


| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 RESERVADO |

RELATÓRIO DE AUDITORIA INTERNA

TIPO DE AUDITORIA: CONFORMIDADE.

Nº DE ORDEM PAINT: 6

RELATÓRIO Nº: 05/2022

PROCESSO Nº: 01430.000149/2022-13

EXERCÍCIO: 2022

1. INTRODUÇÃO / ESCOPO

A presente auditoria destina-se a verificar as medidas adotadas pela Fundação Biblioteca Nacional (FBN) quanto à governança digital, conforme previsto no Planejamento Anual de Atividades de Auditoria Interna – PAINT de 2022, em seu item nº 6, realizados no Edifício Debret da FBN, no período de 29/04/2022 a 31/12/2022, em estrita observância às normas de auditoria aplicáveis ao serviço público federal. Não houve restrição imposta aos exames a ser registrada. Neste período, além do presente trabalho, foram realizadas outras auditorias previstas no PAINT/2022, de forma a otimizar a carga horária disponível para as atividades.


No presente trabalho, foram utilizadas as técnicas básicas de auditoria, a conferir: análise documental, e indagações escritas.

1.1 Unidades auditadas

1.1.1. Diretoria Executiva, no âmbito das competências dos Regimentos Internos vigentes em 2022:

a) conforme o inciso IV, do art. 7º, do Anexo da Portaria MinC nº 74, de 03/08/2018), na qual tem o gerente responsável pelo PTD da FBN:

*“Art. 7º Ao Diretor-Executivo compete:
IV - planejar, dirigir, coordenar e orientar a implementação de ações de informática da Fundação Biblioteca Nacional.*

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

b) conforme Art. 7º, b, do Anexo da Portaria FBN nº 82, de 23 de dezembro de 2022 compete ao Diretor Executivo:

*“Art. 7º Ao Diretor Executivo incumbe:
b) a governança digital da Fundação Biblioteca Nacional*

- Coordenação-Geral de Planejamento e Administração, conforme o inciso I, do art.12 do Anexo da Portaria MinC nº 74, de 03/08/2018 e Portaria FBN nº 82, de 23/12/2022:

*“Art. 12. À Coordenação-Geral de Planejamento e Administração compete:
I - Coordenar e controlar a implementação de ações relacionadas à administração e desenvolvimento de recursos humanos, de planejamento e de orçamento, de contabilidade, de administração financeira, de administração de convênios e termos congêneres, de tecnologia da informação, de gestão de documentos, de patrimônio, de licitações e gestão de contratos, de serviços gerais e de organização e inovação institucional;”*


1.2 Descrição do Planejamento adotado e base legal

O escopo do trabalho é verificar a atuação do Comitê de Governança Digital, voltadas ao cumprimento dos objetivos previstos no Decreto nº 10332/2020, o qual determina que os órgãos e as entidades elaborarão os seguintes instrumentos de planejamento:

- 1) Plano de Transformação Digital que conterà no mínimo ações de:
 - a) transformação digital de serviços;
 - b) unificação de canais digitais e
 - c) interoperabilidade de sistemas
- 2) Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e sua atualização;
- 3) Plano de Dados Abertos e sua vigência;
- 4) .elaboração do Planejamento Estratégico de Tecnologia da Informação (PETIC);



- 5) Política de Segurança de Informação e sua revisão, de modo a estar aderente às diretrizes do Gabinete de Segurança Institucional da Presidência da República, e de seu Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, e em cumprimento ao art. 9 e demais dispositivos da IN GSI 01/2020;
- 6) A previsão no PTD do Eixo Segurança e Privacidade, considerando a Lei Geral de Proteção de Dados Pessoais, de acordo com os objetivos voltados ao alcance da Estratégia do Governo Digital, conforme prevê o Decreto nº 10.332/2021 e alterações posteriores;
- 7) monitoramento das recomendações constantes no RAI nº 05/2019, que trata da Gestão do Armazenamento Digital, tais como:
 - 7.1) a solicitação de exercício descentralizado de servidores do cargo de “Analista de Tecnologia da Informação – ATI” para a FBN (na qualidade de órgão seccional do SISP), a partir das necessidades identificadas para a implantação do seu futuro Plano de Transformação Digital;
 - 7.2) a reestruturação do Núcleo de Tecnologia da Informação da FBN;
 - 7.3) o estabelecimento de rotinas de monitoramento de estratégias e oportunidades, para serem acompanhadas, tais quais: editais de fomento e incentivo, a exemplo do Edital do Fundo de Defesa de Direitos Difusos – FDD, bem como designar servidores/comissões para que a FBN elabore e submeta, regularmente, projetos para seleção que contemplem liberação de recursos para investimentos em tecnologia, preservação, digitalização, acessibilidade e disseminação de acervo;
 - 7.4) o fortalecimento da BNDigital, dos Laboratórios de Digitalização, Preservação e Restauração voltadas às propostas do Centro de Processamento e Preservação, integrada com a temática de outros projetos e eventos da FBN planejados para o exercício seguinte, entre outros.
- 8) verificação das pautas do Comitê de Governança Digital e seu acompanhamento das atividades da Comissão Permanente de Preservação Digital da FBN e da implementação da Política de Preservação Digital;
- 9) verificação das pautas do Comitê de Governança Digital de seu monitoramento do Plano de Ação para Digitalização dos acervos raros e de valor histórico do

