vr.uff.br	Defacements
11	08/06/2021	www.rasi.vr.uff.br	Defacements
27	30/03/2020	www.revistadepedagogiasocial.uff.br	Defacements
1	03/03/2023	espaco.uff.br	Defacements
6	30/06/2022	periodicos.uff.br	Defacements
14	01/04/2021	periodicos.uff.br	Defacements
26	30/03/2020	periodicos.uff.br	Defacements
23	01/05/2020	www.agendaacademica.uff.br	Defacements
21	25/05/2020	www.cadernosdeletras.uff.br	Defacements
20	01/06/2020	www.culturasjuridicas.uff.br	Defacements
4	06/07/2022	www.diversitates.uff.br	Defacements
16	13/06/2020	www.diversitates.uff.br	Defacements
25	30/03/2020	www.dst.uff.br/ojs	Defacements
9	25/04/2022	www.lagos.vr.uff.br	Defacements
12	23/04/2021	www.lagos.vr.uff.br	Defacements
2	26/12/2022	www.latec.uff.br	Defacements
28	01/03/2020	www.nees.uff.br	Defacements
22	25/05/2020	www.objnursing.uff.br	Defacements
5	06/07/2022	www.periodicoshumanas.uff.br	Defacements
17	13/06/2020	www.periodicoshumanas.uff.br	Defacements
18	01/06/2020	www.rasi.vr.uff.br	Defacements
8	25/04/2022	www.revistadepedagogiasocial.uff.br	Defacements
13	01/04/2021	www.revistadepedagogiasocial.uff.br	Defacements
24	27/04/2020	www.revistapassagens.uff.br	Defacements

Fonte: STI/2023

Quadro 3- Ataques Cibernéticos na UFF

2.4 - TED - Termo de Execução Descentralizada

Segundo o Decreto nº 10.426/2020, Termo de Execução Descentralizada é um instrumento por meio do qual a descentralização de créditos entre órgãos e entidades integrantes do Orçamento Fiscal e de Seguridade Social - OFSS da União com vistas à execução de programas, de projetos e de atividades, nos termos estabelecidos no plano de trabalho e observada a classificação funcional.

A unidade auditada informou não existirem projetos financiados por TED em execução na STI.

2.5 – Achados de auditoria

Elencamos, a seguir, as constatações de fatos ou circunstâncias relevantes, que têm potencial de impactar os objetivos da Segurança da Informação.

2.5.1. Ausência de Regimento Interno da STI formalizado e publicizado

A gestão da STI informou ter enviado versão, considerada final, do regimento interno para a DGI/PROPLAN e que a revisão final seria concluída em janeiro de 2023. No entanto, até a data desse relatório, não foi disponibilizado ou publicado o regimento interno da unidade.

2.5.2. Ausência do mapeamento dos processos de segurança da UFF.

Os processos de segurança da informação da UFF não estão mapeados. O mapeamento de processos é condição necessária para a identificação, análise e avaliação de riscos de segurança. A Gestão de riscos de segurança é um processo obrigatório de acordo com a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021.

2.5.3. Sistema de monitoramento por câmeras sem gravação em mídia nas dependências da *Data Center*.

Foram identificadas camêras de monitoramento nas dependências do *Data Center*. No entanto, não há procedimentos de monitoramento e nem armazenamento de imagens, reduzindo a capacidade desse controle interno.

2.5.4. Inexistência de equipe de combate a incêndios

Não há equipe ou pessoal formalizado e capacitado para atuar em caso de princípio de incêndio nas dependências do *Data Center*.

Apesar da existência de detectores de fumaça/incêndio e demais equipamentos de combate a incêndios, não existe uma equipe para tratamentos de emergências nos dias em que não há expediente.

2.5.5. Oscilação da climatização do Data Center

Segundo a NBR14565:2013, a temperatura e a umidade, em um *Data Center*, devem estar, em todos os pontos, controlados precisamente. Em visita da equipe de auditoria foi constatada diferencial de temperatura entre as salas seguras, além de excesso de umidade aparente nos equipamentos tipo *SPLIT* instalados.

