MINISTÉRIO DA EDUCAÇÃO

SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARANÁ

Av. Victor Ferreira do Amaral, nº 306 – Tarumã – Curitiba – PR – CEP: 82.530-230

Telefone: 41-3595-7626 – e-mail: auditoria@ifpr.edu.br

Número: 09/2016	**RELATÓRIO DE AUDITORIA INTERNA**	**Data de emissão:** 05/10/2016

TIPO DE AUDITORIA: AUDITORIA DE GESTÃO

EXERCÍCIO: 2016

UNIDADE: AUDITORIA INTERNA

PROCESSO: 23411.002184/2016-81

PAINT/2015: 4.3 Auditoria de TI

OBJETIVO: A presente auditoria visa atender ao item 4.3 do PAINT - PLANO ANUAL DE ATIVIDADES DE AUDITORIA/2016, verificando a qualidade dos recursos de TI que interferem na produtividade dos demais servidores.

1. ESCOPO DO TRABALHO, METODOLOGIA E LIMITAÇÕES.

1.1. Os trabalhos foram realizados no período de 06 de abril a 23 de junho de 2016, por meio de testes, análises e consolidação de informações coletadas em, em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal.

1.2. O propósito deste exame consiste em formalizar o posicionamento da Auditoria Interna referentes às atividades de TI que interferem (ou podem) interferir na produtividade dos servidores

1.3. Nenhuma restrição foi imposta à realização dos exames.

1.4. O presente relatório apresenta dois elementos fundamentais para o entendimento de como esse trabalho foi desenvolvido, são eles: a Memória de Entendimento (ME) e os Testes dos Controles. Na Memória de Entendimento são apresentados os pontos de controle selecionados da legislação. Já nos Testes de Controle (TC) são feitos os devidos testes para verificar se os procedimentos previstos nas normas estão sendo atendidos e praticados no desenvolvimento dos atos administrativos. Cada controle apontado no ME será alvo de teste no TC. Qualquer constatação observada será notificada como **impropriedade**, quando apresentar ocorrências de natureza formal, ou como **ilegalidade**, quando for configurado que o ato atentou contra norma legal, foi antieconômico ou ilegítimo.

2. BASE LEGAL E DOCUMENTAÇÃO SUPORTE

- COBIT: ***Control Objectives for Information and related Technology***, é um guia de boas práticas apresentado como *framework*, dirigido para a gestão de tecnologia de informação (TI).
- Manual de Competências IFPR (versão 10/03/2015)
- Plano de Desenvolvimento Institucional (2014 -2018) IFPR
- NBR ISO/IEC 27001: 2006 – Esta norma especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI documentado dentro do contexto dos riscos do negócio globais da organização

3. MEMÓRIA DE ENTENDIMENTO – ME

Primeiramente, cumpre estabelecer o objetivo deste trabalho. Como dito anteriormente, vamos analisar a área de TI com foco na produtividade do trabalho servidor. Isto além de significar a utilização de sistemas, envolve a utilização dos dados e armazenamento dos dados.

Iniciaremos com a customização dos sistemas e em segundo lugar, veremos o Data Center, local onde é armazenado e processado os dados (e informações) produzidos pelos servidores. Em terceiro lugar, faremos uma breve análise do SIPAC. E em seguida veremos Site Institucional e Impressão.

3.1. PLANEJAMENTO INSTITUCIONAL E TI

Segundo o Manual de Competências do IFPR cabe a DTIC:

> - Cumprir e fazer cumprir as normas e procedimentos institucionais;
> - Elaborar, coordenar, e controlar a implantação do Plano Diretor de Tecnologia da Informação e Comunicação- PDTIC e das Políticas de Segurança da Informação;
> - Dirigir o levantamento das necessidades dos usuários; supervisionar projetos de Soluções de Sistemas de Informação, infraestrutura e apoio ao usuário;
> - Buscar Soluções de TIC que venham a agregar valores para instituição;
> - Desempenhar outras atividades inerentes à unidade, função ou cargo, não previstas neste manual, mas de interesse da administração.

Por sua vez, o COBIT 4.1 a área de TI deve estar alinhada ao plano de negócio. Assim:

> Para a área de TI entregar de maneira bem-sucedida os serviços que suportam as estratégias de negócios, deve existir uma clara definição das responsabilidades e direcionamento dos requisitos[1] pela área de negócios (o cliente) e um claro entendimento acerca do que e como precisa ser entregue pela TI (o fornecedor).

