FUNDAÇÃO ELETROBRAS DE SEGURIDADE SOCIAL - ELETROS

Ref.: Relatório de recomendações em 31 de dezembro de 2023

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

3345/24
Rio de Janeiro, 09 de maio de 2024.

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

Ref.:Relatório de recomendações em 31 de dezembro de 2023.

Prezados Senhores,

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 2023, 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/PHQ/MNP

BDO RCS Auditores Independentes SS Ltda., uma empresa brasileira da sociedade simples, é membro da BDO Internacional Limited, uma companhia limitada por garantia do Reino Unido, e faz parte da rede internacional BDO de firmas-membro independentes. BDO é nome comercial para a rede BDO e cada uma das firmas da BDO.

Fundação Eletrobras de Seguridade Social - ELETROS

Relatório de recomendações em 31 de dezembro de 2023

Índice

1. Introdução

1.1. Objetivo dos trabalhos

Como parte de auditoria em 31 de dezembro de 2023, 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. Tecnologia da Informação - TI

2.1. Ausência de um Plano de Contingência

Situação Identificada

Para avaliação deste controle, fomos informados que o ambiente interno de TI não possui uma Política de Contingências devidamente formalizada para a aplicação dos controles periódicos de simulações ou ações tempestivas, a fim de mitigar os riscos em casos significativos de paralização no processamento operacional. Fomos informados que a documentação formal destes controles estava em processo de elaboração em 2023, porém foi reprogramado para elaboração e implantação no primeiro semestre de 2024.

Riscos envolvidos

A falta de plano de contingência pode colaborar com a indisponibilidade de serviços de TI em um eventual incidente e faz com que o Departamento de TI não conheça as fragilidades do ambiente tecnológico. A falta de instruções para lidar com um evento crítico pode gerar complicações na infraestrutura da empresa e o tempo de indisponibilidade será alto.

Recomendações
Recomendamos a criação da política contendo os itens a seguir:

- Desenvolver a declaração de política de contingência;
- Conduzir a análise de impacto do negócio (BIA);
- Identificar controles preventivos;
- Desenvolver estratégias de recuperação;
- Planejar testes, treinamentos e exercícios;
- Planejar a manutenção;
- Testes periódicos;
- Pessoa que elaborou;
- Revisor;
- Aprovador; e
- Data de vigência.

Comentários da Administração: prezados Auditores, agradecemos a análise detalhada realizada em nosso ambiente de TI e as observações apresentadas no relatório de auditoria.

Em resposta à solicitação de avaliação do controle referente à ausência de uma Política de Contingências formalizada, gostaríamos de informar as medidas que já foram implementadas e as que estão em andamento para mitigar os riscos relacionados à paralisação no processamento operacional:

Medidas já implantadas

Aquisição de Notebooks: Como parte do Plano Diretor de Tecnologia da Informação (PDTI), todos os empregados foram fornecidos com notebooks para garantir a continuidade das operações em caso de necessidade de trabalho remoto.

Servidor de Aplicação em nuvem: Servidor de aplicação do ambiente Trust em Cloud, visando maior segurança e disponibilidade dos serviços.

Migração para o Ambiente Microsoft 365 com Licenças E5: Concluímos a migração para o ambiente Microsoft 365, garantindo acesso a todas as ferramentas e recursos necessários para o trabalho no modelo híbrido (presencial e remoto), incluindo licenças E5 para uma segurança avançada.

Aquisição de Links de Internet: Adquirimos dois links de internet, sendo um principal de 1Gb e um de redundância de 500Mb, para assegurar uma conexão estável e confiável, implantamos ainda, a redundância de internet mantendo os 2 links ativos.

Modelo de Trabalho Híbrido: Além disso, gostaríamos de destacar que estamos operando atualmente em um modelo híbrido de trabalho, com dias presenciais (segundas, terças e quartas) e dias de home office (quintas e sextas).

No cenário atual, em caso de ativação de um plano de contingência, nosso modelo de trabalho 100% home office seria acionado, garantindo a continuidade das operações sem risco de indisponibilidade de serviços, com a utilização dos notebooks já disponibilizados a todos os empregados e utilizados nos atuais dias de home office (quintas e sextas).

Medidas em andamento

Conforme informado, foram reprogramados para o decorrer 2024 a formalização do SGCN através da contratação de consultoria especializada para desenvolver e manter PCN (Plano de Continuidade do Negócio) operacionais, contendo os procedimentos a serem seguidos para permitir a operação contínua de processos críticos de negócio, plano de recuperação total ou parcial e testes periódicos.

2.2. Ausência de parâmetros de segurança aplicáveis a complexidade das senhas de acesso

Situação Identificada

De acordo com o resultado das análises realizadas nos sistemas informatizados, identificamos alguns parâmetros que podem ser melhorados, a fim de manter os níveis mínimos de complexidade para o uso dos acessos e mitigar riscos associados a segurança da informação. Abaixo destacamos os resultados:

Item (Critério)	Recomendado BDO	AD/Sistemas	Atena/Benner
Armazenar senha em criptografia reversível	Desabilitado	Desabilitado	Desabilitado
Quantidade de tentativas inválidas para bloqueio	3-5 tentativa(s)	5 tentativas(s)	5 tentativas(s)
Requisitos de complexidade	Habilitado	habilitado	habilitado
Retenção de histórico da senha	5 senha(s)	5 senha(s)	5 senha(s)
Tamanho mínimo para composição da senha	8 caracter(es)	8 caracter(es)	8 caracter(es)
Tempo de duração do bloqueio	30 minuto(s)	30 minuto(s)	30 minuto(s)
Tempo máximo de vida da senha (período de expiração)	30/60/90 dia(s)	90 dia(s)	90 dia(s)
Resetar senha após bloqueio (tempo)	30 minuto(s)	30 minuto(s)	30 minuto(s)
Tempo mínimo de vida da senha	1 dia(s)	30 dia(s)	30 dia(s)

Riscos envolvidos

Riscos em relação a segurança da informação e tentativas de acessos sistêmicos não autorizados.

Recomendações

Na tabela acima descrevemos os parâmetros que devem ser contemplados adequadamente, não se limitando a estes.

Comentários da Administração: no que diz respeito ao parâmetro mínimo de vida de senha, atendemos prontamente à recomendação, alterando o referido parâmetro de 30 dias para 1 dia. Além disso, todos os outros parâmetros já estão em conformidade com as diretrizes recomendadas pela BDO.

Destaco a evidência da alteração do parâmetro recomendado.