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

acervo de obras raras ou de elevado valor histórico: as ações a serem tomadas e os prazos para implementação (item 9.2.1.2.do Acórdão nº 1439/2021/TCU-Plenário);

- 10) verificação das pautas do Comitê de Governança Digital do monitoramento da implantação dos objetivos previstos no Decreto 10332/2020, entre outros assuntos.

As questões enfrentadas por essa equipe de auditoria contribuem para que as medidas de governança digital sejam adotadas, voltadas ao cumprimento dos objetivos previstos no Decreto nº 10332/2020, que trata da Estratégia de Governo Digital.

Ainda sobre esse tema, é importante ressaltar que o escopo do presente relatório não abrange assuntos de caráter técnico, mas, sim, conformidade com os normativos e a atuação da governança da instituição, considerando que não há auditor integrante da equipe da Audin/FBN com formação específica em ciência da computação ou similar.

Foram utilizados como base normativa e documentos de referência na presente atividade:

Decreto-Lei nº 10.332, de 28/04/de 2020 (Estratégia de Governo Digital);

Decreto nº 9.203, de 22/11/2017 (Política de governança da administração pública);


Lei nº 12.527, de 18/11/2011 (Lei de Acesso à Informação);

Lei nº 13.709, de 14/08/2018 (Lei Geral de Proteção de Dados);

Decreto nº 9.637, de 16/12/2018 (Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública).

Referenciais normativos relativo à prática de controle de backup:

- Diretriz 2.3.4 do Decreto nº 10.222, de 5 de fevereiro de 2020;
- Acórdão 1.109/2021 – Plenário Tribunal de Contas da União (TCU);
- Guia do Framework de Segurança - CIS Controle 10: Capacidade de Recuperação de Dados;

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

- CIS Controls v8 - Controle 11: Recuperação de Dados;
- ABNT NBR ISO/IEC 27002 - 12.3 Cópias de segurança;
- Acórdão 1768/2022 – Plenário Tribunal de Contas da União (TCU).

Referenciais normativos acerca do controle de gestão de acesso:


- Art.12, inciso IV, alínea “f” da Instrução Normativa nº 1, de 27 de maio de 2020;
- Item 7.2.4 da Instrução Normativa nº 31, de 23 de março de 2021;
- Norma complementar Nº 07 /IN01/DSIC/GSIPR;
- Guia do Framework de Segurança - CIS Controle 16: Monitoramento e Controle de Credenciais de Acesso;
- CIS Controls v8 - Controle 06: Gestão do controle de acesso;
- ABNT NBR ISO/IEC 27002 - 9 Controle de Acesso.

Referenciais normativos no que se refere à gestão de vulnerabilidade:

- Art.12, inciso IV, alínea “d” da Instrução Normativa nº 1, de 27 de maio de 2020;
- <https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/>;
- Guia do Framework de Segurança - CIS Controle 03: Gestão Contínua de Vulnerabilidades;
- CIS Controls v8 - Controle 07: Gestão contínua de vulnerabilidades;
- ABNT NBR ISO/IEC 27002 - 12.6 Gestão de vulnerabilidades técnicas.

2 - RESULTADO DOS TRABALHOS

Os resultados serão apresentados por eixos de análise, em relação a cada item listado no planejamento da auditoria.

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

2.1 Informação nº 001 – Atuação do Comitê de Governança Digital da FBN no exercício de 2022.

Inicialmente, o Comitê de Governança Digital tem como objetivo discorrer sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação, e sua criação está prevista no Decreto nº 10.332, de 28/04/2020.