Desta forma, entende-se a área de Tecnologia da informação deva estar alinhada com a estratégia do negócio, ao ponto que seja claro tanto para a TI como para o negócio o que se espera da TI. (Controle 1)

3.2. DATA CENTER E DEMAIS CONTROLES

Data Center, ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores, e outros. Por isso, é considerado o "sistema nervoso" das empresas. No caso específico do IFPR, o Data Center abriga os seguinte serviços: Websites, Videoconferência, Sistema (SIG, SISA, PERGAMUN), Backup. (Controle 2).

Em relação aos demais recursos abarcados neste relatório, temos as redes, o SIPAC, o Site Institucional e as impressões. Nestes temas, analisaremos questões que dizem respeito ao acesso dos servidores, sua identificação, o impacto potencial da ausência de determinados requisitos para utilização destes recursos. Para tanto, utilizamos os controles definidos na NBR ISO/IEC 27001: 2006. (Controle 3 ao Controle 5)

1 **Requisitos** são instruções que definem como atingir o objetivo de negócio. Em geral, refletem funções que o usuário precisa realizar para atingir o objetivo do sistema ou funções de apoio à estratégia do negócio. Registros, controle de fluxo, consultas e cadastros são requisitos típicos. Em geral, requisito é algo que o usuário solicita explicitamente (ou *requisita*). O requisito é algo que reflete a forma como o usuário enxerga a solução para o seu problema, já convertida em fases do processo. É muito comum que os requisitos reflitam diretamente em telas e ações do sistema. Durante a atividade de extração ou detalhamento de requisitos, seja em entrevista ou observação do processo, o analista deve estar atento para identificar, nas entrelinhas, as regras de negócio ocultas. Como a maioria das pessoas já se habituou ao mundo informatizado cabe ao analista identificar na lista de requisitos fornecida pelo usuário, aqueles requisitos que realmente são necessários para atingir os objetivos de negócio da forma mais simples. (http://dextra.com.br/requisito-ou-regra-de-negocio/)

4. TESTES DE CONTROLE

4.1. ALINHAMENTO TI COM PLANEJAMENTO ESTRATÉGICO

Para testar os controles relacionados ao alinhamento da TI com os objetivos estratégicos primeiramente

Controle 1 – Definição dos Requisitos

Este controle visa deixar esclarecer como as Pró-reitorias do IFPR planejam e comunicam este planejamento à TI (DTIC). Primeiramente testamos se as Pró-reitorias possuem planejamento para as suas atividades (cabe dizer que se há mapeamento de processos nas Pró-reitorias, ou se houver, não há publicidade no site institucional). A SA 09/2016-02 questionou em seu item 3: *"A pró-reitoria possui todos os seus processos e fluxos mapeados?"*Em resposta as Pró-reitorias responderam:

PROPLAN:

> Os processos internos das Pró-reitorias são desenhados no próprio Manual de Competências. Está em elaboração pela comissão formada pela Portaria nº 1313 de 02 de Junho de 2015, o Manual Administrativo que trará os fluxos de todas as Pró-reitorias mapeados. Por hora, a comissão finalizou a elaboração do fluxograma dos processos do Setor de Protocolo. O mapeamento da PROPLAN se dará na sequência, conforme os trabalhos avancem.

PROAD: "*Ainda não possui. Estamos da dependência do desenvolvimento de um manual a ser elaborado por Comissão específica da Reitoria."*

PROEPI: "*As diretorias e coordenadorias da PROEPI possuem fluxos estabelecidos, mas estão trabalhando na construção de documentos que sistematizem e formalizem esses fluxos, principalmente em parceria com a DTIC."*

PROGEPE:

> Quanto aos fluxos, informamos que há na Reitoria uma comissão designada para desenvolver fluxos e procedimentos, que foi designada pela Portaria nº 1.313/2015 Comissão Permanente de Elaboração do 02/06/2016 Memorando Eletrônico SIPAC https://sipac.ifpr.edu.br/sipac/protocolo/memorando_eletronico/memorando_eletronico.jsf?idMemorandoEletronico=275103 2/2 Manual de Procedimentos Administrativos do IFPR. (Disponível em http://reitoria.ifpr.edu.br/wpcontent/uploads/2015/08/1313COMISS%C3%83OPERMANENTEDEELABORA%C3%87%C3%83ODOMANUALDEPROCEDIMENTOSADMINISTRATIVOSDOIFPR.pdf

Como visto, ainda não há dentro do IFPR processos mapeados (de forma sistêmica). O mapeamento de processos pode trazer muitas vantagens para as instituições: identificação de gargalos operacionais, controle e padronização do processo produtivo, formalização do conhecimento, otimização e aumento da produção e melhoria da qualidade de produtos ou serviços. Entende-se que para o mapeando de processos têm-se que estudar cada etapa verificando sua efetividade, eficiência e eficácia no processo como um todo.