2.5.6. Inexistência de uma política geral que defina os níveis de acesso a serem usados em todos os sistemas da instituição.

Foi comunicado haver política de acesso ao sistema SIA-COMPRAS e ao SEI. Nos demais sistemas o controle de acesso é definido pelos responsáveis. Não identificamos a existência de política geral que defina as credenciais mínimas de acesso a ser exigidas nos diversos sistemas utilizados pela UFF.

2.5.7. Inexistência de Plano de Continuidade de Negócios - PCN

Segundo o Gabinete de Segurança Institucional -GSI, o PCN é a “capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.”

2.4.8. Inexistência de uma política de coscientização e treinamento dos usuários sobre segurança da Informação

O TCU e CIS recomendam como controle crítico para mitigação de ataques cibernéticos a conscientização sobre segurança e treinamento de competências, com o objetivo de estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento da força de trabalho para ser consciente em segurança e devidamente qualificada para reduzir os riscos de segurança cibernética para a UFF.

2.4.9. Inatividade do Comitê de Segurança da Informação CSI

O Comitê de Segurança da Informação foi oficialmente instituído pela Portaria 68.302, de 5/01/2022, e foram feitas duas reuniões em 2022. No entanto, desde então não houve progresso na produção dos resultados pretendidos pela política. Segunda a gestão do STI a CSI está em reformulação.

O CSI é responsável por normatizar e monitorar os seguintes temas: Estratégias de backup e recuperação de incidentes de segurança; - Políticas de autenticação e controle de acesso; Definição de ferramentas de prevenção contra ameaças; Segurança e acesso ao ambiente físico de TI; Atualização de sistemas e softwares; Conscientização de segurança para os servidores.

2.4.10. Política de Segurança da Informação PSI desatualizada.

A Política de Segurança da Informação – PSI abrange segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais. A gestão da STI informou que PSI está em reformulação.

2.4.11. Não formalização da política de backup e recuperação da UFF

A STI mantem, publicado em seu site, rascunho de política de backup e restauração. Apesar da gestão da unidade declarar que utiliza os procedimentos indicados no "rascunho" da política, a não formalização da normativa precariza o processo de controle e responsabilização.

2.4.12. Sistemas legados suportando aplicações críticas de TI da UFF

A gestão informou que sistemas de informação relevantes da UFF estão baseados em plataformas legadas, como o NX Versão 3.2 e FDI versão 2.0 (dados funcionais).

Tais sistemas encontram-se obsoletos e/ou desatualizados, apresentando alto risco de incompatibilidade com novos sistemas ou tecnologias. O CIS recomenda a revisão de versões de software mensalmente ou com mais frequência para verificar o devido suporte.

2.4.13. Não normatização Interna sobre o uso seguro de computação na nuvem

O art. 4º da IN 05 de 30 de agosto de 2021 determina que: "Todos os órgãos ou as entidades, que desejarem utilizar computação em nuvem, deverão editar, obrigatoriamente, um ato normativo sobre o uso seguro de computação em nuvem". Não identificamos normatização interna sobre o uso de computação na nuvem.

2.4.14. Não implantação de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR

A ETIR foi instituída pelo Decreto nº 9.637/2018. Instrução Normativa GSI/PR nº 01/2020 e Instrução Normativa GSI/PR nº 02/2020 e preconiza a instalação de uma equipe para Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

2.6 – Recomendações

Neste tópico relacionamos nossas recomendações aplicáveis às constatações observadas durante nossos exames. Solicitamos que, ao questionar ou responder sobre o assunto, a área auditada utilize a numeração, que tem a

seguinte estrutura de formação: RA0223NNN, onde RA = Relatório de auditoria, 0223 = número e ano do relatório de auditoria e NNN = número sequencial da recomendação.