A constituição do Comitê de Governança Digital da Fundação Biblioteca Nacional (0050718) ocorreu em dezembro de 2020, por meio da Portaria FBN/PRESI nº 135, de 10/12/2020. A única reunião ocorrida foi em 27/07/2021, conforme consta no processo SEI nº 01430.000335/2020-82.

No exercício 2022, a Auditoria Interna apresentou a Nota de Auditoria nº 01/2022, de 16/05/2022, contendo recomendações voltadas para o aprimoramento da governança digital da instituição, o que envolveria toda a Alta Administração da FBN. Inicialmente, elencamos as seguintes.

“RECOMENDAÇÃO 01: Que a Diretoria Executiva elabore uma agenda de reuniões mensais com o Comitê de Governança Digital da FBN para tratar do andamento das medidas voltadas à implantação das diretrizes e objetivos previstos na Lei nº 14129/2021, no Decreto nº 10.332/2020, entre outras normas. ”

“RECOMENDAÇÃO 02: Que a Diretoria Executiva proceda à abertura de um processo SEI específico para o acompanhamento das atividades do Comitê de Governança Digital.”

A nova Diretoria Executiva, no exercício 2022, reinstalou o Comitê de Governança Digital em 11/07/2022, e conseguiu realizar quatro reuniões ordinárias (13/09/2022, 27/10/2022, 24/11/2022 e 16/12/2022), e com melhor resultado, quando comparado ao exercício 2021. As pautas e respectivas atas foram instruídas no processo SEI (01430.000335/2020-82).

Consta no sítio eletrônico oficial da FBN, relativo ao Comitê de Governança Digital – CGD, o seguinte:

As reuniões do Comitê de Governança Digital ocorrem na terceira semana de cada mês. Uma vez que o art. 16 do Decreto nº 9.203, de 22/11/2017 prevê que



*"os comitês internos de governança **publicarão suas atas e suas resoluções em sítio eletrônico, ressalvado o conteúdo sujeito a sigilo.**" (grifos nossos)*

Verificamos que as atas não foram publicadas, conta somente o extrato, com a data das reuniões ordinárias, bem como suas pautas sinalizando conclusão ou vigência de respectivo assunto.

A Lei de Acesso à Informação (LAI) assegura aos cidadãos o direito de receber dos Órgãos Públicos informações de seu interesse, vejamos:

*"Art. 3º Os procedimentos previstos nesta Lei destinam-se a **assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública** e com as seguintes diretrizes:*

*I - **observância da publicidade como preceito geral e do sigilo como exceção;***

*II - **divulgação de informações de interesse público, independentemente de solicitações;***

*III - **utilização de meios de comunicação viabilizados pela tecnologia da informação;***

*IV - **fomento ao desenvolvimento da cultura de transparência na administração pública;***

*V - **desenvolvimento do controle social da administração pública.**"*

(grifos nossos)

Quanto à classificação do sigilo de informações os arts. 27 e 28 da LAI dispõem que:

*"Art. 27. **A classificação do sigilo de informações no âmbito da administração pública federal é de competência:***

I - no grau de ultrassecreto, das seguintes autoridades:

a) Presidente da República;

b) Vice-Presidente da República;

c) Ministros de Estado e autoridades com as mesmas prerrogativas;

d) Comandantes da Marinha, do Exército e da Aeronáutica; e

e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior;

II - no grau de secreto, das autoridades referidas no inciso I, dos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista; e

III - no grau de reservado, das autoridades referidas nos incisos I e II e das que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo-Direção e Assessoramento Superiores, ou de hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade, observado o disposto nesta Lei.



§ 1º A competência prevista nos incisos I e II, no que se refere à classificação como ultrassecreta e secreta, poderá ser delegada pela autoridade responsável a agente público, inclusive em missão no exterior, vedada a subdelegação.

§ 2º A classificação de informação no grau de sigilo ultrassecreto pelas autoridades previstas nas alíneas “d” e “e” do inciso I deverá ser ratificada pelos respectivos Ministros de Estado, no prazo previsto em regulamento.

§ 3º A autoridade ou outro agente público que classificar informação como ultrassecreta deverá encaminhar a decisão de que trata o art. 28 à Comissão Mista de Reavaliação de Informações, a que se refere o art. 35, no prazo previsto em regulamento.