Dizer que os processos estão mapeados não quer dizer engessados, porém tal confusão pode haver, uma vez que a instituição que possui os processos mapeados tem mais maturidade, ou seja, os processos já foram questionados (estudados) antes de serem formalizados. Pelo fato dos processos serem mais maduros a instituição reage melhor em momentos de estresse, de mudanças.

A produção de um software ou a sua customização depende muito da estabilidade dos processos, maturidade institucional. Processos que mudam constantemente (instáveis) replicam no trabalho e retrabalho de atualização (customização) dos sistemas. Portanto, ao solicitar customizações de sistemas à DTIC, é necessário que as Pró-reitorias tenham os seus processos mapeados (e estudados). **(RC 01)**

Controle 2 – DATA CENTER

Para testar os riscos inerentes ao DATA CENTER do IFPR, aplicamos a NBR ISO/IEC 27001: 2006, especificamente o seu Anexo A.9.2 que diz respeito a segurança dos equipamentos (objetivo: impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização).

A primeira, segunda e terceira colunas apresentam o item da norma do anexo A.9.2 da norma ISO/IEC 27001: 2006. Na quarta coluna apresentamos como os itens que dizem respeito a norma estão sendo aplicados no IFPR.

A.9.2 Segurança de equipamentos Objetivo: impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização			
ITEM	ASSUNTO	CONTROLE	COMO É FEITO
A.9.2.1	Instalação e Proteção do equipamento	Os equipamentos devem ser colocados no local ou protegidos para reduzir ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.	O acesso é feito por chaves comuns (sem identificação de quem está acessando a sala). Não há proteção contra ameaças do meio ambiente (incêndios, enchentes) **(RC 02)**
A.9.2.2	Utilidades	Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções	Os equipamentos de Nobreak e gerador estão com operação parcial, sem garantia e

		causadas por falhas de segurança	contrato de manutenção. **(RC 03)**
A.9.2.3	Segurança no cabeamento	O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegidos contra interceptação ou danos.	A fibra ótica de onde chega o acesso à RNP passa pelo Data Center, vai até outra sala – onde pessoas além da DTIC têm acesso, sendo o sinal da RNP convertido em sinal elétrico voltando para o Data Center, via cabo de rede. **(RC 04)**
A.9.2.4	Manutenção dos equipamentos	Os equipamentos devem ter manutenção correta, para assegurar sua disponibilidade e integridade.	Servidores, storages, nobreak, geradores e ativos de redes estão sem garantia e cobertura contratual **(RC 05)**

Riscos potenciais: na sala do Data Center é onde se encontra (praticamente) todo o armazenamento de dados referente aos sistemas institucionais. A não identificação dos profissionais que tem acesso à sala, o não provimento de recursos (tais como energia, telecomunicações, ar condicionado), não manutenção preventiva dos equipamentos podem fazer com que qualquer incidente (relativo a falha da infraestrutura, dos equipamentos ou ações de servidores que detêm acesso ao Data Center) leve o IFPR a perder todos os seus dados (informações) institucionais, gerando um prejuízo incalculável para a instituição.

Ainda em relação ao Data Center , abordamos agora o tema Backup, Anexo A. 10.5:

A.10.5 Cópias de Segurança Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação			
ITEM	ASSUNTO	CONTROLE	COMO É FEITO
A. 10.5.1	Cópias de segurança das informações	Cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente, conforme política de geração de cópias de segurança definida.	A DTIC informou que há backup de todos os dados inseridos no sistemas, no entanto, as cópias encontram-se na sala do Data Center. **(RC 06)**

Riscos potenciais: a não utilização de Backup em outro espaço geográfico no qual os dados estão sendo gerados/gravados pode fazer com que a segurança proporcionada

pelas cópias não seja efetivamente conquistada. Em caso de incêndio, catástrofe da natureza, sobrecarga de energia, os equipamentos de Backup podem ser tão danificados quanto os equipamentos onde são gravados os dados "originais".