RA0223001

Publicizar o Regimento Interno da STI aprovado e finalizado pelos meios formais de divulgação.

Achado n.º 01

RA0223002

Mapear os principais processos de segurança da informação da Universidade e identificar e avaliar os riscos de segurança da informação.

Achado n.º 02

RA0223003

Avaliar e adequar o nível de segurança física do *Data Center*

1. Implementar sistema de monitoramento das imagens no ambiente do *Data Center*. Achado n.º 03;
2. Selecionar e treinar equipe de combate a incêndios dentre os servidores e funcionários da STI que atuam no *Data Center.* Achado n.º 04;
3. Avaliar a adequação dos equipamentos de climatização do *Data Center*. Achado n.º 05

RA0223004

Reconstituir e Publicizar o Comitê de Segurança da Informação – CSI

Achado n.º 09

RA0223005

Implementar e publicizar Plano de Continuidade de Negócios PCN da STI.

Achado n.º 07

RA0223006

Implementar Plano, Programa, Política ou equivalente com a finalidade de conscientizar os usuários sobre segurança da Informação.

Achado n.º 08

RA0223007

Revisar e publicizar a Politica de Segurança da Informação- PSI, em especial os itens:

1. Política de Backup e Restauração;
2. Política de acessos, privilégios e restrições.

Achados n.º 6 e 11

RA0223008

Elaborar plano de ação ou equivalente para levantar as necessidades de atualização das soluções baseadas atualmente em sistemas legados, em especial, as plataformas NX e FDI.

Achado n.º 12

RA0223009

Elaborar norma interna que regule utilização segura de computação na nuvem.

Achado n.º 13

RA0223010

Definição e implementação de equipe para Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR.

Achado n.º 14

3. CONCLUSÃO

Esta auditoria de Tecnologia da Informação significou uma provocação e um estímulo para a equipe de auditoria interna. Entendemos que o resultado, além do condão de agregar valor à unidade auditada, efetivou ganhos concretos para a própria auditoria interna seja pelo pioneirismo em sua abordagem de identificação de riscos, seja na ampliação de conhecimento dos auditores internos. Em decorrência, os futuros trabalhos de avaliação na área de tecnologia da informação, ganham contornos mais nítidos e promissores.

Entendemos que os resultados demonstram a premente necessidade da focalização, por parte da gestão e também de toda a comunidade UFF, da hodierna e abrangente ameaça que ronda a segurança da informação. A Lei Geral de Proteção de Dados –

LGPD e as diversas normas infralegais sobre o tema são respostas claras da importância desse tema.

Esperamos que o conteúdo desse relatório vá ao encontro desse foco e sirva de suporte para o desenvolvimento de melhores controles pela gestão.

Por fim, consideramos que a UFF se encontra no primeiro quartil do nível intermediário de segurança da informação e comunicação, conclusão corroborada pelo Acórdão 2164/2021-TCU-Plenário sobre Levantamento de Governança e Gestão Públicas 2021 do TCU.

É o nosso relatório:

Angelo Borges Ciuffo
Matrícula nº. 3143234

gov.br Documento assinado digitalmente
ANGELO BORGES CIUFFO
Data: 15/06/2023 15:39:24-0300
Verifique em https://validar.iti.gov.br

Rafael Barreto Esteves
Matrícula nº. 3271280

gov.br Documento assinado digitalmente
RAFAEL BARRETO ESTEVES
Data: 15/06/2023 16:02:46-0300
Verifique em https://validar.iti.gov.br

Ruy Barbosa Cavalcanti de Amorim
Matrícula nº 1474775

1 – Aprovo o Relatório de Auditoria nº 002/2023.
2 – Ao Conselho de Curadores, para apreciação.

gov.br Documento assinado digitalmente
NEWLEY MAGALHAES
Data: 16/06/2023 10:35:53-0300
Verifique em https://validar.iti.gov.br

Newley Magalhães
Chefe da Unidade de Auditoria Interna AT/CUR
SIAPE 1997915

ANEXO I – Ativos de Informação – *Data Center*.