Art. 28. A classificação de informação em qualquer grau de sigilo deverá ser formalizada em decisão que conterá, no mínimo, os seguintes elementos:

I - assunto sobre o qual versa a informação;

II - fundamento da classificação, observados os critérios estabelecidos no art. 24;

III - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, conforme limites previstos no art. 24; e

IV - identificação da autoridade que a classificou.

Parágrafo único. A decisão referida no caput será mantida no mesmo grau de sigilo da informação classificada.”

(grifos nossos)

Podemos observar, pela análise dos artigos acima, que é de responsabilidade da autoridade competente classificar a informação como sigilosa, como também formalizar a decisão, o que não está evidenciado no processo, ou seja, havendo justificativa para a classificação do sigilo e não publicação das atas no sitio eletrônico da FBN, devem ser cumpridas as exigências previstas na Lei de Acesso à Informação.


O art. 30 da LAI prevê que autoridade máxima de cada órgão ou entidade publicará, anualmente, em sítio à disposição na internet e destinado à veiculação de dados e informações administrativas, o seguinte:

“Art. 30. A autoridade máxima de cada órgão ou entidade publicará, anualmente, em sítio à disposição na internet e destinado à veiculação de dados e informações administrativas, nos termos de regulamento:

I - rol das informações que tenham sido desclassificadas nos últimos 12 (doze) meses;

II - rol de documentos classificados em cada grau de sigilo, com identificação para referência futura;

III - relatório estatístico contendo a quantidade de pedidos de informação recebidos, atendidos e indeferidos, bem como informações genéricas sobre os solicitantes. § 1º Os

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

órgãos e entidades deverão manter exemplar da publicação prevista no caput para consulta pública em suas sedes.

§ 2º Os órgãos e entidades manterão extrato com a lista de informações classificadas, acompanhadas da data, do grau de sigilo e dos fundamentos da classificação.”

(grifos nossos)

Nesse sentido, trazemos o art. 4º § 6º da Portaria FBN nº 82, de 23/12/2022 que discorre sobre a publicação das atas de reunião ordinária.

“Art. 4º A FBN será dirigida por uma Diretoria Colegiada composta pelos seguintes membros:

§ 6º O calendário, a pauta, as atas e as resoluções das reuniões ordinárias da Diretoria Colegiada serão divulgados no sítio eletrônico da FBN, excetuando-se as informações restritas ou sigilosas nos termos da lei.” (grifos nossos)

Em consulta ao sítio eletrônico da FBN (<https://www.gov.br/bn/pt-br/acesso-a-informacao-2/informacoes-classificadas>), consta que a Fundação não possui informações classificadas como sigilosa.


“ Sendo assim, dada a natureza das atividades da FBN, não possuímos informações classificadas. Lembrando que utilizamos o SEI-FBN apenas para criação e tramitação de processos administrativos, até a presente data, 15 de julho de 2022, não existem processos sigilosos no SEI-FBN.” (grifos nossos)

Além da classificação do sigilo, é importante mencionar também, a publicação da desclassificação do sigilo mencionada no art. 45 do Decreto nº 7.724/2012.

“Art. 45. A autoridade máxima de cada órgão ou entidade publicará anualmente, até o dia 1º de junho, em sítio na Internet:

I - rol das informações desclassificadas nos últimos doze meses;” (grifos nossos)

A exemplo de órgão que divulga o rol de classificação e desclassificação de informações sigilosas, temos o Instituto Nacional da Propriedade Industrial - INPI, que especifica a fundamentação legal, o grau de sigilo, a data da classificação e o prazo de restrição do acesso.

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

Identificamos que o sítio eletrônico da FBN não está de acordo com os parâmetros contidos na LAI, uma vez que não disponibiliza as atas das reuniões ordinárias, bem como, não cumpre com o disposto nos artigos acima no que tange ao sigilo.

Colacionamos abaixo algumas informações que constaram das pautas de reunião ordinária do Comitê de Governança e que precisam ser retomadas em 2023:

- Encaminhar à presidência a repactuação do PTD
- Agendar reunião com a RNP sobre o Dataverse do CPE
- Recuperar o acesso ao catálogo virtual do EDA
- Levar ao Ministério questionamento sobre EDA
- Encaminhar vídeo da Gale Digital Scholar Lab
- Encaminhar a proposta da Google DEX Pendente
- Adaptar os editais do CPE para uma melhor aplicabilidade às necessidades internas da FBN
- Solicitar visita da DATAPREV e do SERPRO para diagnosticar as necessidades

Importante mencionar que, tendo em vista a nova composição da Presidência e Diretoria Colegiada da FBN, deverão ser publicadas no sítio eletrônico o nome atualizado da pessoa encarregada pelo tratamento de dados pessoais, conforme preceituado no art. 41§ 1º Lei Geral de Proteção de Dados Pessoais (LGPD).


“Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. ”

Vale destacar o conceito de controlador e encarregado incluído pela Lei Geral de Proteção de Dados Pessoais (LGPD).

“Art. 5º Para os fins desta Lei, considera-se:

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |


RESERVADO

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) ” (grifos nossos)

Em consulta ao sitio eletrônico da FBN, (<https://www.gov.br/bn/pt-br/aceso-a-informacao-2/servico-de-informacao-ao-cidadao/atendimento-presencial>), identificamos na *autoridade de monitoramento do serviço de informação ao cidadão – sic*, o nome de uma pessoa que não faz parte do atual quadro de servidores da FBN, devendo ser atualizado o nome do responsável por este serviço conforme dispõe a LGPD.

Ressaltamos alguns itens, que, embora cumpridos, precisam ser retomados no exercício de 2023, em especial no que tange à formalização de designação de responsáveis, como a atualização das seguintes Portarias:

- Portaria FBN nº 72, de 30/11/2022 com a designação de uma nova Autoridade de Monitoramento do Serviço de Informação ao Cidadão, conforme Lei nº 12.527/2011, art. 40, e o Decreto nº 7.724/2012, art. 67;
- Portaria FBN nº 036 de 11 de julho de 2022.(0085422), que reinstituí o Comitê de Governança Digital e nomeação do Encarregado pelo Tratamento de Dados Pessoais., e revogou a Portaria FBN/PRESI nº 135, de 10/12/2020, que trata da constituição do Comitê de Governança Digital da Fundação Biblioteca Nacional (0050718).
- Portaria FBN nº 041 de 18 de julho de 2020 (0086185)., que designou como Autoridade de Monitoramento de Acesso à Informação o Diretor Executivo da Fundação Biblioteca Nacional, conforme determinado no caput do artigo 40 da Lei nº 12.527/2011;
- Portaria FBN nº 073 de 30 de novembro de 2022 (0097628), que implementou a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) na própria equipe da Coordenação de Tecnologia da Informação da FBN, auxiliada pelo Encarregado pelo Tratamento dos Dados Pessoais e pelo Gestor da Segurança Orgânica.

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

Quanto à agenda, entre os benefícios alcançados a partir das recomendações da Auditoria Interna, e relacionados aos marcos previstos no Decreto 10.332/2020, destacamos, no exercício 2022, a aprovação do seu Plano de Transformação Digital, bem como da nova Política de Segurança de Informação, e a atualização do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC):


1) elaboração e aprovação do Plano de Transformação Digital (processo SEI 01430.000319/2022-51, com vigência prevista de julho a dezembro de 2022, com as ações para: a transformação digital de serviços; unificação de canais digitais; interoperabilidade de sistemas, havendo reuniões periódicas de acompanhamento do cronograma de metas e prazos;

O Plano de Transformação digital foi elaborado e aprovado em julho de 2022 (0085351) englobando o acesso ao patrimônio da Fundação Biblioteca Nacional bibliográfico e documental, visando ser o canal que promove informações e conhecimentos, tanto na esfera nacional, como na esfera internacional eliminando sempre que possível as barreiras do espaço e do tempo. Além disso, o plano apresenta alvos específicos como:

- Ampliar o leque de recursos digitais oferecidos pela FBN, em consonância com a iniciativa exitosa da BN Digital;
- Facilitar e simplificar a comunicação com o público-alvo;
- Viabilizar as inscrições virtuais nos editais de seleção promovidos pela FBN.

A Fundação Biblioteca Nacional em seu Plano de Transformação Digital se fundamentou em distinguir 4 eixos, no qual demandam ações e prazos distintos que são classificados como:

- EIXO 1 – Transformação Digital dos Serviços Públicos
- EIXO 2 – Unificação de Canais Digitais
- EIXO 3 – Interoperabilidade de Sistemas
- EIXO 4 – Segurança e Privacidade

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

Foi elaborado também um Comitê Estratégico do Plano de Transformação Digital que é formado pelo Secretário de Modernização da Administração Federal - SEME/SG/PR, Secretário de Governo Digital do Ministério da Economia - SGD/ME e Presidente da Fundação Biblioteca Nacional – FBN

Com a exoneração do gerente do Plano de Transformação, é necessário sua atualização.


