AUDITORIA-GERAL
Coordenação-Geral de Auditoria em Gestão Interna
Coordenação de Inteligência e Suporte em Auditoria
Divisão de Auditoria em Tecnologia e Inovação

RELATÓRIO DE AUDITORIA

Auditoria de Avaliação do Incidente de Segurança no Sistema CONSIGWEB

Ação nº 5540/2019

Brasília/DF, 15 de junho de 2020

Relatório de Auditoria

Ação Especial nº 5540/2019
Unidade Auditada: Diretoria de Tecnologia da Informação e Inovação – DTI

QUAL FOI O TRABALHO REALIZADO PELA AUDITORIA?

Avaliação dos controles relacionados à segurança do sistema ConsigWeb.

POR QUE A AUDITORIA REALIZOU ESSE TRABALHO?

O trabalho foi motivado pelo incidente de Segurança da Informação e Comunicação no sistema ConsigWeb.

A avaliação levou em consideração as seguintes questões:

- estrutura de controle de acesso adotada para o sistema ConsigWeb;
- como são realizados os controles de acesso ao servidor de aplicação em *colocation* na Dataprev;
- procedimentos de gestão de incidente e controle de acesso adotados para mitigar o incidente; e
- aderência das configurações do servidor de aplicação às melhores práticas de mercado.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDITORIA? QUAIS RECOMENDAÇÕES DEVERÃO SER IMPLEMENTADAS?

A ocorrência de acessos indevidos no sistema ConsigWeb, através da rede de dados do INSS, possivelmente permitindo a recuperação, por terceiros, de informações financeiras e operacionais de empréstimos consignados em folha de segurados do Instituto.

Verificou-se também a concessão indevida de perfis de acesso ao ConsigWeb a servidores e estagiários, utilizados para a recuperação das informações citadas acima. Foram analisadas as inconsistências em procedimentos de gestão de incidente e controle de acesso adotados para mitigar o incidente.

Nesse sentido, foi recomendado adotar providências visando aprimorar os controles relativos à gestão de acesso ao sistema ConsigWeb e ao equipamento servidor *colocation*.

LISTA DE SIGLAS E ABREVIATURAS

APS	Agência da Previdência Social
AUDGER.....	Auditoria-Geral
ConsigWeb.....	Sistema de Consulta de Empréstimos Consignados
CTIR.....	Centro de Tratamento de Incidente de Redes
Dataprev.....	Empresa de Tecnologia e Informações da Previdência Social
DIRAT	Diretoria de Atendimento
DIRBEN	Diretoria de Benefícios
DSIC.....	Departamento de Segurança da Informação e Comunicações
DTI	Diretoria de Tecnologia da Informação e Inovação
ETIR.....	Equipe de Tratamento de Incidente de Redes
GERID.....	Sistema Gerenciador de Identidade
GSI	Gabinete de Segurança Institucional
INSS.....	Instituto Nacional do Seguro Social
IP	*Internet Protocol*
LDAP.....	*LightweightDirectory Access Protocol*
PCAL.....	Política de Controle de Acesso Lógico
SEI	Sistema Eletrônico de Informações
SSH.....	*Secure Shell*

GLOSSÁRIO

Autenticidade – propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Confidencialidade – propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizada nem credenciado.

Download - termo da língua inglesa que significa transferir (baixar) um ou mais arquivos de um servidor remoto para um computador local

Firewall - recurso destinado a evitar acesso não autorizado a uma determinada rede, ou um a conjunto de redes, ou a partir dela.

Keylogger - programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Utilizado quase sempre para capturar senhas, dados bancários, informações sobre cartões de crédito e outros tipos de dados pessoais.

Pragas Virtuais - programas desenvolvidos para corromper o sistema, obter dados ou danificar demais programas instalados na máquina.

Quebra de segurança - ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

Script - conjunto de instruções.

Segurança da Informação – preservação da integridade e da confidencialidade da informação e proteção contra uso ou acesso não-autorizado ou negação do serviço a usuários autorizados.

Trojan Horse ou Cavalo de Troia - programa que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Upload - termo da língua inglesa que se referente a ação de enviar dados de um computador local para um computador ou servidor remoto, geralmente através da internet.

SUMÁRIO

INTRODUÇÃO

Trata-se de auditoria para avaliar controles relacionados a incidente de Segurança da Informação no sistema ConsigWeb.

O Sistema ConsigWeb, desenvolvido pela Dataprev e gerido pela DIRBEN, é utilizado pelos servidores do INSS para realizar consultas de histórico de crédito consignado e tem por objetivo tornar mais fácil o entendimento das informações referentes aos contratos averbados na folha de pagamento dos aposentados e pensionistas desde 2004, como também, facilitar o atendimento pelas Agências da Previdência Social, conforme Memorando-Circular Conjunto nº 12 /DIRBEN/DIRAT, de 10 de março de 2010.

O incidente de segurança envolveu:

- utilização de credenciais de acesso ao sistema ConsigWeb para acesso não autorizado, massivo e automatizado a informações de empréstimos consignados de segurados do INSS; e
- inclusão de códigos maliciosos em equipamento servidor do INSS hospedado em regime de colocation na Dataprev, visando acesso às informações disponibilizadas pelo ConsigWeb.

A avaliação foi realizada a partir da análise de informações coletadas dos sistemas Gerenciador de Identidade (GERID) e ConsigWeb, do Serviço de Diretório LDAP do INSS, relatórios técnicos emitidos pela Dataprev, além de informações fornecidas pela DTI e DIRBEN, em atendimento às Solicitações de Auditoria emitidas pela equipe de auditoria. O trabalho foi realizado no período de outubro/2019 a março/2020.

RESULTADOS DOS EXAMES

Achado 1. Inobservância da Política de Controle de Acesso Lógico (PCAL) do INSS, que trata da necessidade de normativo específico motivando e regulamentando os acessos ao sistema ConsigWeb por estagiários.

Foram identificados estagiários utilizando o perfil de acesso exclusivo para servidores. Não há norma regulamentadora de tais cadastros e tampouco perfil específico implementado no sistema para uso por estagiários. Cabe destacar que os estagiários estavam lotados nas GEX São Paulo-Centro e GEX Novo Hamburgo/RS e que seus contratos de trabalho foram encerrados no 1º semestre de 2019, mas os acessos foram concedidos no 2º semestre do referido ano, por gestor de acesso lotado na APS Feira de Santana/BA.

De acordo com o item 4.10 da PCAL, Resolução nº 413/PRES/INSS, de 20 de maio de 2014, é vedado o acesso a sistemas corporativos por estagiários, salvo os casos em que acesso seja essencial ao desempenho das atividades relacionadas à área de formação. A seguir descrição do item 4.10 da PCAL:

> *"4.10 É vedado o cadastro e consequentemente a emissão de credenciais de acesso a Sistemas Corporativos do INSS para estagiários, salvo nos casos em que o acesso a sistemas corporativos seja essencial para desempenho das atividades relacionadas à área de formação profissional do estagiário. Desta forma a emissão de credencial de acesso se dará tendo como requisito as seguintes condições:*
>
> *I - a empresa que atuar como agente de integração do estágio supervisionado deve manter Contrato direto com o INSS;*
>
> *II - o contrato de estágio supervisionado deverá conter cláusula de confidencialidade e sigilo de informações pré-estabelecido com a Administração Pública;*
>
> *III - o acesso será concedido mediante solicitação expressa de servidor do quadro do INSS, responsável pela supervisão do estágio, definindo quais informações serão disponibilizadas e eventuais restrições referentes aos dias e horários para a realização do acesso;*
>
> *IV - os acessos deverão ser realizados única e exclusivamente por necessidade do serviço; e*
>
> *V - para os acessos previstos neste item, caberá ao INSS viabilizar perfil de acesso específico limitando às atividades ao estritamente necessário. "*

Tanto a DTI quanto a DIRBEN, em suas respostas aos questionamentos realizados, afirmaram desconhecer a existência de normativos que regulamentasse os acessos ao sistema por estagiários. Citaram ainda que não existem perfis de acesso exclusivos para uso por estagiários, destacando na sua resposta os perfis (papéis) existentes para acesso ao ConsigWeb.