Rack B 04				
Identificação do Ativo	**Equipamento**	**Descrição**	**Suporta/Hospeda**	**Hardware**
SpamAssassin	HP Proliant DL380g5	Linux mysqlspam	mysqlspam Banco de dados	RAM: 9gb CPU: Intel x86_64 com 8 núcleos (CPU(s))
MTA	HP Proliant DL380g5	Postfiix 2.7.1	Servidor de e-mail	RAM: 24gb CPU: Intel x86_64 com 8 núcleos (CPU(s))
KvmDin	HP Proliant DL380g5		Virtualização Carteirinha	RAM: 15gb CPU: Intel x86_64 com 8 núcleos e suporte a virtualização VT-x
Mysqlinfra2	HP Proliant DL380g5	Mysql 5.6	Banco de dados Mysql	RAM: 9gb CPU: Intel x86_64 com 8 núcleos e suporte a virtualização VT-x
Oracle	HP Proliant DL380g5	Oracle 12C	Banco de dados Oracle Produção	RAM: 10gb CPU: Intel x86_64 com 8 núcleos e suporte a virtualização VT-x
Oracle desenv	HP Proliant DL380g5	Oracle 12C	Banco de dados Oracle Desenvolvimento	RAM: 10gb CPU: Intel x86_64 com 8 núcleos e suporte a virtualização VT-x
fsdck20p	DELL POWEREDGE R710	Produção	Maquina Docker	RAM: 62gb Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
fsbck03p	Lenovo SR630	Backup	Bacula Backup	RAM: 30gb Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz
fskvm07p	DELL EMC POWEREDGE R740	Ovirt 4.2	Virtualização	RAM: 566gb Intel(R) Xeon(R) Gold 6230N CPU @ 2.30GHz
fskvm01h	DELL EMC POWEREDGE R740	oVirt 4.2 hostingine	VMs: 181 Gerencia da Virtualização	RAM: 566gb Intel(R) Xeon(R) Gold 6230N CPU @ 2.30GHz
kvm2	DELL POWEREDGE R710	virtualização Legado	Virtualização (14 VMs)	RAM: 94gb Intel(R) Xeon(R) CPU X5690 @ 3.47GHz
kvm1	DELL POWEREDGE R710	virtualização legado	Virtualização (17 VMs)	RAM: 78gb Intel(R) Xeon(R) CPU X5690 @ 3.47GHz
Rack B 03				
Identificação do Ativo	**Equipamento**	**Descrição**	**Suporta/Hospeda**	**Hardware**
Mysql Corporate	DELL POWEREDGE R730	Mysql 5.6	Banco de dados	RAM: 94gb Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz
fskvm05p	DELL POWEREDGE R710	Ovirt 4.2	Virtualização	RAM: 62gb Intel(R) Xeon(R) CPU E5530 @ 2.40GHz
fsbck04p	HP Proliant DL385p Gen8	bacula-dir	Backup	RAM: 47gb AMD Opteron(TM) Processor 6238
fskvm01p	DELL POWEREDGE R730	Ovirt 4.2	Virtualização	RAM: 188gb Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz
fskvm02p	DELL POWEREDGE R730	Ovirt 4.2	Virtualização	RAM: 188gb Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz
fskvm02p	DELL POWEREDGE R730	Ovirt 4.2	Virtualização	RAM: 188gb Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz
Neworacle	DELL POWEREDGE R730	oracleprod	Banco de dados	RAM: 94gb Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz
fskvm05p	DELL POWEREDGE R730	Ovirt 4.2	Virtualização	RAM: 62gb Intel(R) Xeon(R) CPU E5530 @ 2.40GHz
fskvm04p	DELL POWEREDGE R730	Ovirt 4.2	Virtualização	RAM: 62gb Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz
Rack B 02				
Identificação do Ativo	**Equipamento**	**Descrição**	**Suporta/Hospeda**	**Hardware**
mysqlsites	DELL POWEREDGE R710	mysql 5.7	Banco de dados	RAM: 62gb Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
Firewall	Fortigate 1500D	Firewall De Borda	VPN Roteador de Rede Regras de bloqueio e acesso VIP	
Rack EMC				
Data Domain	EMC DD6300		Capacidade: 31TB	
Storage	EMC VNX5400		Capacidade: 115TB	
Robo Fita				
Type Library	Qualstarxls XLS-820500	Robo de Fita	.- Slots: 355 - Drives: 03 - Fitas LTO4: 87	