2) **revisão da Política de Segurança de Informação**, de modo a estar aderente às diretrizes do Gabinete de Segurança Institucional da Presidência da República, e de seu Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, e em cumprimento ao art. 9 e demais dispositivos da IN GSI 01/2020;

“Art. 9º É obrigatório a todos os órgãos e as entidades da administração pública federal possuir uma Política de Segurança da Informação, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.”

A POSIN foi atualizada em novembro de 2022, visando conduzir de forma adequada, a utilização de recursos da informação e da tecnologia, possuindo como objetivos:

- a) Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.
- b) Apoiar a implantação das iniciativas relativas à Segurança da Informação.
- c) Orientar o grupo responsável pela Segurança da Informação.
- d) Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

Foi promulgada a Política de Segurança da Informação e Comunicações da FBN (POSIN), com vigência de quatro anos, por meio da publicação da Portaria FBN nº 073 de 30 de novembro de 2022.

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

Foi designado como Gestor de Segurança da Informação o o titular da Coordenação de Tecnologia da Informação da FBN, a quem caberá atribuir responsabilidades à ETIR, por meio da Portaria FBN nº 073 de 30 de novembro de 2022(0097628)

Foi instituído o Subcomitê de Gestão de Segurança da Informação da FBN (SGSI), por meio da Portaria FBN nº 073 de 30 de novembro de 2022(0097628)

3) atualização do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);

Foi aprovada na 5ª reunião ordinária do Comitê de Governança Digital o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), com vigência para 2023 a 2024, e sua promulgação pela Portaria FBN Nº 80, DE 19 DE DEZEMBRO DE 2022, pelo Presidente da FBN.


Dessa forma, a FBN está aderente ao previsto no art. 3º, II, § 1º, II do Decreto 10332/2020.

O PDTIC é um instrumento de gestão voltado para a execução de ações de TIC, que justificam a maximização ou minimização na aplicação dos recursos, conduzindo assim, a melhora no direcionamento do gasto público e na entrega do serviço à sociedade, com sua atualização, verifica-se o objetivo de sistematizar o planejamento de TIC para o biênio 2023- 2024, servindo também para declarar os objetivos e as estratégias da área de TIC.

4) elaboração do Planejamento Estratégico de Tecnologia da Informação (PETIC):

Essa pauta foi tratada na reunião ordinária do dia 13/12/2022 nos seguintes temas:

“(…)o Guia de Elaboração do PDTIC do SISP não obriga a confeccionar um Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC), pois o PDTIC já contempla elementos estratégicos. O CGD decide que a elaboração do PETIC poderá ser feita oportunamente, por ocasião da aprovação do novo PEI do

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

período 2024-2027". (grifos nosso) (Documento Sei 0098433 – Processo nº 01430.000335/2020-82)

Dessa forma, será retomada oportunamente no exercício de 2023

5) **A previsão no PTD do Eixo Segurança e Privacidade**, considerando a Lei Geral de Proteção de Dados Pessoais, de modo a estar aderente à segurança e privacidade, entre outros objetivos voltados ao alcance da Estratégia do Governo Digital, conforme prevê o Decreto nº 10.332/2021 e alterações posteriores;

Conforme disposto no Decreto nº 10.332, de 28/04/2020, um dos objetivos a serem alcançados, por meio da Estratégia de Governo Digital, incluem implementar a Lei Geral de Proteção de Dados, no âmbito do Governo federal, e garantir a segurança das plataformas de governo digital.


Importante trazer à tona o art. 1º da Lei nº 13.709, de 14/08/2018, que diz respeito acerca da aplicação ampla e abrangente da Lei, que abarca, além do setor privado, todos os órgãos públicos.

*“Art. 1º Esta Lei dispõe sobre o **tratamento de dados pessoais**, inclusive nos meios digitais, por pessoa natural ou por **pessoa jurídica de direito público ou privado**, com o objetivo de **proteger os direitos fundamentais de liberdade e de privacidade** e o livre desenvolvimento da personalidade da pessoa natural.*

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.” (grifos nosso)

Tal assunto está sendo acompanhado pelo Tribunal de Contas da União - TCU, por meio do Acórdão nº 1384/2022 TCU - Plenário, que busca avaliar as ações governamentais e os riscos à proteção de dados pessoais. É necessário o andamento dessa pauta, tendo, entre outros objetivos.