Tabela 1: Papéis dos Subsistemas ConsigWeb

Subsistema	Papel	Descrição
CONSIGWEB_DTP	CONSIGWEB_DTP_CONSULTA	Perfil de consulta dos empréstimos consignados da Dataprev
CONSIGWEB_MDS	CONSIGWEB_MDS_CONSULTA	Perfil de consulta dos empréstimos consignados do MDS
CONSIGWEB_INSS	CONSIGWEB_DC_MASTER	Diretoria Central Master
CONSIGWEB_INSS	CONSIGWEB_APS_ATENDENTE	Atendente da APS
CONSIGWEB_INSS	CONSIGWEB_SUP_GERENTE	Gerente da superintendência
CONSIGWEB_INSS	CONSIGWEB_GEX_SUPERVISOR	Supervisor da GEX

A DIRBEN apresenta em sua manifestação que o acesso ao sistema ConsigWeb não é essencial para o desempenho das atividades relacionadas à área de formação profissional do estagiário, conforme previsto no item 4.10 da Política de Controle de Acesso Lógico (PCAL) - Resolução nº 413/2014.

No entanto, constatou-se que foi atribuído perfil a estagiários no sistema GERID para acesso ao sistema ConsigWeb sem a observância das restrições expressas no item 4.10 da PCAL, mencionado no parágrafo anterior.

A justificativa apresentada pela DIRBEN de que o acesso atribuído a estagiários poderia ser justificado para auxílio no desempenho das atividades nas unidades do INSS, contraria a legislação legal (Lei nº 11.788, de 25 de setembro de 2008) que dispõe sobre o estágio de estudantes.

Quanto à alegação da DIRBEN de “mera consulta” no sistema ConsigWeb por estagiário, tal conduta viola o princípio da “necessidade de conhecer” definido no § 1º do art. 25 da Lei nº 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação, haja vista permitir acesso a informações sigilosas de beneficiários, cujo conteúdo deve ser permitido somente mediante autorização do titular da informação ou agentes públicos autorizados por lei.

Quanto à indagação da existência de perfil específico para estagiários para acesso ao ConsigWeb, a DIRBEN se manifestou que todos os papéis constantes na Tabela 1 acessam a mesma tela e as mesmas informações independentes da função exercida de modo que apenas um papel seria suficiente para atender a todos os perfis.

No entanto, tal afirmação contraria o que prescreve o artigo 3º da Portaria nº 2.194/PRES/INSS, de 15 de agosto de 2019 e o inciso V do item 4.10 da Resolução nº 413/PRES/INSS, de 20 de maio de 2014 (PCAL), que determina a criação de perfil específico para estagiário.

Além das impropriedades relatadas acima, verificou-se também a inexistência de mecanismo no sistema GERID que impedisse a atribuição de perfil destinado a servidores para estagiários.

Diante do exposto, concluiu-se que houve o descumprimento da Lei nº 11.788/2008, da PCAL e da Portaria nº 2.194/PRES/INSS, considerando que o acesso ao sistema ConsigWeb não é essencial para o desempenho das atividades relacionadas à área de formação profissional dos estagiários.

Achado 2. Atribuição de acesso ao sistema ConsigWeb para estagiários após data de desligamento/encerramento do estágio.

Conforme descrito no achado 1, foram identificados cadastros e acessos de estagiários ao sistema ConsigWeb após o encerramento do contrato de estágio.

O item 3.2 da PCAL – Resolução nº 413/PRES/INSS, disciplina que:

> *"3.2 A área responsável pela gestão de pessoas do INSS disponibilizará mensalmente relação de servidores e estagiários contendo obrigatoriamente as seguintes informações:*
>
> *I - nome do usuário: nome completo do servidor ou estagiário;*
>
> *II - matrícula: Registro do usuário no Sistema Integrado de Administração de Recursos Humanos – SIAPE do servidor ou estagiário;*
>
> *III - CPF: número de registro do servidor ou estagiário no Cadastro de Pessoas Físicas;*
>
> *IV - área de lotação: nome e código da unidade de lotação do servidor ou estagiário;*
>
> *V - telefone para contato: número de telefone para contato do servidor ou estagiário;*
>
> *VI - categoria: vínculo do usuário com o INSS (servidor, estagiário, etc.); e*
>
> *"VII - situação: status do servidor indicando se o mesmo encontra-se ativo, suspenso, de licença, férias, etc."*

Também no item 3.3.3 da PCAL – prevê que:

> *"3.3.3 Deverá ser viabilizada a integração de forma automática da base de dados dos servidores do Instituto ao serviço de diretório, possibilitando a aplicação imediata de uma política de gestão de usuários."*

Portanto, observou-se dos fatos relatados que não houve atendimento à prescrição da norma, pois não foi realizada a exclusão das credenciais dos estagiários no serviço diretório (LDAP) quando do encerramento do contrato de estágio, possibilitando o uso das credenciais para acesso ao sistema ConsigWeb, caracterizando assim o uso indevido "por terceiros", já que os mesmos não estavam mais em atividade no Instituto. Cabe ressaltar que tal situação pode ocorrer com os demais usuários (servidores aposentados, cedidos, falecidos, etc) no âmbito do Instituto, fragilizando a Segurança da Informação em especial o princípio da confidencialidade.

Achado 3. Ausência de comunicação eletrônica e automática referente aos procedimentos realizados no cadastramento e permissões de acessos entre os gestores e usuários.

Em agosto de 2019, a Dataprev identificou um alto número de acessos oriundos do equipamento "servidor", de responsabilidade da Secretaria de Previdência, com destino à aplicação ConsigWeb, envolvendo as credenciais de acesso.

O incidente foi reportado pela Dataprev à Diretoria de Tecnologia da Informação e Inovação (DTI) do INSS, e esta por sua vez autorizou o Centro de Tratamento de Incidente de Redes - CTIR da Dataprev a realizar a expiração das credenciais envolvidas nos acessos.

Em setembro de 2019, foram identificadas novas ocorrências utilizando novas credenciais de acesso e endereços IP distintos, de origem interna (equipamento servidor *colocation* da PFE/INSS e equipamento servidor da DATAPREV com função de Proxy) e externa (acessos VPN oriundos da África do Sul), conforme reportado pela equipe do CTIR da Dataprev.

A DTI e DIRBEN relataram ainda na sua manifestação que o sistema gerenciador de identidade (GERID) não possui funcionalidade com objetivo de notificar os usuários e gestores de acessos a respeito das permissões concedidas para acesso ao sistema ConsigWeb.

Do exposto, ficou constatado que o sistema GERID não possui mecanismos de notificação automática entre os gestores e usuários quanto aos procedimentos de cadastro de acesso realizados.

Achado 4. Impossibilidade de realizar consultas ou gerar relatórios das ações efetuadas (logs) pelos gestores de acesso e usuários diretamente no sistema.

Constatou-se a necessidade de realizar extrações de dados avulsas devido à inexistência de funcionalidade, tanto no sistema GERID quanto no ConsigWeb, que permitisse realizar consultas ou gerar relatórios das ações efetuadas (logs) pelos gestores de acesso e usuários.

Foi solicitada à DTI a disponibilização das informações de logs relativas aos usuários que acessaram o sistema ConsigWeb no período de janeiro/2019 a novembro/2019. Em resposta, a DTI informou que as ações realizadas pelos usuários são registradas em logs do próprio sistema, sendo que a consulta dessas informações depende de extração solicitada à Dataprev. Em 13/11/2019, a DTI formalizou a demanda nº DM.083669 no sistema Clarity visando o atendimento da solicitação de auditoria em questão e a Dataprev, por meio do Ofício/DERC/0755/2019, de 20/11/2019, acordou o prazo para entrega final da demanda para 30/12/2019. No entanto, até a conclusão deste relatório, não houve manifestação por parte da DTI e/ou Dataprev quanto ao atendimento da presente solicitação de auditoria.

