FUNDAÇÃO ELETROBRAS DE SEGURIDADE SOCIAL - ELETROS

Ref.: Relatório de recomendações em 31 de dezembro de 2022

Tel.: + 55 21 2210 5166
Fax: + 55 21 2224 5285
www.bdo.com.br

Rua Barão de Tefé, 27
9° andar, Saúde, Rio de Janeiro, RJ
Brasil 20220-460

2088/23
Rio de Janeiro, 17 de abril de 2023.

À
Fundação Eletrobrás de Seguridade Social - ELETROS
At.: Administradores, Participantes e Patrocinadores
Rio de Janeiro - RJ

Ref.:Relatório de recomendações em 31 de dezembro de 2022

Prezados,

Estamos encaminhando, aos cuidados de V.S.as, nosso relatório de recomendações sobre os sistemas de controles internos, elaborados em conexão com a auditoria das demonstrações contábeis do exercício findo em 31 de dezembro de 2022, da Fundação Eletrobrás de Seguridade Social - ELETROS.

Logo após cada ponto de recomendação, foram inseridos os Comentários da Administração, concordante com a recomendação, e quando aplicável, um plano com ações constantes de aprimoramento dos seus procedimentos internos.

Aproveitamos esta oportunidade para agradecer a colaboração recebida da equipe interna durante a execução dos nossos trabalhos e colocamo-nos à disposição para quaisquer esclarecimentos adicionais.

Cordialmente,

Monika Marielle Du Mont Collyer

MMDMC/PH/KP/PVJ

Fundação Eletrobras de Seguridade Social - ELETROS

Relatório de recomendações em 31 de dezembro de 2022

Índice

1. Introdução

1.1. Objetivo dos trabalhos

Como parte de auditoria em 31 de dezembro de 2022, efetuada de acordo com as práticas contábeis, emanadas na legislação aplicável às Entidades Fechadas de Previdência Complementar, da Fundação Eletrobrás de Seguridade Social - ELETROS ("ELETROS"), obtivemos um entendimento dos controles internos que consideramos relevantes para o processo de auditoria, com a finalidade de identificar e avaliar riscos de distorção relevante nas referidas demonstrações contábeis e determinar a época, natureza e extensão dos nossos exames de auditoria.

1.2. Metodologia

Avaliamos os controles internos relevantes na extensão necessária para planejar os procedimentos de auditoria que julgamos apropriados nas circunstâncias para emitir uma conclusão sobre os registros contábeis e não para expressar uma opinião sobre a eficácia dos controles internos. Assim, não expressamos uma opinião ou conclusão sobre os controles internos da ELETROS.

A Administração da ELETROS é responsável pelos controles internos por ela determinados como necessários para permitir a elaboração de demonstrações contábeis livres de distorção relevante, independentemente se causada por fraude ou erro. No cumprimento desta responsabilidade, a Administração fez estimativas e tomou decisões para determinar os custos e os correspondentes benefícios esperados com a implantação dos procedimentos de controle interno.

Em atendimento à norma brasileira de auditoria NBC TA 265 - Comunicação de Deficiências de Controle Interno, no processo de avaliação de riscos de distorção relevante nas demonstrações contábeis e durante o processo de auditoria, identificamos deficiências nos controles internos, para as quais medidas corretivas devem ser consideradas. A responsabilidade de avaliar as deficiências e tomar medidas corretivas é da Administração do ELETROS.

1.3. Identificação dos pontos de recomendações - significativos

De acordo com as normas brasileiras e internacionais de auditoria e regulamentações específicas de nossa jurisdição, o auditor deve reunir e comunicar por escrito todas as deficiências ou ineficácias significativas dos controles internos que foram identificadas, bem como outras que não sejam significativas, mas que mesmo assim têm importância suficiente para merecer a atenção da Administração. As recomendações do auditor independente são divulgadas neste relatório com a expressão "Significativa" no final da chamada de cada ponto de recomendação, quando assim for necessário.

2. TI

2.1. Ausência de termo de responsabilidade para os usuários administradores

Situação Identificada

Durante a reunião de entendimento, fomos informados que os usuários com permissão de administrador não possuem termo de responsabilidade.

Riscos envolvidos

Usuários com privilégios de acesso além do necessário para desempenhar suas atribuições, significando em segregação de função inadequada.

Recomendações

Recomendamos que os usuários não possuam tais privilégios, evitando desta forma, a execução e ou instalação de softwares, aplicativos e executáveis indevidos e ou desconhecidos. Caso seja necessário o uso, necessário realizar periodicamente a revisão dos acessos e logs, contudo é importante formalizar o uso das contas contendo o termo de responsabilidade.

Comentários da Administração: apenas alguns usuários possuem perfis de administradores nas máquinas. Isso se deve, por exigência de sistemas legados que exigem esse perfil de usuário e que estão sendo descontinuados. A Eletros está revisando suas políticas relacionadas à segurança da informação e implantando novas tecnologias que permitam maiores controles para acesso de usuários.