- Elaboração plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD;
- Identificação das categorias de titulares de dados pessoais com os quais se relaciona;

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

- identificação dos operadores que realizam tratamento de dados pessoais em seu nome.

No que tange à implementação da Lei Geral de Proteção de Dados no âmbito do governo federal, os objetivos previstos no Decreto nº 10.332, de 28/04/2020 são de estabelecer método de adequação e conformidade dos órgãos com os requisitos da LGPD e uma plataforma de gestão da privacidade e uso dos dados pessoais do cidadão.

Verificamos que a FBN não possui políticas relacionadas à classificação da informação e proteção de dados pessoais, desse modo, deverá ser instituído de forma a mostrar mais comprometimento e adequação com a iniciativa de adequação à LGPD e ao Decreto nº 10.332, de 28/04/2020.


É importante que a FBN reforce o plano de conscientização e capacitação dos colaboradores em proteção dos dados pessoais, no plano de capacitação da instituição.

Além disso, a FBN também precisa estar em conformidade do tratamento, isto é, deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos. Para fins de conformidade e tratamento desses dados deve ser realizado um relatório de impacto à proteção de dados pessoais.

A Lei Geral De Proteção De Dados Pessoais, em seu art. 5º, XVII, traz o conceito de relatório de impacto:

*“Art. 5º Para os fins desta Lei, considera-se:
XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;”*

Em relação aos direitos do titular, a FBN deve publicar, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais, igualmente, deve estar preparada para atender todos os direitos dos titulares que são elencados no art. 9º da LGPD.

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

“Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e


VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.” (grifos nossos)

No que tange ao compartilhamento de dados pessoais, reforçamos que a Fundação deve adotar medidas de adoção de controles adequados para mitigar riscos que possam comprometer a proteção dos dados pessoais.

Quanto ao gerenciamento incidentes de segurança da informação que envolvem a violação de dados pessoais, a FBN deve conter o plano de resposta a incidentes que abrange o tratamento de incidentes que envolvem violação de dados pessoais, bem como monitorar proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais, e também estabelecer procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

No que compete às medidas de proteção, reforçamos que a FBN deve adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais. Para isso, convém que sejam implementados controles capazes de mitigar riscos que possam resultar em violação da privacidade.

“Art. 46. Lei nº 13.709, de 14/08/2018: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. ”

6) acompanhamento do Plano de Dados Abertos, abordado pelo RAI nº 02/2019, de modo a zelar pela atualização das informações junto ao Painel de Monitoramento de Dados Abertos (<http://painéis.cgu.gov.br/dadosabertos/index.htm>), e do Portal Brasileiro de Dados Abertos (<http://dados.gov.br/>);

Foi instituído o Plano de Dados abertos da Fundação Biblioteca Nacional – FBN, aprovado pelo Comitê de Governança Digital da FBN de acordo com Decreto nº 10.332, Art 3º, § 1, II, para o período 2021-2023, por meio da Portaria FBN nº 043 de 8 de setembro de 2021. (0062778) no processo SEI nº 01430.000335/2020-82, no qual está disponível no sítio eletrônico da Fundação Biblioteca Nacional e pode ser acessado no endereço <https://www.bn.gov.br/acessoinformacao/dados-abertos>

Essa pauta deverá ser acompanhada, tendo em vista que a vigência vai até o exercício 2023, sendo importante verificar o seu cumprimento.


7) monitoramento das recomendações constantes no RAI nº 05/2019, que trata da Gestão do Armazenamento Digital, tais como:

7.1) a solicitação de exercício descentralizado de servidores do cargo de “Analista de Tecnologia da Informação – ATI” para a FBN (na qualidade de órgão seccional do SISP), a partir das necessidades identificadas para a implantação do seu futuro Plano de Transformação Digital;

Este assunto não foi pauta nas reuniões do Comitê de Governança Digital no exercício de 2022, o que pode ser retomado em 2023.