Ressalta-se que a ausência de funcionalidade específica para obtenção direta das informações de logs impossibilita o devido acompanhamento das atividades dos usuários que utilizam o sistema, além de gerar custos adicionais ao Instituto advindos de pedidos de extrações de dados à Dataprev para verificações e análises, pelas áreas do INSS e órgãos de controle, de casos ou demandas específicas, prejudicando assim uma gestão efetiva do controle de acesso por parte do Instituto.

Diante do exposto, concluiu-se que as áreas auditadas não dispõem de ferramentas ou recursos tecnológicos que possam auxiliar na gestão efetiva do controle acesso ao sistema, dependendo em grande medida de informações enviadas pela Dataprev e de notificações internas realizadas por gestores e usuários.

Achado 5. Concessão de acesso ao sistema ConsigWeb para servidor perito médico previdenciário, cujas atribuições são incompatíveis com os perfis de atendimento administrativo, contrariando os itens 4.12 e 4.13 da PCAL.

Foi constatada a utilização de contas de usuários pertencentes a servidores com cargo de "perito médico previdenciário" para realizar acessos ao sistema ConsigWeb.

A DIRBEN informou que não há uma justificativa para os acessos atribuídos aos servidores ocupantes do cargo de perito médico previdenciário, pois as atividades exercidas por estes não são compatíveis com as atividades de atendimento que dependem das informações sobre consignações disponibilizadas pelo sistema ConsigWeb.

Constatou-se também que o sistema GERID não é capaz de diferenciar as categorias de usuários (servidores ou estagiários), ou seja, possibilita o cadastro de perfil a qualquer usuário sem observar o cargo, as atividades exercidas e o princípio da "necessidade de conhecer", deixando a cargo do gestor de acesso realizar tal controle, fato que fragiliza os controles e a segurança da informação.

Achado 6. Concessão de acesso ao sistema ConsigWeb realizada por gestor de acesso de APS para usuários fora da sua área de abrangência, contrariando o inciso II do item 6.3.9 da PCAL.

O gestor de acesso em exercício na função de Gerente de Agência, lotado na APS Feira de Santana/BA, foi capaz de atribuir perfil de acesso ao sistema ConsigWeb para servidores e estagiários lotados em unidades fora da sua abrangência.

Constatou-se que o sistema GERID permitiu o cadastro e liberação de acessos ao sistema ConsigWeb para usuários de fora da área de lotação e exercício do gestor de acesso da APS, contrariando o inciso II, do item 6.3.9, da PCAL, Resolução nº 413/2014.

Diante do exposto, concluiu-se que a ausência de funcionalidade no GERID que restrinja ou impeça permissão de acesso para usuários fora da área de lotação do gestor de acesso da APS contraria o inciso II, do item 6.3.9 da PCAL. Além disso, expõe os colaboradores ao risco de ter permissão de acesso estranha a sua lotação e área de atuação, conforme constatado no presente incidente.

Achado 7. A autenticação no sistema ConsigWeb se dá predominantemente por meio de *(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*.

Constatou-se que o acesso ao sistema ConsigWeb é realizado predominantemente por meio de ***(informação suprimida por solicitação da unidade auditada, em função de***

restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020). Este método possui certa ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***, considerando que a autenticação utiliza duas informações ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** que podem ser ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***. Acrescenta-se que os equipamentos no ambiente de trabalho nas unidades de atendimento (APS) são utilizados de ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** e que não há autenticação dos usuários por meio de ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS de 21/10/2020)***, mas somente autenticação por ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***.

A utilização de autenticação de multifatores é recomendada pelo item 6.1.7. da Norma Complementar n.º 07/IN01/DSIC/GSIPR de 15 julho de 2014. Esse método de autenticação possui um nível maior de segurança, pois além de senha para realização da autenticação torna-se necessário o uso de um dispositivo físico, tanto no formato de um cartão inteligente (que depende de uma leitora) ou de um token (similar a um *pendri*ve) para validação da credencial de acesso. Ademais, possibilita auditorias das ações maliciosas que possam ocorrer no sistema.

Logo, concluiu-se que o tipo de acesso predominante no sistema ConsigWeb apresenta ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***, pois os dados de ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** podem ser ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***. Desta forma, a orientação prevista no item 6.1.7 da Norma Complementar nº 07/IN01/DSIC/GSIPR não foi satisfatoriamente atendida até o presente momento.

Achado 8. O Gerenciador de Identidade (GERID) permitiu acesso ao sistema ConsigWeb por usuário com senha expirada no LDAP.

Verificou-se na avaliação do incidente que, em 02/09/2019, foram realizados acessos ao sistema ConsigWeb utilizando as credenciais de acesso com senha expirada no serviço de diretório (LDAP) desde 20/12/2018.

O acesso ao sistema ConsigWeb por usuário com senha expirada no LDAP, configurou uma fragilidade existente no GERID que pode comprometer a confiabilidade do sistema e impactar na segurança da informação. Este fato contrariou as boas práticas definidas na NBR ISO / IEC 27.002/2013, pois permitiu o acesso a informações por usuário com senha expirada.

Devido à necessidade de redirecionamento à Dataprev para obtenção das informações que esclareceriam a causa do evento, constatou-se que o INSS não tem condição de detectar nem de esclarecer os acessos realizados por usuários com senhas expiradas no LDAP.

Achado 9. O INSS não comunicou o incidente de Segurança da Informação do sistema ConsigWeb ao Centro de Tratamento de Incidentes de Redes de Governo (CTIR-GOV), conforme previsto na Norma Complementar nº 08/IN01/DSIC/GSI-PR, de 19/08/2010.

Constatou-se que o INSS não comunicou o incidente ao Centro de Tratamento de Incidentes de Redes de Governo (CTIR – GOV) conforme previsto na Norma Complementar nº 08 /IN01/DSIC/GSI-PR, de 19/08/2010, que define Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal.

De acordo com as informações prestadas pela DTI, o incidente de segurança da informação não foi reportado ao CTIR-GOV, tendo em vista que o mesmo somente recebe incidentes de outros CTIR's. Informou ainda que o INSS não possui Equipe de Tratamento de Incidente de Redes - ETIR implantada e que tais incidentes serão reportados pelo CTIR-Dataprev.

Cumpre esclarecer que o incidente em questão envolveu equipamento servidor sob responsabilidade do INSS e utilização de credenciais de acesso pertencentes a servidores e estagiários da Autarquia, portanto, caberia ao INSS a responsabilidade pela comunicação do incidente ao CTIR-GOV, pois existe normativo do GSI-PR, Norma Complementar nº 05 /IN01/DSIC/GSIPR, de 14/08/2009, que determina a implementação da ETIR nos órgãos da Administração Pública Federal, direta e indireta.

Apesar de se constatar a inexistência da ETIR no INSS, evidenciaram-se algumas providências adotadas para tratamento do incidente e controle de acesso, como: a) o bloqueio e reinicialização das credenciais envolvidas no incidente; b) o servidor em colocation foi retirado do ar em 18/10/2019; e c) o tratamento do incidente foi realizado pelas equipes da diretoria.

Conforme avaliação realizada no GERID, constatou-se que os perfis de acesso existentes no GERID não foram desativados, visto que são utilizados pelos servidores do INSS. Já as credenciais dos estagiários envolvidos no incidente e que possuíam acesso por meio destes perfis foram devidamente bloqueados ou tiveram suas senhas reinicializadas no serviço de diretório LDAP.

Do exposto, concluiu-se o que o incidente não foi reportado ao CTIR-GOV devido à inexistência de ETIR estabelecida no INSS, ficando a cargo do CTIR-Dataprev comunicar o incidente. Cabe ressaltar que o INSS adotou algumas providências visando mitigar o incidente, conforme o descrito acima.

Achado 10. Deficiência na gestão de acesso ao equipamento servidor em *colocation* na Dataprev.

Observou-se que a gestão de acesso ao equipamento servidor destinado a hospedar aplicações da Procuradoria Federal Especializada (PFE/INSS), alocado no *Data Center* da Dataprev (*contrato colocation*), não possui uma estrutura formal, pois não há normativo interno instituindo regras de "acesso e controle".

Verificou-se que o acesso ao equipamento é realizado ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***.