ANEXO II – Inventário de sistemas da UFF

Sistemas		Finalidade
1	Pergamum	Sistema de gerenciamento de bibliotecas com funções integradas para administração da base bibliográfica das bibliotecas da UFF
2	SIGADOC	Sistema de gestão documental da UFF.
3	Portal Periodicos	Portal de Periódicos Acadêmicos UFF
4	RAD	Sistema do Relatório Anual de Docente, onde são registradas todas as atividades do docente realizadas na UFF, sejam as acadêmicas ou as administrativas.
5	PIBIC	O sistema desenvolvido para processo de submissão e avaliação de projetos de pesquisa, a bolsa de Iniciação Científica
6	Graduação Monitoria	Sistema de gerência das atividades de monitoria acadêmica
7	Diploma Privado UFF	Sistema que serve para que a UFF consiga gerenciar os processos de registro e emissão de diplomas de faculdades Privadas
8	Diploma Digital UFF	Sistema que serve para que a UFF consiga gerenciar os processos de registro e emissão de diplomas de Graduação.
9	DSPACE – RIUFF	Repositório digital com funções de armazenamento, gerenciamento, preservação e visibilidade da produção intelectual da UFF.
10	CPD	Sistema responsável por controlar o processo seletivo de docentes na UFF
11	SISBOL	Sistema de controle e conseção de Bolsas de estudos de apoio estudantil
12	CPPD	Sistema de Controle de Interstício de Docentes e progressão funcional
13	SIA-CHEFIAS	Sistema de Controle de Chefias Titulares – Acadêmicas e Administrativas
14	SISAP	Sistema de Controle Patrimonial dos bens móveis da universidade
15	SISPOS - Gestão Acadêmica	Sistema Acadêmico de controle de processos da Pós-graduação
16	SISPOS - Alunos	Sistema responsável por prover serviços (Declarações online, Periódicos Capes, Carteirinhas UFF, Plano de Estudo, Boletim e etc..) para todos alunos e pesquisadores ativos da Pós-graduação
17	SISPOS - Candidatura	Sistema responsável por gerenciar todo processo de inscrição online em cursos de pós-graduação lato e stricto sensu.
18	SisPPGE	Sistema de Gestão Acadêmica do Programa de Pós-Graduação em Gestão e Empreendedorismo
19	SISPRO	Sistema de Controle de Contratos UFF – FEC (Fundação de apoio a UFF)
20	SISPTA	Sistema de Informações da CPTA (Coordenação de Pessoal Técnico Administrativo) – Gestão de Competências e solicitação de força de trabalho de Pessoal Técnico Administrativo da UFF