Controle 3 – RECURSOS DE REDES

Para testar os riscos inerentes ao controle de acesso à rede do IFPR aplicamos a NBR ISSO/IEC 27001: 2006, especificamente o seu Anexo A.11 (A.11.1 e A11.2). Neste quesito analisaremos o acesso à rede de servidores (docentes e técnicos) e alunos

A. 11.1 Requisito de negócio para controle de acesso Objetivo: Controlar o acesso à informação **(RC 07)**			
ITEM	ASSUNTO	CONTROLE	COMO É FEITO
A.11.11	Política de Controle de Acesso	A política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e da segurança da informação.	Não há política de controle de acesso, mas política de boas práticas estabelecidas pela IIP 27.
A. 11.2 Gerenciamento de acesso do usuário			
A.11.2.1	Registro do usuário	Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços	Não há procedimento formalizado
A. 11.2.2	Gerenciamento de Privilégio	A concessão e o uso de privilégios devem ser restritos e controlados	Não há gerenciamento
A. 11.2 .3	Gerenciamento de senha do usuário	A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal	Não há gerenciamento
A.11.2.4	Análise crítica dos direitos de acesso de usuário	O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal	Não há análise

Riscos potenciais: a não necessidade de autenticação na rede do IFPR pode facilitar a entrada de estranhos, principalmente se conectados fisicamente com roteador dentro da instituição. A concessão de acesso com usuário identificados é benéfica também por identificar as ações dos servidores e alunos dentro da rede (evitando, por exemplo, a sites impróprios e em caso de acesso ter como identificar e punir os usuários). Com tal

ação fica possível a segmentação de perfis onde os usuários tenham mais ou menos acessos conforme interesse da gestão.

Controle 4 – SIPAC

Para testar os riscos inerentes ao controle de acesso ao SIPAC do IFPR aplicamos a NBR ISSO/IEC 27001: 2006, especificamente o seu Anexo A.11 (A.11.1 e A11.2). Neste quesito analisaremos o acesso à rede de servidores:

B. 11.1 Requisito de negócio para controle de acesso Objetivo: Controlar o acesso à informação			
ITEM	ASSUNTO	CONTROLE	COMO É FEITO
A.11.11	Política de Controle de Acesso	A política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e da segurança da informação.	Há política de controle de acesso - IIP 29 DTIC. Embora "a política" não contemple o mapeamento de perfil para cada servidor (algo que pode ser melhorado). Consideramos satisfatória.
B. 11.2 Gerenciamento de acesso do usuário			
A.11.2.1	Registro do usuário	Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços	Sim, há.
A. 11.2.2	Gerenciamento de Privilégio	A concessão e o uso de privilégios devem ser restritos e controlados	Sim, há.
A. 11.2 .3	Gerenciamento de senha do usuário	A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal	Sim, há.
A.11.2.4	Análise crítica dos direitos de acesso de usuário	O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal	Sim, há.

Controle 5 – WEB SITE INSTITUCIONAL

Para testar os riscos inerentes ao controle de acesso ao Site Institucional do IFPR aplicamos a NBR ISSO/IEC 27001: 2006, especificamente o seu Anexo A.11 (A.11.1 e A11.2). Neste quesito analisaremos o acesso dos servidores (docentes e técnicos) que fazem a manutenção do site:

C. 11.1 Requisito de negócio para controle de acesso Objetivo: Controlar o acesso à informação **(RC 08)**			
ITEM	ASSUNTO	CONTROLE	COMO É FEITO
A.11.11	Política de Controle de Acesso	A política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e da segurança da informação.	Não há política, porém a orientação quanto à utilização e boas práticas, IIP 007
C. 11.2 Gerenciamento de acesso do usuário			
A.11.2.1	Registro do usuário	Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços	Há formalização na concessão, porém o acesso é indiscriminado. Todos os usuários têm acesso a todos os arquivos (no caso da Reitoria), podem alterá-los ou excluí-los.
A. 11.2.2	Gerenciamento de Privilégio	A concessão e o uso de privilégios devem ser restritos e controlados	A concessão de uso é controlada, no entanto os usuários não possuem perfis que restrinjam, minimizem erros ou atuações maliciosas.
A. 11.2 .3	Gerenciamento de senha do usuário	A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal	A Comunicação (IFPR) gerencia o acesso
A.11.2.4	Análise crítica dos direitos de acesso de usuário	O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.	Não. Depende do envio de informações da unidade (DTIC).