Segundo manifestação da DTI, não há normativo tratando da estrutura, regras e procedimentos relativo à gestão de acesso ao equipamento servidor em *colocation* e que adota a forma de acesso ao equipamento ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***. Além disso, a DTI informou que ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***.

Concluiu-se, do exposto, que há ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** ao equipamento servidor, devido ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** e tampouco de ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** ocasionando uma que eventualmente mudaram de lotação ou de atribuições funcionais.

Achado 11. Ausência de *(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)* e de ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** no

equipamento servidor em *colocation*.

Constatou-se que o sistema operacional do equipamento servidor ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***. Além disso, ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***.

De acordo com a manifestação da DTI o equipamento servidor ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** em virtude de o mesmo ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***, e, em caso de atualização, ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***. Em relação à checagem ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***, a área relatou a ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** de realizar o ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***, em virtude da existência do ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** ativo no equipamento e que, além disso, a DTI ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***.

Concluiu-se que a DTI enfrenta diversos desafios, dentre eles, dificuldade ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***, que em caso de ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** poderá ocasionar ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** no equipamento.

Achado 12. ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** **configuradas no equipamento servidor em *colocation*.**

De acordo com as informações prestadas pela DTI o equipamento servidor ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***.

Além disso, ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** pela DTI ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** e ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***, para o equipamento servidor em “colocation”.

Concluiu-se, do exposto, que existem medidas de prevenção a ataques cibernéticos ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** e para o ambiente de rede. Já em relação ao equipamento servidor ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)*** implementados para proteção do sistema e serviços hospedados, ***(informação suprimida por solicitação da unidade auditada, em função de restrição de acesso na forma do Art. 31 da Lei nº 12.527/2011, do Art. 56 do Decreto nº 7.724/2012 e do inciso I, §3º do Art. 3º da Portaria nº 1.089/PRES/INSS, de 21/10/2020)***.

RECOMENDAÇÕES

1. Cessar os acessos de estagiários ao sistema ConsigWeb, por este não ser essencial ao desempenho das atividades relacionadas à área de formação profissional do estagiário, conforme resposta da área auditada à Solicitação de Auditoria nº 34.825/2019.

Achado nº 01

2. Implantar um mecanismo de trava no sistema GERID que impeça a atribuição de perfil de acesso destinado a servidor para uso por estagiário.

Achado nº 01

3. Promover a atualização contínua das bases de dados de usuários do LDAP, bem como a integração com a base de dados dos servidores do Instituto (SIAPE-INSS), conforme preceitua os itens 3.2 e 3.3 da PCAL – Resolução nº 413/PRES/INSS, de 20 de maio de 2014.

Achado nº 02

4. Implementar mecanismo eletrônico e automatizado no GERID para notificação dos gestores de acesso e usuários visando informá-los a respeito dos cadastros e das permissões de acessos concedidas.

Achado nº 03

5. Disponibilizar solução tecnológica (módulo de auditoria) que permita à DTI, ou partes afins, consultar informações (logs) que demonstrem as ações efetuadas pelos usuários nos sistemas GERID e ConsigWeb.

Achado nº 04

6. Cessar acessos atuais e bloquear futuros acessos ao sistema ConsigWeb para perito médico previdenciário e demais cargos com atribuições incompatíveis, observando-se o princípio da “necessidade de conhecer”, as atribuições funcionais e atividades desenvolvidas pelos servidores, conforme item 4.12 da PCAL - Resolução nº 413/PRES/INSS, de 20 de maio de 2014.

Achado nº 05

7. Garantir que o sistema GERID esteja aderente à nova Norma de Controle de Acesso (NCAL), que se encontra em fase de aprovação e publicação, quanto às regras estabelecidas para emissão de credenciais de acesso lógico no âmbito do INSS.

Achado nº 06

8. Reavaliar o processo de autenticação de acesso ao GERID de forma que o mesmo esteja alinhado ao item 6.1.7 da Norma Complementar nº 07/IN01/DSIC/GSIPR, quanto a utilização de autenticação de multifatores.

Achado nº 07

9. Revisar os requisitos de validação de senha entre os sistemas GERID e o LDAP, a fim de garantir as sincronizações com as devidas permissões.

Achado nº 08

10. Implantar Equipe de Tratamento de Incidentes de Redes (ETIR), conforme Norma Complementar nº 08/IN 01/DSIC/GSI-PR/2010 para que os eventuais incidentes de segurança da informação sejam reportados ao CTIR-GOV.

Achado nº 09

11. Adequar a forma de autenticação e acesso de usuários no servidor ao nível de criticidade dos dados.

Achado nº 10

12. Avaliar periodicamente se o nível de segurança da aplicação e das plataformas que a sustentam são compatíveis com o risco que a administração definir como aceitável.

Achado nº 11 e 12

CONCLUSÕES

Após análise do incidente de Segurança da Informação e Comunicação no sistema ConsigWeb, reportado pela Diretoria de Tecnologia da Informação e Inovação (DTI) por meio da Nota Informativa nº 1 /SSEG/DTI/INSS, de 17 de setembro de 2019, a equipe de auditoria identificou:

1. Quebra do princípio da autenticidade e confidencialidade;
2. Consultas indevidas a informações e dificuldade de identificação do agente causador;
3. Concessão de perfil de acesso ao sistema para usuários com atribuições incompatíveis as atividades exercidas;
4. Inexistência de ferramenta para consulta e geração de relatórios de logs do sistema;
5. Excesso de burocracia para extração e obtenção de dados (envolvimento de vários atores do INSS e Dataprev) e incidência de custos adicionais;
6. Acessos automatizados indevidamente ao sistema ConsigWeb por meio de robô;
7. Vulnerabilidades a ataques internos e externos;
8. Ausência de Equipe de Tratamento de Incidente de Rede (ETIR) no Instituto;
9. Deficiência na gestão de acesso ao equipamento servidor em *colocation* na Dataprev por falta de padronização formal no cadastro e acesso ao servidor por meio físico e remoto;
10. Fragilidade na segurança, na guarda e na manutenção de informações; e
11. Inclusão de conteúdos no servidor *colocation* por agentes não autorizados.

Cumpre lembrar que a maioria das fragilidades apontadas neste relatório já foi objeto de recomendações oriundas de ações de auditoria realizadas em 2010, 2011 e 2012, sob nº 03/2010, 19/2011 e 17/2012, respectivamente, que se tivessem sido implementadas pelo INSS poderiam ter contribuído para mitigar o presente incidente.

Convém destacar que o INSS não desenvolve, de forma contínua, a disseminação da cultura de segurança da informação visando à proteção individual e coletiva dos seus dados.

Dessa forma, torna-se urgente a necessidade de implantar uma ETIR no âmbito do INSS e aprimorar seus sistemas de acesso, atendendo às normas e boas práticas de segurança da informação, preconizadas nacional (GSI/PR) e internacionalmente (ISO 27.001/2013 e 27.002/2013), considerando o universo de dados pessoais e financeiros mantidos pelo Instituto.

Por fim, espera-se que com o cumprimento das recomendações emanadas neste relatório, haja melhorias nos controles relativos à gestão de acesso aos sistemas e equipamentos servidores, contribuindo para:

- O restabelecimento do princípio da “segregação de funções” de servidores administrativos, médicos peritos previdenciários e estagiários;
- Aprimoramento do monitoramento de controle de acessos de gestores e usuários pelas áreas afins;
- Facilitação da atuação da auditoria interna e demais órgãos de controle; eliminação de custos adicionais decorrentes da necessidade de extrações de dados de forma avulsa;
- Observância das normas vigentes; e
- Garantia dos princípios de Segurança da Informação no que se refere à autenticidade, confidencialidade, integridade e disponibilidade.

ANEXO I – MANIFESTAÇÃO DA UNIDADE AUDITADA

A manifestação da Unidade Auditada foi remetida à Equipe de Auditoria por meio do Despacho SEI_INSS nº 0816878, do Serviço de Segurança em Tecnologia da Informação e Comunicação, de 15 de maio de 2020, encaminhando as informações integralmente reproduzidas em sequência.

"1. Trata-se do Relatório Preliminar (0739224) da Ação 5540/2019 - Auditoria de Avaliação do Incidente de Segurança no Sistema CONSIGWEB.