21	SRI	Sistemas de Relacionamento Internacional - Gestão de Mobilidade Internacional In (Estrangeiro na UFF) e Out (Aluno UFF no exterior), Gestão de Convênios Internacionais, Gestão de Programa de Universalização de Línguas Estrangeiras.
22	SIA - Compras	Sistema de controle e aquisição de Compras de materiais
23	IDUFF	Sistema Acadêmico de Graduação (Ferramentas para gerenciamento de currículos, inscrição em disciplinas e cursos), Inscrição Online, Declarações, solicitação de Diploma, DAE (Gerenciamento de Alunos)
24	Administração Acadêmica UFF	Sistema de controle de Administração Acadêmica dos alunos de Graduação
25	Inscrição UFF	Sistema da inscrição para coordenação (Presencial, Ajuste)
26	Quadro de Horários UFF	Sistema de controle de turmas de disciplinas da graduação e alocação de docentes
27	ENADE UFF	Sistema de suporte para inscrição dos alunos no ENADE
28	Lançamento de Notas UFF	Sistema para registro de notas no Histórico Escolar do aluno de Graduação
29	SACI	Sistema de Carteirinha Digital de estudante da UFF visa modernizar a gestão de serviços estudantis da Universidade Federal Fluminense; agregar novos serviços para a comunidade acadêmica e trazer mais facilidades e segurança para o dia-a-dia de todos os estudantes.
30	SAI	Sistema para coleta e análise para conhecer a opinião dos discentes, docentes, e técnicos- administrativos sobre os cursos de graduação, do trabalho realizado nas disciplinas, e da infraestrutura disponível ao funcionamento dos mesmos.
31	SCAB	Sistema de Controle de Biblioteca
32	SGCA	Sistema de Gerenciamento de Controle de Acesso da UFF
33	Sistema de Processos UFF	Sistema de Controle de Processos Administrativos da UFF
34	SIGICON	Sistema de Gerenciamento de Informações Contratuais
35	SCTM	Sistema de controle de transações monetárias dos restaurantes universitários
36	SISAD	Sistema de Avaliação de Desempenho do corpo técnico da Universidade
37	SIRH	Sistemas Integrados de Recursos Humanos da UFF
38	Calculo Horas UFF	Sistema de Cálculo de Horas de Adicional e Extra do corpo técnico da UFF
39	Capacitação UFF	Sistema de controle de Capacitação do corpo técnico
40	Contracheques UFF	Sistema de Emissão de Contracheques
41	Ex Servidores UFF	Controle e Cadastramento de EX-SERVIDORES
42	Ficha Financeira UFF	Sistema de Cadastramento de Ficha Financeira
43	Fita Espelho UFF - Produção	Atualização do BD de pessoal Produção
44	Frequência UFF	Sistema de Frequência de todo o corpo técnico da Universidade
45	Incentivo Qualificação UFF	Sistema de controle ao processo de Incentivo à Qualificação
46	Pericia Medica UFF	Sistema de Perícia Médica UFF

47	Consulta Contracheques	Sistema de Emissão de Contracheque UFF
48	SEI	Sistema de gestão eletrônica de documentos e processos.da UFF
49	SIORG	Sistema de consulta ao organograma da UFF
50	Velti	Sistema de Ponto Eletrônico da UFF
51	Superbol	Sistema de Controle e Consulta de bolsas estudantis
52	ClubUFF	Aplicativo que oferece descontos em estabelecimento comercial aos usuários da carteirinha inteligente da UFF
53	UFF Mobile Plus	Aplicativo onde agrega vários serviços mobile da UFF
54	CITSmart	Sistema de Gerenciamento de Serviços de TI - ITSM
55	CEUA	Sistema da Comissão de Ética em Pesquisa com uso de animais
56	FDI	Sistema de acervo funcional
57	SolicitaUFF	Sistema de solicitação de inscrição de ingressantes UFF
58	Portal IDUFF	Portal de serviços acadêmicos e de apoio para toda a comunidade da UFF
59	PASUFF	Sistema de controle e cadastro de Arrecadação da UFF
60	Portal Transparencia UFF	Portal de transparência de informações da UFF
61	CKAN	Sistema de Gestão de Dados Abertos da UFF
62	REDMINE	Sistema de cadastro e gestão de projetos da UFF
63	ICA-AtoM	Sistema para descrição de documentos arquivísticos
64	Archivematica	Sistema de preservação digital da UFF
65	Helios Voting	Sistema de Eleições on-line utilizado para consultas eleitorias de toda necessidade da comunidade acadêmica da UFF
66	Teleport	Sistema responsável pelo Programa de Gestão de UFF

ANEXO III – Ameaças Digitais.