2.2. Usuários Genéricos.

Situação Identificada

Conforme entendimento realizado durante nossas análises, identificamos a existência de usuários não nominais na rede corporativa AD (15) e no sistema TRUST (02) usuários genéricos conforme exemplificado na planilha abaixo. Após a identificação, solicitamos o retorno de justificativa de utilização das contas e como retorno foi informado que os usuários não possuem termo de responsabilidade.

AD (Active Directory):

UserName	Groups	FullName	AcctDisabled	LastLogonTime
AdminEletros	Usuários do domínio	AdminEletros	No	05/02/2018 12:03
administrador	Usuários do domínio	Administrador	No	20/09/2022 09:57
alogadmin	Usuários do domínio	alogadmin	No	25/09/2019 13:49
alogerencia	Usuários do domínio	alogerencia	No	25/09/2019 11:30
AtendimentoES	Usuários do domínio	AtendimentoES	No	05/08/2022 15:23
bloomberg	Usuários do domínio	Bloomberg	No	18/09/2022 22:46
consultor-ann	Usuários do domínio	consultor-ann	No	02/01/2019 11:14
convidado	Usuários do domínio	Convidado	No	05/01/2018 11:30
convidado-es	Usuários do domínio	convidado-es	No	10/03/2020 12:51
eletros	Usuários do domínio	Eletros	No	14/09/2022 15:57
eletros.user	Usuários do domínio	Eletros User	No	02/06/2022 19:59
eqcas	Usuários do domínio	Eqcas	No	14/09/2022 14:59
folha	Usuários do domínio	folha	No	11/12/2018 14:17
temporario	Usuários do domínio	temporario	No	03/11/2021 11:39
temporario.es	Usuários do domínio	Temporario Eletros Saude	No	30/07/2021 08:34

TRUST:

Pessoa	Login	Perfil	Ativo
TRUST SOLUTIONS BRASIL	RSOUZA	ADM CONTABIL	S
USUARIO TRUST	TRUST	ADM CONTABIL	S

Riscos Envolvidos

Tal situação pode comprometer a CIDAL (Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade), uma vez que tais contas não são trocadas periodicamente, pois quando não são utilizadas por serviços dos próprios servidores, estas são compartilhadas entre diversos usuários, além disso, em uma eventual troca de responsabilidade na gestão da rede e ou sistema, tais contas perderiam a validade. Ressaltamos ainda, que se a conta de acesso for utilizada indevidamente, a identificação do responsável pelo erro pode não ocorrer devido seu uso e ser compartilhado.

Recomendações

Recomendamos que a utilização de usuários genéricos seja revisada, e se o uso for necessário, a ID deve possuir um único responsável, bem como, assinar um documento descrevendo o perfil de acesso, as responsabilidades da conta e o responsável pelo uso.

Comentários da Administração: o acesso dos usuários é controlado pela área de TI (ex: EQCAS: usuário para controle de registros de impressão e de posse da TI). A Eletros está revendo toda a infraestrutura física, lógica, rede e segurança da informação, bem como a revisão das políticas de acessos, no âmbito do Plano Diretor de Tecnologia da Informação (PDTI).

2.3. Complexidade de senha (TRUST e Active Directory)

Situação Identificada

Após validarmos os parâmetros de senhas definidos na rede corporativa (AD) e nos sistemas TRUST, identificamos fragilidade nas definições de complexidade de senha e na política de bloqueio. Identificamos também que determinados parâmetros não foram configurados, segue as análises abaixo:

AD – Active Directory:

ITEM (CRITÉRIO)	Recomendação BDO	Configurado AD	NOTA(S)
Tamanho mínimo para composição da senha	8 Caractere(s)	6 SENHAS	X
Quantidade de tentativas inválidas para bloqueio	3-5 tentativas	N/A	%
Duração de bloqueio	30 minutos	N/A	%
Resetar senha após o bloqueio	30 minutos	N/A	%
Criptografia reversível	Desabilitado	N/A	%
Histórico mínimo de senhas utilizadas	5 senhas	0 SENHAS	X
Requisitos de complexidade	Habilitado	N/A	%
Tempo mínimo de vida da senha	1 Dia(s)	0 DIAS	X

TRUST:

ITEM (CRITÉRIO)	Recomendação BDO	Configurado TRUST	NOTA(S)
Tamanho mínimo para composição da senha	8 Caractere(s)	N/A	%
Tempo máximo de vida da senha (período de expiração)	30/60/90 Dia(s)	N/A	%
Quantidade de tentativas inválidas para bloqueio	3-5 tentativas	N/A	%
Duração de bloqueio	30 minutos	N/A	%
Resetar senha após o bloqueio	30 minutos	N/A	%
Histórico mínimo de senhas utilizadas	5 senhas	N/A	%
Requisitos de complexidade	Habilitado	N/A	%

Riscos Envolvidos

A ausência de políticas de senhas formalizadas ou ainda mecanismos de autenticação inadequados nos sistemas e/ou rede podem significar em ineficiência na restrição de acesso a usuários devidamente autorizados e apropriados, bem como em vulnerabilidade do ambiente tecnológico e impactos à confiabilidade dos sistemas de informação e dados críticos do negócio.