2. Após reunião entre as equipes da AUDGER e da DTI, para entendimento do relatório de Avaliação do Incidente de Segurança no Sistema CONSIGWEB relativa a ação nº 5540/2019, segue os apontamentos da Equipe SSEG/DTI quanto as recomendações descritas:

2.1. Recomendação 1: Cessar os acessos de estagiários ao sistema CONSIGWEB, por este não ser essencial ao desempenho das atividades relacionadas à área de formação profissional do estagiário, conforme resposta da área auditada à Solicitação de Auditoria nº 34.825/2019. Achado nº 01

Manifestação DTI: De acordo com a Norma Complementar nº 10/IN01/DSIC/GSIPR, de 20 de janeiro de 2012, o proprietário do ativo de informação refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

A mesma norma define ainda as responsabilidades do proprietário do ativo de informação, que deve assumir, no mínimo, as seguintes atividades:

a) descrever o ativo de informação;

b) definir as exigências de segurança da informação e comunicações do ativo de informação;

c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;

d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo; e,

e) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação;

Sendo assim, a definição de quem deve ou não acessar as informações disponibilizadas no CONSIGWEB deve ser feita pela área de negócio responsável pelo sistema.

No entanto, a DTI tem atuado no processo de concessão de acesso aos sistemas corporativos a partir da tramitação do processo SEI nº 35014.003440/2019-62 em resposta a Nota de Auditoria nº: 1/AUDGER/INSS (0002187) emitida tendo em vista a publicação da Portaria nº 2.194/PRES/INSS, de 15 de agosto de 2019.

Esta ação gerou manifestação das áreas envolvidas na questão, por meio do Ofício SEI Circular Conjunto nº 45/DIRBEN/DIRAT/DTI/DGPA (0125511).

Este entendimento, acerca da necessidade da implementação de perfis de acesso específico para as atividades dos estagiários, é mantido na Norma de Controle de Acesso Lógico (0411838) que irá substituir a atual Política de Controle de Acesso Lógico - PCAL, mais especificamente no Inciso XIV, do Artigo 5º que trata do credenciamento de estagiários.

2.2. Recomendação 2: Implantar um mecanismo de trava no sistema GERID que impeça a atribuição de perfil de acesso destinado a servidor para uso por estagiário. Achado nº 01

Manifestação DTI: Esta regra pode ser objeto de discussão e demandada pela DTI para a Dataprev, no entanto tem como premissa a criação dos perfis específicos para estagiários.

2.3. Recomendação 3: Promover a atualização contínua das bases de dados de usuários do LDAP, bem como a integração com a base de dados dos servidores do Instituto (SIAPE-INSS), conforme preceitua os itens 3.2 e 3.3 da PCAL – Resolução nº 413/PRES/INSS, de 20 de maio de 2014. Achado nº 02

Manifestação DTI: A DTI está promovendo reuniões técnicas envolvendo membros da Diretoria de Gestão de Pessoas e Administração - DGPA e a Dataprev para definir um processo de trabalho e um conjunto de informações que devem ser enviadas periodicamente pelo INSS para permitir a atualização da base do LDAP.

Esta integração busca efetivar as diretrizes contidas na PCAL-INSS que serão aprimoradas na proposta da atualização da norma.

2.4. Recomendação 4: Implementar mecanismo eletrônico e automatizado no GERID para notificação dos gestores de acesso e usuários visando informá-los a respeito dos cadastros e das permissões de acessos concedidas. Achado nº 03

Manifestação DTI: Deverá ser retomada as negociações com a Dataprev para a implantação da ferramenta de mensageira no GERID, a fim de flexibilizar a comunicação da concessão, alteração e exclusão dos perfis de acesso e de gestão por parte dos gestores de acesso.

2.5. Recomendação 5: Disponibilizar solução tecnológica (módulo de auditoria) que permita à DTI, ou partes afins, consultar informações (logs) que demonstrem as ações efetuadas pelos usuários nos sistemas GERID e ConsigWeb. Achado nº 04

Manifestação DTI: As tratativas para disponibilização de um módulo de auditoria, onde seja possível consultar informações dos logs registrados pelo sistema GerID, já foram iniciadas com a Dataprev. No entanto tais informações se restringem apenas aos acessos concedidos no GERID, não sendo aplicadas aos sistemas parceiros.

Para que tal ação englobe ações transacionais dos sistemas corporativos, caso do CONSIGWEB, a área responsável pela gestão do sistema deve cadastrar demanda junto a Dataprev definindo tais requisitos.

2.6. Recomendação 6: Cessar acessos atuais e bloquear futuros acessos ao sistema CONSIGWEB para perito médico previdenciário e demais cargos com atribuições incompatíveis, observando-se o princípio da "necessidade de conhecer", as atribuições funcionais e atividades desenvolvidas pelos servidores, conforme item 4.12 da PCAL - Resolução nº 413/PRES/INSS, de 20 de maio de 2014. Achado nº 05

Manifestação DTI: Todo acesso à informação deve ser motivado pela necessidade de conhecer. O INSS não tem uma política de acesso orientada pelo cargo ocupado pelos usuários (servidores do quadro) e a DTI não tem esta atribuição regimental (conforme descrito no item 2.1. deste despacho).

Quanto a diferenciar as categorias de usuários, o GERID funciona com perfis de acesso criados pelos gestores dos sistemas corporativos. A informação do cargo é inserida no cadastro do usuário no LDAP. Atualmente, esse alinhamento depende de uma questão processual, o sistema GERID não faz essa crítica por perfil x cargo. Para este item ser atendido dependerá de uma de análise da área de negócio (responsável pela gestão do sistema) e possível evolução na ferramenta.

2.7. Recomendação 7: Implementar mecanismo no GERID visando garantir as atribuições e responsabilidades previstas no item 6.3 da PCAL - Resolução nº 413/PRES/INSS, de 20 de maio de 2014. Achado nº 06

Manifestação DTI: Devido à necessidade de mutirões de trabalho nas unidades do INSS foi implementado nas regras do GERID, que um gestor de acesso pode atribuir perfis de acesso a servidores que outras unidades (UO) na sua abrangência de acordo com a necessidade de trabalho. Esta regra está de acordo com processo de trabalho estabelecido pelas áreas de negócio a época do desenvolvimento e implantação do GERID.

Se houver manifestação formal das áreas de negócio, solicitando que tal regra seja alterada (limitando o cadastro de acessos à unidade de lotação do gestor), a DTI pode demandar a mudança para a Dataprev.

2.8. Recomendação 8: Garantir que autenticação de acesso ao GERID esteja alinhada ao item de conclusão do Relatório Incidente de Segurança nº 201908002502, da Dataprev, que recomenda: "O acesso ao Sistema GERID deve ser restrito a endereços IP nacionais e devem ser realizados utilizando um Certificado Digital do tipo A3, visando aumentar o nível de segurança com relação aos acessos realizados e auditorias para ações maliciosas que possam ocorrer no sistema". Achado nº 07

Manifestação DTI: A possibilidade do uso de certificado digital por parte dos gestores de acesso dos sistemas corporativos parceiros ao GERID e dos usuários está sendo analisado pela DTI, Áreas de Negócio do INSS e Dataprev. No entanto, cabe esclarecer que o contrato em vigência firmado com o SERPRO para emissão de Certificados Digitais, tem um estoque (contratado) limitado e não contempla os gestores dos sistemas corporativos do GERID. Uma nova contratação está sendo iniciada para contemplar certificados digitais para todos os servidores do INSS, o que poderá atender a questão de autenticação de acesso o sistema CONSIGWEB ser simples, ou seja, realizado somente por meio de "usuário e senha".

2.9. Recomendação 9: Revisar os requisitos de validação de senha entre os sistemas GERID e o LDAP, a fim de garantir as sincronizações com as devidas permissões. Achado nº 08

Manifestação DTI: A atualização periódica dos cadastros dos usuários no OpenLdap possibilitará maior segurança na autenticação do sistema GERID, que utiliza a mesma senha de acesso registrada no OpenLdap.