1 - ***Backdoor*** é um tipo de cavalo de troia (trojan) que dá ao invasor o acesso ao sistema infectado e lhe permite um controle remoto. Com essas permissões, o cibercriminoso consegue abrir, modificar e deletar arquivos, executar programas, instalar softwares maliciosos e enviar e-mails em massa.

2 - O ***phishing*** é um método dentro da linha de engenharia social que se aproveita da confiança depositada por um usuário para roubar seus dados. O cibercriminoso se passa por uma pessoa ou instituição legítima para enganar o usuário. Por isso, o phishing pode acontecer de diversas formas, seja em conversas de mensageiros instantâneos, seja em links de e-mails falsos.

3 - O ***spoofing*** está relacionado com a falsificação de endereços de IP, de DNS e de e-mails. Com essa prática, os criminosos podem simular uma fonte de IP confiável, editar o cabeçalho de um e-mail para parecer ser legítimo, ou modificar o DNS a fim de redirecionar um determinado nome de domínio para outro endereço IP.

4 - O ***ataque por manipulação de URL*** é usado por alguns hackers para fazer o servidor transmitir páginas às quais ele não teria autorização de acesso. Na prática, o usuário só tem acesso a links que são fornecidos pela página do site. Se o usuário altera manualmente a URL, ele pode testar diversas combinações para chegar a um endereço que esconde uma área restrita.

5 - ***Ataque DoS (Denial Of Service)*** - O ataque DoS, traduzido como negação de serviço, sobrecarrega um servidor ou um computador com um alto volume de pedidos de pacotes. Por não conseguir lidar com as requisições, o sistema não consegue mais responder, ficando indisponível. Portanto, não se trata aqui de uma invasão.

6. ***Ataque DdoS*** - Ao passo que o ataque DoS envolve apenas um computador fazendo vários pedidos de pacotes ao um servidor, ele não consegue derrubar sistemas mais robustos. Por isso, há uma técnica mais avançada, o DDoS (Distributed Denial of Service).

Como o nome indica, o ataque de negação de serviço distribuído, compartilha os pedidos para várias máquinas. É como se um computador mestre dominasse outras máquinas para que, simultaneamente, acessassem o mesmo recurso de um servidor, causando sobrecarga mesmo em alvos mais fortes.

7. Ataque ***DMA (Direct Memory Access)*** O ataque de Acesso Direto à Memória é uma função que permite ao hardware da máquina ter um acesso direto à memória RAM sem passar pelo processador, acelerando, assim, a taxa de transferência e processamento do computador.

8. ***Eavesdropping -*** neste ataque, o hacker utiliza diferentes sistemas de e-mail, mensagens instantâneas e telefonia, além de serviços de internet, para violar a confidencialidade da vítima, roubando seus dados para usá-los de forma indevida posteriormente. A palavra significa bisbilhotar, e é basicamente o que o criminoso faz, sem modificar as informações, apenas interceptando e armazenando.

9. ***Decoy*** - Neste tipo de ataque, o hacker simula um programa legítimo, de modo que o usuário faz o login e armazena suas informações, que poderão ser utilizadas pelo atacante.

10. ***Shoulder Surfing*** - significa “espiar sobre os ombros”. Sendo assim, não se trata de uma tecnologia ou ferramenta, mas sim um ato de olhar a tela de um usuário enquanto ele acessa dados sigilosos.

11. ***Defacements*** - O termo vem do verbo em inglês 'deface', que significa danificar ou desfigurar a aparência original de algo. No universo da Tecnologia o nome dado caracteriza ataques para modificar a página de um site na Internet.

12. ***MiitM ou man-in-the-middle*** utilizando a mesma rede de seus alvos, o agente malicioso se posiciona entre as duas partes (usuários, redes, empresas) que estão trocando informações, espionando toda a comunicação feita e se aproveitando de falhas na segurança cibernética.