Riscos potenciais: pelo funcionamento da ferramenta hoje utilizada (Wordpress) não há distinção entre a área de responsabilidade entre os servidores – da Reitoria - que atualizam o site. Por exemplo, se um servidor (técnico ou docente) tiver acesso ao wordpress ele poderá alterar várias páginas pertencentes ao IFPR, não apenas aquela que lhe diz respeito, possibilitando ações intencionais (“maldosas”) de agentes humanos e facilitar erros.

Controle 5 – Impressão

Para testar os riscos inerentes ao controle de acesso à impressão do IFPR aplicamos a NBR ISSO/IEC 27001: 2006, especificamente o seu Anexo A.11 (A.11.1 e A11.2). Neste quesito analisaremos o acesso dos servidores (docentes e técnicos) que imprimem

D. 11.1 Requisito de negócio para controle de acesso Objetivo: Controlar o acesso à informação **(RC 09)**			
ITEM	ASSUNTO	CONTROLE	COMO É FEITO

A.11.11	Política de Controle de Acesso	A política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e da segurança da informação.	Não há
D. 11.2 Gerenciamento de acesso do usuário			
A.11.2.1	Registro do usuário	Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços	Não há
A. 11.2.2	Gerenciamento de Privilégio	A concessão e o uso de privilégios devem ser restritos e controlados	Não há
A. 11.2 .3	Gerenciamento de senha do usuário	A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal	Não há
A.11.2.4	Análise crítica dos direitos de acesso de usuário	O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal	Na há

Riscos potenciais: Os riscos com relação à impressão dizem respeito a pouca eficiência da ferramenta, pois não há controle sobre tal. Efetivamente hoje no IFPR, um servidor pode imprimir quantas cópias quiser (relativas ao trabalho ou particular). A identificação do usuário permitiria dimensionar quantas páginas são necessárias para o setor /servidor realizar seu trabalho e em caso de descontrole, identificar os responsáveis. O controle causaria efeitos benéficos sobre a economicidade e com relação ao meio ambiente – as pessoas tenderiam a imprimir somente o necessário.

5. RELATÓRIO DE CONSTATAÇÕES

RELATÓRIO DE AUDITORIA Nº 09/2015 – AUDITORIA DE TI

Item do Relatório de Auditoria	**Constatação (01) - Recomendação (01.01)**
Descrição da Constatação	As pró-reitorias (e DTIC) não possuem mapeamento de processos. Tal fato faz com que não se tenha estabilidade (maturidade) nos procedimentos e da mesma forma pode haver retrabalho no desenvolvimento e aquisição de sistemas.
Descrição da Recomendação	Recomendamos que todas as Pró-reitorias realizem o mapeamento de seus processos, delineando a partir dos produtos e serviços que oferecem (seja atividade fim ou atividade meio) os processos (recursos) necessários para produzi-los. A partir disto, que a DTIC desenvolva os sistemas, como meio de eliminar gargalos, melhorar os produtos e otimizar os recursos tornando os processos mais eficientes, eficazes e efetivos.
1. Nome da unidade interna responsável pelo atendimento da recomendação	
PROAD, PROEPI, PROENS, PROPLAN, PROEGEPE e DTIC	
2. Manifestação da unidade acerca da recomendação	
3. Análise da Auditoria Interna	

Item do Relatório de Auditoria	**Constatação (02) - Recomendação (02.01)**
Descrição da Constatação	O acesso à sala do Data Center é feito por chaves comuns, não sendo possível identificar quem tem acesso.
Descrição da Recomendação	Implantar sistema que identifique os profissionais que entrem na sala com fechadura com senha, biometria ou outro recurso semelhante. Implantar câmeras.
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	
2. Manifestação da unidade acerca da recomendação	
3. Análise da Auditoria Interna	

Item do Relatório de Auditoria	Constatação (03) - Recomendação (03.01)
Descrição da Constatação	Os equipamentos que dão suporte ao Data Center em relação a ausência de energia elétrica – No Break e gerador - estão com funcionamento comprometido e sem garantia ou contrato de manutenção
Descrição da Recomendação	Recomendamos que sejam postos em pleno funcionamento o No Break e gerador, com contrato válido de manutenção. Sugerimos uma verificação técnica em relação à obsolescência dos equipamentos e posterior substituição, se for o caso.
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	
2. Manifestação da unidade acerca da recomendação	
3. Análise da Auditoria Interna	