A Dataprev já foi notificada pela DTI acerca dos problemas com senhas expiradas de usuários que continuavam ativos no GERID, no entanto ainda não apresentou uma resposta acerca do assunto.

2.10. Recomendação 10: Implantar Equipe de Tratamento de Incidentes de Redes (ETIR), conforme Norma Complementar nº 08/IN 01/DSIC/GSI-PR/2010 para que os eventuais incidentes de segurança da informação sejam reportados ao CTIR-GOV. Achado nº 09

Manifestação DTI: A DTI propôs norma que institui a Equipe de Tratamento de Incidentes de Redes – ETIR-INSS (SEI processo nº 35014.047735/2020-84). Tal proposta foi analisa e aprovada pelo Comitê Estratégico de Governança - CEGOV do INSS e aguarda os trâmites necessários para sua publicação.

2.11. Recomendação 11: Adequar a forma de autenticação e acesso de usuários no servidor ao nível de criticidade dos dados. Achado nº 10

Manifestação DTI: Os acessos locais aos servidores foram atualizados, estes acessos são restritos aos administradores de rede da DTI. Será analisado a criação de um POP (Procedimento Operacional Padrão) para formalizar os procedimentos de acesso aos equipamentos. Por serem acessos somente realizados e controlados pelos administradores da DTI este procedimento pode fazer parte de um processo da unidade de TIC ou inserido em uma Norma Complementar ou na Norma de controle de Acesso Lógico.

2.12. Recomendação 12: Avaliar periodicamente se o nível de segurança da aplicação e das plataformas que a sustentam são compatíveis com o risco que a administração definir como aceitável. Achado nº 11 e 12

Manifestação DTI: A DTI elaborará um relatório a cada 06 meses de acompanhamento dos níveis de segurança dos recursos de TIC, incluindo os ambientes e aplicações do INSS. Os itens de TIC comuns serão migrados para o ambiente contratado da AWS e um dos pré-requisitos é a atualização do ambiente operacional desses itens de TIC (sistemas operacionais, servidores de aplicação, ...). As checagens dos ativos de TIC em menor periodicidade ficam prejudicadas pela DTI ter uma equipe técnica reduzida e uma grande quantidade de itens de TIC. A DTI buscará formas de otimizar esse monitoramento do ambiente.

Quanto às ferramentas de prevenção, detecção e eliminação de pragas virtuais e ataques cibernéticos, este tratamento é feito nos limites da rede pelo prestador de serviço. A defasagem tecnológica é outro fator inibidor de utilização local dessas ferramentas, o que deverá ser mitigado com a disponibilização de ambientes atualizados para migração ao ambiente AWS.

3. Encaminhe-se à Coordenação-Geral de Infraestrutura e Operações, para conhecimento e considerações cabíveis.

ALEXINALDO MESSIAS CERQUEIRA
Chefe do Serviço de Segurança em Tecnologia da Informação e Comunicação”

ANEXO II – ANÁLISE DA EQUIPE DE AUDITORIA

A Diretoria de Tecnologia da Informação e Inovação (DTI) apresentou suas manifestações conforme Anexo I deste Relatório, pelo o que passamos a proceder à seguinte análise e considerações:

Manifestação da Unidade Examinada: recomendação nº 01 (achado nº 01)

Em relação à recomendação nº 01, achado nº 01, que trata da cessação de acessos de estagiários ao sistema ConsigWeb, a DTI apresentou a seguinte manifestação:

"2.1. Recomendação 1: Cessar os acessos de estagiários ao sistema CONSIGWEB, por este não ser essencial ao desempenho das atividades relacionadas à área de formação profissional do estagiário, conforme resposta da área auditada à Solicitação de Auditoria nº 34.825/2019. Achado nº 01

Manifestação DTI: De acordo com a Norma Complementar nº 10/IN01/DSIC/GSIPR, de 20 de janeiro de 2012, o proprietário do ativo de informação refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

A mesma norma define ainda as responsabilidades do proprietário do ativo de informação, que deve assumir, no mínimo, as seguintes atividades:

a) descrever o ativo de informação;

b) definir as exigências de segurança da informação e comunicações do ativo de informação;

c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;

d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo; e,

e) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação;

Sendo assim, a definição de quem deve ou não acessar as informações disponibilizadas no CONSIGWEB deve ser feita pela área de negócio responsável pelo sistema.

No entanto, a DTI tem atuado no processo de concessão de acesso aos sistemas corporativos a partir da tramitação do processo SEI nº 35014.003440/2019-62 em resposta a Nota de Auditoria nº: 1/AUDGER/INSS (0002187) emitida tendo em vista a publicação da Portaria nº 2.194/PRES/INSS, de 15 de agosto de 2019.

Esta ação gerou manifestação das áreas envolvidas na questão, por meio do Ofício SEI Circular Conjunto nº 45/DIRBEN/DIRAT/DTI/DGPA (0125511).

Este entendimento, acerca da necessidade da implementação de perfis de acesso específico para as atividades dos estagiários, é mantido na Norma de Controle de Acesso Lógico (0411838) que irá substituir a atual Política de Controle de Acesso Lógico - PCAL, mais especificamente no Inciso XIV, do Artigo 5º que trata do credenciamento de estagiários."

Análise da Equipe de Auditoria

Após análise da manifestação da Unidade Auditada, a equipe de auditoria concorda com as indagações realizadas, mas, é importante destacar que:

A Norma Complementar nº 10/IN01/DSIC/GSIPR, além das definições mencionadas na manifestação da DTI, define que:

> *"3.8 Custodiante do ativo de informação - refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação;"*

Além disso, a DIRBEN se manifestou em relação os acessos ao sistema ConsigWeb atribuídos a estagiários, tendo a mesma destacado que o referido sistema não é essencial ao desempenho das atividades relacionadas à área de formação profissional do estagiário, devendo-se, portanto, aplicar a vedação expressa no item 4.10 da PCAL.

Quanto ao fato de a DTI afirmar que "a definição de quem deve ou não acessar as informações disponibilizadas no CONSIGWEB deve ser feita pela área de negócio responsável pelo sistema", cumpre esclarecer que a própria área de negócio já se manifestou em relação aos acessos por estagiários ao sistema conforme mencionando no parágrafo anterior.

Do exposto, conclui-se que a DTI, como área responsável pela gestão de TI, tem a responsabilidade de aplicar os controles de segurança em conformidade com as exigências de segurança comunicadas pelo proprietário do ativo de informação. Deve, portanto, realizar as exclusões dos acessos de estagiários ao referido sistema.

Manifestação da Unidade Examinada: recomendação nº 02 (achado nº 01)

Quanto à recomendação nº 02, achado nº 01, que trata da implantação de mecanismo de trava no sistema GERID que impeça a atribuição de perfil de acesso destinado a servidor para uso por estagiário, a DTI apresentou a seguinte manifestação:

"2.2. Recomendação 2: Implantar um mecanismo de trava no sistema GERID que impeça a atribuição de perfil de acesso destinado a servidor para uso por estagiário. Achado nº 01

Manifestação DTI: Esta regra pode ser objeto de discussão e demandada pela DTI para a Dataprev, no entanto tem como premissa a criação dos perfis específicos para estagiários."

Análise da Equipe de Auditoria

De acordo com a DIRBEN, o sistema ConsigWeb não é essencial ao desempenho das atividades relacionadas à área de formação profissional do estagiário. Portanto, conclui-se que os perfis/papéis ativos atualmente para acesso ao sistema ConsigWeb são destinados exclusivamente para uso por servidores do INSS. Dessa forma, a atribuição desses perfis para estagiários deveria ser bloqueada pelo sistema GERID. Além disso, com base na manifestação da área de negócio, conclui-se que não devem existir perfis exclusivos atribuídos a estagiários para acesso ao referido sistema.