ANEXO IV – Tabela de Grandezas

Prefixos do SI							
Prefixo		1000^m	10^n	Escala curta	Escala longa	Equivalente numérico	Desde[nota 1]
Nome	Símbolo						
iota	Y	1000^8	10^{24}	Septilhão	Quadrilião	1 000 000 000 000 000 000 000 000	1991
zeta	Z	1000^7	10^{21}	Sextilhão	Milhar de trilião	1 000 000 000 000 000 000 000	1991
exa	E	1000^6	10^{18}	Quintilhão	Trilião	1 000 000 000 000 000 000	1975
peta	P	1000^5	10^{15}	Quadrilhão	Milhar de bilião	1 000 000 000 000 000	1975
tera	T	1000^4	10^{12}	Trilhão	Bilião	1 000 000 000 000	1960
giga	G	1000^3	10^9	Bilhão	Milhar de milhão	1 000 000 000	1960
mega	M	1000^2	10^6	Milhão	Milhão	1 000 000	1960
quilo	k	1000^1	10^3	Mil	Milhar	1 000	1795
hecto	h	$1000^{2/3}$	10^2	Cem	Centena	100	1795
deca	da	$1000^{1/3}$	10^1	Dez	Dezena	10	1795
nenhum		1000^0	10^0	Unidade	Unidade	1	
deci	d	$1000^{-1/3}$	10^{-1}	Décimo	Décimo	0,1	1795
centi	c	$1000^{-2/3}$	10^{-2}	Centésimo	Centésimo	0,01	1795
mili	m	1000^{-1}	10^{-3}	Milésimo	Milésimo	0,001	1795
micro	μ	1000^{-2}	10^{-6}	Milionésimo	Milionésimo	0,000 001	1960
nano	n	1000^{-3}	10^{-9}	Bilionésimo	Milésimo de milionésimo	0,000 000 001	1960
pico	p	1000^{-4}	10^{-12}	Trilionésimo	Bilionésimo	0,000 000 000 001	1960
femto	f	1000^{-5}	10^{-15}	Quadrilionésimo	Milésimo de bilionésimo	0,000 000 000 000 001	1964
atto	a	1000^{-6}	10^{-18}	Quintilionésimo	Trilionésimo	0,000 000 000 000 000 001	1964
zepto	z	1000^{-7}	10^{-21}	Sextilionésimo	Milésimo de trilionésimo	0,000 000 000 000 000 000 001	1991
iocto	y	1000^{-8}	10^{-24}	Septilionésimo	Quadrilionésimo	0,000 000 000 000 000 000 000 001	1991

1. ↑ O sistema métrico foi introduzido em 1795 com seis prefixos. As outras datas estão relacionadas ao reconhecimento pela resolução da Conferência Geral de Pesos e Medidas (CGPM).

REFERÊNCIAS

Brasil. Tribunal de Contas da União. Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU.

Brasil, Gabinete de Segurança Institucional. Cartilha de Gestão de Segurança da Informação / GSI/PR.

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. Framework de Privacidade e Segurança da Informação / SGD. – Versão 1.1 , Março, 2023.

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. Guia de Gerenciamento de Vulnerabilidades / SGD. – Versão 2, Março, 2023.

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. Instrução Normativa nº 5 de 30 de agosto de 2021.

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. Modelo de Política de Gestão de Registros (logs) de Auditoria / SGD. – Versão 2, Março, 2023.

Brasil. Controladoria Geral da União/CGU. Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental, 2018.

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852 de 28 de março de 2023.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. ABNT NBR ISSO 27005**. Gestão de Riscos de Segurança da Informação. Rio de Janeiro. 2011.

Brasil. Tribunal de Contas da União.Cinco controles de segurança cibernética para ontem /Tribunal de Contas da União. – Brasília: TCU, 2022.

CIS – *Center for Internet Security.* Controles CIS versão 8.

BRASIL. Presidencia da República. LGPD - Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018, de 14 de agosto de 2018.Brasil.