Item do Relatório de Auditoria	Constatação (04) - Recomendação (04.01)
Descrição da Constatação	A fibra ótica de onde chega o acesso à RNP passa pelo Data Center, vai até outra sala – onde pessoas além da DTIC têm acesso, sendo o sinal da RNP convertido em sinal elétrico voltando para o Data Center, via cabo de rede.
Descrição da Recomendação	Recomendamos que a fibra ótica chegue diretamente ao Data Center, sem passagens por outras salas ou ambientes que tenham acesso de terceiros
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	
2. Manifestação da unidade acerca da recomendação	
3. Análise da Auditoria Interna	

Item do Relatório de Auditoria	Constatação (05) - Recomendação (05.01)
Descrição da Constatação	Servidores, *storages*, e ativos de redes estão sem garantia e cobertura contratual.
Descrição da Recomendação	Recomendamos que sejam postos em pleno funcionamento os equipamentos danificados do Data Center, com contrato válido de manutenção. Sugerimos uma verificação técnica em relação à obsolescência dos equipamentos e posterior substituição, se for o caso.
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	

2. Manifestação da unidade acerca da recomendação

Item do Relatório de Auditoria	**Constatação (06) - Recomendação (06.01)**
Descrição da Constatação	A DTIC informou que há backup de todos os dados inseridos nos sistemas, no entanto, as cópias encontram-se na sala do Data Center. A não utilização de Backup em outro espaço geográfico no qual os dados estão sendo gerados/gravados pode fazer com que a segurança proporcionada pelas cópias não seja efetivamente conquistada. Em caso de incêndio, catástrofe da natureza, sobrecarga de energia, os equipamentos de Backup podem ser tão danificados quanto os equipamentos onde são gravados os dados.
Descrição da Recomendação	Criar mecanismos de Backup em local diferente do Data Center, como forma de reduzir a criticidade em relação a perda de dados institucionais.
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	
2. Manifestação da unidade acerca da recomendação	

Item do Relatório de Auditoria	**Constatação (07) - Recomendação (07.01)**
Descrição da Constatação	Não há política de controle de acesso à rede (embora haja política de boas práticas estabelecidas pela IIP 27). Não há procedimento formalizado para cadastrar usuários na rede. Não há distinção de privilégios e uso de senhas, consequentemente não há avaliação do acesso dado anteriormente.
Descrição da Recomendação	Recomendamos a criação de "domínios" para que cada servidor (Docente e Técnico) e alunos tenham suas atividades na rede identificadas
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	
2. Manifestação da unidade acerca da recomendação	
3. Análise da Auditoria Interna	

Item do Relatório de Auditoria	**Constatação (08) - Recomendação (08.01)**
Descrição da Constatação	Não há política de acesso à modificação do site institucional. Muitos usuários têm acesso e podem modificar áreas do site que não são de suas

	competências.
Descrição da Recomendação	Recomendamos que sejam utilizas das ferramentas para controle de acesso, onde cada usuário tenha permissões para acessar a pagina do IFPR referente a sua atuação (atividade).
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	
2. Manifestação da unidade acerca da recomendação	
3. Análise da Auditoria Interna	

Item do Relatório de Auditoria	**Constatação (09) - Recomendação (09.01)**
Descrição da Constatação	Não há política de acesso à impressão. O acesso é dado por igual a todos, "sem limites". Os usuários não têm identificação e o IFPR não sabe quem imprime o que.
Descrição da Recomendação	Recomendamos que o acesso às impressoras seja individualizado de modo, a saber, quantas impressões cada usuários faz. Caso seja possível, sugerimos que seja dada (ou esclarecidas) a opção dos usuários pagarem por suas impressões (cópias particulares)
1. Nome da unidade interna responsável pelo atendimento da recomendação	
DTIC	
2. Manifestação da unidade acerca da recomendação	
3. Análise da Auditoria Interna	

6. CONCLUSÃO

Analisamos no relatório de TI aspectos referentes ao Data Center, à customização de sistemas, ao SIPAC, ao Site Institucional, à impressora. A escolha de tais temas foi circunstanciada por entender que interferem na produtividade dos servidores. De forma geral, entendemos que os processos podem ser aprimorados paulatinamente e concomitantemente precisam que seja feita a analise de riscos na atuação de TI.

Os riscos aos quais nos referimos dizem respeito principalmente à segurança da informação, por exemplo, a perda de dados no Data Center, o acesso indiscriminado de servidores à algumas ferramentas são algumas frentes na quais acreditamos que a gestão deva atuar e mitigar riscos.

Curitiba, 05 de outubro de 2016.

Kétura Silva Paiva

Auditor

Rodrigo de Costa

Auditor

Roberto Batista

Chefe da Auditoria Interna