Manifestação da Unidade Examinada: recomendação nº 03 (achado nº 02)

No que diz respeito a recomendação 3, achado nº 4, que trata da atualização contínua das bases de dados de usuários do LDAP, bem como a integração com a base de dados dos servidores do Instituto (SIAPE-INSS), a DTI apresentou a seguinte manifestação:

"2.3. Recomendação 3: Promover a atualização contínua das bases de dados de usuários do LDAP, bem como a integração com a base de dados dos servidores do Instituto (SIAPE-INSS), conforme preceitua os itens 3.2 e 3.3 da PCAL – Resolução nº 413/PRES/INSS, de 20 de maio de 2014. Achado nº 02

Manifestação DTI: A DTI está promovendo reuniões técnicas envolvendo membros da Diretoria de Gestão de Pessoas e Administração - DGPA e a Dataprev para definir um processo de trabalho e um conjunto de informações que devem ser enviadas periodicamente pelo INSS para permitir a atualização da base do LDAP.

Esta integração busca efetivar as diretrizes contidas na PCAL-INSS que serão aprimoradas na proposta da atualização da norma."

Análise da Equipe de Auditoria

Observou-se da manifestação da DTI que estão em curso ações e tratativas no sentido de definir um processo de trabalho para realizar a atualização periódica da base de dados de usuários do serviço de diretório (LDAP) e com isso atender as diretrizes definidas na PCAL-INSS.

Manifestação da Unidade Examinada: recomendação nº 04 (achado nº 03)

Em relação à recomendação nº 04, achado nº 03, que trata da implantação de mecanismo eletrônico e automatizado no GERID para notificação dos gestores de acesso e usuários visando informá-los a respeito dos cadastros e das permissões de acessos concedidas, a DTI informou que:

"2.4. Recomendação 4: Implementar mecanismo eletrônico e automatizado no GERID para notificação dos gestores de acesso e usuários visando informá-los a respeito dos cadastros e das permissões de acessos concedidas. Achado nº 03

Manifestação DTI: Deverá ser retomada as negociações com a Dataprev para a implantação da ferramenta de mensageira no GERID, a fim de flexibilizar a comunicação da concessão, alteração e exclusão dos perfis de acesso e de gestão por parte dos gestores de acesso."

Análise da Equipe de Auditoria

Conforme relato da DTI, deverá ser retomada junto a Dataprev negociação para a implantação de ferramenta no GERID que permita a flexibilização da comunicação da concessão, alteração e exclusão dos perfis de acesso e de gestão por parte dos gestores de acesso.

Diante da situação relatada no achado nº 03, e visando mitigar o risco de que algum usuário, seja gestor de acesso ou usuário comum, tenha as suas credenciais de acesso utilizadas indevidamente por terceiros, a notificação eletrônica e automatizada é uma forma de aumentar o nível de segurança e garantir maior transparência.

Manifestação da Unidade Examinada: recomendação nº 05 (achado nº 04)

Quanto a recomendação nº 05, achado nº 04, que trata da disponibilização de solução tecnológica (módulo de auditoria) que permita consultar informações de logs dos sistemas GERID e ConsigWeb, a DTI se pronunciou que:

"2.5. Recomendação 5: Disponibilizar solução tecnológica (módulo de auditoria) que permita à DTI, ou partes afins, consultar informações (logs) que demonstrem as ações efetuadas pelos usuários nos sistemas GERID e ConsigWeb. Achado nº 04

Manifestação DTI: As tratativas para disponibilização de um módulo de auditoria, onde seja possível consultar informações dos logs registrados pelo sistema GerID, já foram iniciadas com a Dataprev. No entanto tais informações se restringem apenas aos acessos concedidos no GERID, não sendo aplicadas aos sistemas parceiros.

Para que tal ação englobe ações transacionais dos sistemas corporativos, caso do CONSIGWEB, a área responsável pela gestão do sistema deve cadastrar demanda junto a Dataprev definindo tais requisitos."

Análise da Equipe de Auditoria

A DTI afirmou que já foram iniciadas tratativas junto à Dataprev para que haja a disponibilização de um módulo de auditoria para consultas de informações dos logs registrados no sistema GERID. Essa iniciativa, no entanto, não contempla o ConsigWeb, na condição de sistema parceiro, ou seja, não resolve o problema apontado.

Manifestação da Unidade Examinada: recomendação nº 06 (achado nº 05)

A DTI apresentou a seguinte manifestação a respeito da recomendação nº 06, achado nº 05, que trata da cessação de acessos atuais e futuros ao sistema ConsigWeb para perito médico previdenciário e demais cargos com atribuições incompatíveis:

"2.6. Recomendação 6: Cessar acessos atuais e bloquear futuros acessos ao sistema CONSIGWEB para perito médico previdenciário e demais cargos com atribuições incompatíveis, observando-se o princípio da "necessidade de conhecer", as atribuições funcionais e atividades desenvolvidas pelos servidores, conforme item 4.12 da PCAL - Resolução nº 413/PRES/INSS, de 20 de maio de 2014. Achado nº 05

Manifestação DTI: Todo acesso à informação deve ser motivado pela necessidade de conhecer. O INSS não tem uma política de acesso orientada pelo cargo ocupado pelos usuários (servidores do quadro) e a DTI não tem esta atribuição regimental (conforme descrito no item 2.1. deste despacho).

Quanto a diferenciar as categorias de usuários, o GERID funciona com perfis de acesso criados pelos gestores dos sistemas corporativos. A informação do cargo é inserida no cadastro do usuário no LDAP. Atualmente, esse alinhamento depende de uma questão processual, o sistema GERID não faz essa crítica por perfil x cargo. Para este item ser atendido dependerá de uma de análise da área de negócio (responsável pela gestão do sistema) e possível evolução na ferramenta."

Análise da Equipe de Auditoria

A recomendação trata de cessar os acessos ao sistema ConsigWeb por perito médico e outros cargos com atribuições incompatíveis. Caberá a DTI definir a melhor forma de implementar a recomendação, podendo fazê-lo em conjunto com a DIRBEN, se entender pertinente.

Manifestação da Unidade Examinada: recomendação nº 07 (achado nº 06)

Em relação à recomendação nº 07, achado nº 06, que trata da implementação de mecanismo no GERID visando garantir as atribuições e responsabilidades previstas no item 6.3 da PCAL, a DTI realizou a seguinte manifestação:

"2.7. Recomendação 7: Implementar mecanismo no GERID visando garantir as atribuições e responsabilidades previstas no item 6.3 da PCAL - Resolução nº 413/PRES/INSS, de 20 de maio de 2014. Achado nº 06

Manifestação DTI: Devido à necessidade de mutirões de trabalho nas unidades do INSS foi implementado nas regras do GERID, que um gestor de acesso pode atribuir perfis de acesso a servidores que outras unidades (UO) na sua abrangência de acordo com a necessidade de trabalho. Esta regra está de acordo com processo de trabalho estabelecido pelas áreas de negócio a época do desenvolvimento e implantação do GERID.

Se houver manifestação formal das áreas de negócio, solicitando que tal regra seja alterada (limitando o cadastro de acessos à unidade de lotação do gestor), a DTI pode demandar a mudança para a Dataprev."

Análise da Equipe de Auditoria

Observou-se da manifestação da DTI que existem situações impostas pela necessidade das unidades do INSS realizarem mutirões de trabalho com participação de servidores de outras unidades do INSS.

Além disso, a equipe de auditoria observou que está em trâmite no Comitê Estratégico de Governança (CEGOV) proposta de Resolução que irá atualizar as regras para a emissão de credenciais de acesso lógico no âmbito do INSS, a nova Norma de Controle de Acesso Lógico (NCAL).

Pela proposta em trâmite, os papéis de "gestor de acesso local da Superintendência Regional, da Gerência Executiva e da Agência da Previdência Social" deixam de existir, passando a figurar apenas o papel de "gestor de acesso interno" que poderá ser atribuído a servidor lotado na Administração Central, Superintendência Regional, Gerência Executiva e Agência da Previdência Social, sendo este o responsável pela atribuição do perfil de acesso e de gestão dos usuários no INSS. Dessa forma, a nova proposta poderá alterar de forma considerável as atribuições e responsabilidades dos gestores de acessos e usuários no âmbito do INSS.