Recomendações

Recomendamos que a política de senha seja revisada, destacamos abaixo os parâmetros que apresentam fragilidade e que devem ser revistos:

Active Directory

- Tamanho mínimo para composição da senha;
- Quantidade de tentativas inválidas para bloqueio;
- Duração de bloqueio;
- Resetar senha após o bloqueio;
- Criptografia reversível;
- Histórico mínimo de senhas utilizadas;
- Requisitos de complexidade;
- Tempo mínimo de vida da senha.

TRUST

- Tamanho mínimo para composição da senha;
- Tempo máximo de vida da senha (período de expiração);
- Quantidade de tentativas inválidas para bloqueio;
- Duração de bloqueio;
- Resetar senha após o bloqueio;
- Histórico mínimo de senhas utilizadas;
- Requisitos de complexidade.

Comentários da Administração: todas as políticas de tecnologia e segurança da informação estão sendo revisadas, bem como a reestruturação de toda a arquitetura física e lógica, além da adoção de novas tecnologias (*hardware e software*) que preveem maiores controles de segurança da informação (AD). Quanto ao sistema da TRUST, uma nova versão do sistema está em fase de desenvolvimento que permitirá novas implementações de controle de senhas.

2.4. Revisão periódica de acesso

Situação Identificada

Quando solicitado o relatório de revisão de acesso aos sistemas e a rede pelos gestores, fomos informados que o processo não ocorrido nas áreas sem a devida formalização e execução de forma pontual, ou seja, e feita a revisão dos acessos somente por demanda.

Riscos Envolvidos

Entendemos que a situação atual pode vir a comprometer a segurança das informações da empresa, pois em um momento de situações críticas e/ou de altas demandas de suporte no departamento de TI, o referido e-mail pode não ser lido e atendido pelos gestores dos processos, ocasionando em usuários de rede e/ou sistemas indevidamente habilitados, podendo ser utilizados por outras pessoas mal-intencionadas.

Recomendações

Recomendamos à Eletros que adote um procedimento entre os departamentos envolvidos em cada módulo do sistema, para efetuar revisões periódicas nos perfis de acessos, objetivando o controle fidedigno.

Comentários da Administração: será contemplada a recomendação no âmbito das políticas e normativos de segurança da informação em desenvolvimento.

2.5. Segregação de acesso

Situação Identificada

Para avaliação deste controle, verificamos se a Eletro s, possui segregação de funções sistêmicas de modo a evitar conflitos de aplicações para os acessos realizados pelos usuários do sistema em escopo.

Riscos Envolvidos

A ausência de matriz de segregação de função pode permitir que usuários com privilégios de acesso além do necessário e/ou não autorizados realizem alterações indevidas sem o consentimento dos gestores responsáveis pelas atividades. Acessos indevidos podem trazer impactos à confiabilidade dos dados críticos do negócio e aos sistemas de informação.

Recomendação

Estabelecer matriz de segregação de funções, em conjunto com os gestores das áreas de negócio, com as transações definidas como críticas e conflitantes, a ser utilizada nos processos de concessão e revisão de acessos, bem como no mapeamento de conflitos e controles mitigatórios, tais como monitoramento.

Comentários da Administração: será contemplada a recomendação no âmbito das políticas e normativos de segurança da informação já em desenvolvimento.

2.6. Trilhas de auditoria

Situação Identificada

Durante nossos trabalhos, identificamos que os logs adquiridos através da ativação das trilhas de auditoria estão ativados, porém não recebemos documentação.

Riscos Envolvidos

Consideramos que tal fato pode permitir que manipulações, tais como, inclusões, alterações, exclusões incorretas ou indevidas sejam realizadas nos sistemas ou diretamente nas tabelas de dados sem que ocorra identificação adequada de tais atividades e de seus executores.

Recomendações

Recomendamos que os logs gerados de usuários críticos sejam ativados e revisados periodicamente, vale ressaltar a importância de confrontar com a segregação de funções.

Comentários da Administração: está em desenvolvimento uma nova versão do sistema financeiro, em tecnologia *web*, bem como a migração da base de dados onde estão armazenadas as informações do sistema atual para nova versão de banco de dados Oracle, que possibilitará a implementação de controles e políticas mais robustas relacionadas à segurança da informação, controles de acessos e logs de transações.