Do exposto, a equipe de auditoria concluiu pela não pertinência de manter a recomendação nos moldes propostos, pois diante do cenário atual de iminente mudança da Norma de Controle de Acesso Lógico, alterações de requisitos funcionais do sistema GERID não seriam pertinentes e, se tais alterações ocorrerem, deixariam de ter validade após publicação da nova NCAL, impactando assim o próprio sistema e gerando custos adicionais com desenvolvimento para alterar novamente os requisitos do sistema.

Desta forma, sugerimos que a DTI, como área responsável pela gestão do sistema GERID, ratifique e monitore o alinhamento das funcionalidades do sistema GERID com a nova Norma de Controle de Acesso Lógico que entrará em vigor após aprovação e publicação.

Manifestação da Unidade Examinada: recomendação nº 08 (achado nº 07)

Em relação à recomendação nº 08, achado nº 07, que trata da autenticação de acesso ao GERID por meio de certificado digital, conforme recomendado pela Dataprev, a DTI apresentou as seguintes informações:

“2.8. Recomendação 8: Garantir que autenticação de acesso ao GERID esteja alinhada ao item de conclusão do Relatório Incidente de Segurança nº 201908002502, da Dataprev, que recomenda: “O acesso ao Sistema GERID deve ser restrito a endereços IP nacionais e devem ser realizados utilizando um Certificado Digital do tipo A3, visando aumentar o nível de segurança com relação aos acessos realizados e auditorias para ações maliciosas que possam ocorrer no sistema”. Achado nº 07

Manifestação DTI: A possibilidade do uso de certificado digital por parte dos gestores de acesso dos sistemas corporativos parceiros ao GERID e dos usuários está sendo analisado pela DTI, Áreas de Negócio do INSS e Dataprev. No entanto, cabe esclarecer que o contrato em vigência firmado com o SERPRO para emissão de Certificados Digitais, tem um estoque (contratado) limitado e não contempla os gestores dos sistemas corporativos do GERID. Uma nova contratação está sendo iniciada para contemplar certificados digitais para todos os servidores do INSS, o que poderá atender a questão de autenticação de acesso o sistema CONSIGWEB ser simples, ou seja, realizado somente por meio de “usuário e senha”.”

Análise da Equipe de Auditoria

Observou-se da manifestação da DTI que já existem iniciativas no sentido de viabilizar o uso de certificado digital por usuários e gestores de acessos dos sistemas corporativos parceiros ao GERID. A DTI esclarece ainda que o contrato vigente de certificados digitais possui estoque limitado, não contemplando os gestores dos sistemas corporativos GERID e, que, atualmente está sendo iniciada uma nova contratação de certificados digitais para atender todos os servidores do INSS.

Cabe ressaltar que a adoção do uso de certificado digital por usuários e gestores de acessos dos sistemas corporativos parceiros ao GERID contribuirá para a segurança da informação e o atendimento da orientação prevista no item 6.1.7 da Norma Complementar nº 07/IN01/DSIC/GSIPR.

Manifestação da Unidade Examinada: recomendação nº 09 (achado nº 08)

A área auditada apresentou a sua manifestação a respeito da recomendação nº 09, achado nº 08, que trata de revisar os requisitos de validação de senha entre os sistemas GERID e o LDAP, a fim de garantir as sincronizações com as devidas permissões:

“2.9. Recomendação 9: Revisar os requisitos de validação de senha entre os sistemas GERID e o LDAP, a fim de garantir as sincronizações com as devidas permissões. Achado nº 08

Manifestação DTI: A atualização periódica dos cadastros dos usuários no OpenLdap possibilitará maior segurança na autenticação do sistema GERID, que utiliza a mesma senha de acesso registrada no OpenLdap.

A Dataprev já foi notificada pela DTI acerca dos problemas com senhas expiradas de usuários que continuavam ativos no GERID, no entanto ainda não apresentou uma resposta acerca do assunto.”

Análise da Equipe de Auditoria

Conclui-se que a DTI concorda com a recomendação e que adotará providências para seu atendimento.

Manifestação da Unidade Examinada: recomendação nº 10 (achado nº 09)

Com relação à recomendação nº 10, achado nº 09, que trata da implantação da Equipe de Tratamento de Incidentes e Redes (ETIR), a DTI apresentou as seguintes manifestações:

"2.10. Recomendação 10: Implantar Equipe de Tratamento de Incidentes de Redes (ETIR), conforme Norma Complementar nº 08/IN 01/DSIC/GSI-PR/2010 para que os eventuais incidentes de segurança da informação sejam reportados ao CTIR-GOV. Achado nº 09

Manifestação DTI: A DTI propôs norma que institui a Equipe de Tratamento de Incidentes de Redes – ETIR-INSS (SEI processo nº 35014.047735/2020-84). Tal proposta foi analisa e aprovada pelo Comitê Estratégico de Governança - CEGOV do INSS e aguarda os trâmites necessários para sua publicação."

Análise da Equipe de Auditoria

De acordo com a manifestação da DTI, observa-se que aquela Diretoria já apresentou ao Comitê Estratégico de Governança (CEGOV) proposta no sentido de instituir a Equipe de Tratamento de Incidentes de Rede – ETIR-INSS. No entanto, consultando o sistema SEI, na data de 12.06.2020, o processo referenciado na resposta da DTI, constatou-se que ainda não foi publicada a Resolução que instituirá a ETIR.

Manifestação da Unidade Examinada: recomendação nº 11 (achado nº 10)

Com relação ao Achado 10, Recomendação 11, que diz respeito a adequar a forma de autenticação e acesso de usuários no servidor ao nível de criticidade dos dados, a manifestação da DTI foi ao sentido de que:

"2.11. Recomendação 11: Adequar a forma de autenticação e acesso de usuários no servidor ao nível de criticidade dos dados. Achado nº 10

Manifestação DTI: Os acessos locais aos servidores foram atualizados, estes acessos são restritos aos administradores de rede da DTI. Será analisado a criação de um POP (Procedimento Operacional Padrão) para formalizar os procedimentos de acesso aos equipamentos. Por serem acessos somente realizados e controlados pelos administradores da DTI este procedimento pode fazer parte de um processo da unidade de TIC ou inserido em uma Norma Complementar ou na Norma de controle de Acesso Lógico."

Análise da Equipe de Auditoria

Apesar da DTI informar que já realizou a atualização dos acessos ao equipamento servidor – Colocation, depreende-se da resposta que inexiste o procedimento de operacionalização e que as providências para instituí-lo ainda são incipientes.

Manifestação da Unidade Examinada: recomendação nº 12 (achado nº 11 e 12)

Com relação à recomendação nº 12, achados nº 11 e 12, sobre "avaliar periodicamente se o nível de segurança da aplicação e das plataformas que a sustentam são compatíveis com o risco que a administração definir como aceitável", a DTI apresentou as seguintes considerações:

"2.12. Recomendação 12: Avaliar periodicamente se o nível de segurança da aplicação e das plataformas que a sustentam são compatíveis com o risco que a administração definir como aceitável. Achado nº 11 e 12

Manifestação DTI: A DTI elaborará um relatório a cada 06 meses de acompanhamento dos níveis de segurança dos recursos de TIC, incluindo os ambientes e aplicações do INSS. Os itens de TIC comuns serão migrados para o ambiente contratado da AWS e um dos pré-requisitos é a atualização do ambiente operacional desses itens de TIC (sistemas operacionais, servidores de aplicação, ...). As checagens dos ativos de TIC em menor periodicidade ficam prejudicadas pela DTI ter uma equipe técnica reduzida e uma grande quantidade de itens de TIC. A DTI buscará formas de otimizar esse monitoramento do ambiente.

Quanto às ferramentas de prevenção, detecção e eliminação de pragas virtuais e ataques cibernéticos, este tratamento é feito nos limites da rede pelo prestador de serviço. A defasagem tecnológica é outro fator inibidor de utilização local dessas ferramentas, o que deverá ser mitigado com a disponibilização de ambientes atualizados para migração ao ambiente AWS."

Análise da Equipe de Auditoria

Conclui-se da manifestação da DTI que não existe avaliação periódica do nível de segurança das aplicações e plataformas de sustentação. No entanto, a DTI informa que irá elaborar relatório de avaliação semestral.