7.2) a reestruturação do Núcleo de Tecnologia da Informação da FBN;

Com o novo Regimento Interno, a estrutura organizacional passou a contar com uma Coordenação de Tecnologia da Informação, com dois Núcleos: Núcleo de Suporte e Infraestrutura e Núcleo de Segurança da Informação, o que representa uma melhoria

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

em relação à estrutura do Regimento Interno anterior, que previa apenas o Núcleo de Tecnologia de Informação. Comparando as competências, temos:

Portaria nº74, de 3 de agosto de 2018 (Regimento Interno da Fundação Biblioteca Nacional):


“Art. 16: Ao Núcleo de Tecnologia da Informação compete:

- I. executar ações de planejamento estratégico voltadas à tecnologia da informação no âmbito da Fundação Biblioteca Nacional;*
- II-Realizar ações de soluções tecnológicas e implementação de processos de governança de tecnologia da informação;*
- III acompanhar e fiscalizar os serviços de tecnologia da informação;*
- IV. Elaborar, gerir, executar e atualizar, diretamente ou por meio de terceiros, os projetos, padrões de interface, identidade visual, navegabilidade e ergonomia dos sítios eletrônicos em internet e intranet, das soluções em rede, dos portais corporativos e sistemas de informação da Fundação Biblioteca Nacional; e*
- V administrar a utilização de recursos e serviços da rede corporativa da Fundação Biblioteca Nacional”*

Portaria FBN nº 82, de 23 de dezembro de 2022, (Novo Regimento Interno da Fundação Biblioteca Nacional):

“Art. 34. À Coordenação de Tecnologia da Informação compete:

- I - supervisionar e gerir os recursos de Tecnologia da Informação da FBN;*
- II - coordenar a elaboração, análise e execução dos Planos e as Políticas de Tecnologia da Informação, subsidiando a alta administração no âmbito estratégico e operacional;*
- III - elaborar, implementar, monitorar e revisar periodicamente o Plano Diretor de Tecnologia da Informação da FBN;*
- IV - prospectar, desenvolver e coordenar projetos concernentes aos sistemas de informação e à infraestrutura tecnológica da FBN;*
- V - planejar, coordenar e supervisionar as atividades necessárias à sustentação dos serviços de Tecnologia da Informação da FBN;*
- VI - supervisionar a prestação de suporte técnico, a utilização e a operação dos recursos computacionais da FBN;*
- VII - informar, orientar e apoiar as unidades da FBN quanto ao cumprimento da Política de Segurança da Informação e da cultura de segurança cibernética da instituição;*
- VIII - planejar, coordenar e supervisionar a execução das atividades relacionadas ao Sistema de Administração dos Recursos de Tecnologia da Informação - SISP no âmbito da FBN.”*

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

“Art. 35. Ao Núcleo de Suporte e Infraestrutura compete:

I - supervisionar, orientar, acompanhar e avaliar as atividades de atendimento de suporte técnico e manutenção dos recursos computacionais da FBN, incluindo a rede corporativa, ativos de rede e links de comunicação;

II - administrar e supervisionar a operação e a disponibilidade dos serviços de TI da FBN; e

III - supervisionar, implantar e analisar os requisitos técnicos para aquisição de bens, serviços e soluções de infraestrutura tecnológica, com o objetivo de fomentar sua padronização no âmbito da FBN.

Art. 36. Ao Núcleo de Segurança da Informação compete:

I - supervisionar, orientar, acompanhar e avaliar as ações relativas ao cumprimento da Política de Segurança da Informação e da cultura de segurança cibernética da instituição;

II - propor normas e diretrizes relacionadas à gestão da Segurança da Informação; e


III - monitorar políticas, normas, procedimentos e padrões que incidam na gestão da Segurança da Informação no âmbito da FBN.”

Apesar da reestruturação organizacional, ainda há aprimoramentos a serem realizados, com atribuições específicas ao serviço de gestão e governança.

De acordo com o Art. 7º, II da portaria FBN nº 82, de 23/12/2022 compete ao Diretor Executivo planejar, orientar e supervisionar a governança digital da Fundação Biblioteca Nacional.

Constatamos que a Coordenação de Tecnologia da Informação da FBN está subordinado à CGPA, quando poderia estar vinculado diretamente à Diretoria Executiva, como ocorre em outros órgãos, a exemplo, o Instituto Nacional da Propriedade Industrial.

7.3) o estabelecimento de rotinas de monitoramento de estratégias e oportunidades, para serem acompanhadas, tais quais: editais de fomento e incentivo, a exemplo do Edital do Fundo de Defesa de Direitos Difusos – FDD, bem como designar servidores/comissões para que a FBN elabore e submeta, regularmente,

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

projetos para seleção que contemplem liberação de recursos para investimentos em tecnologia, preservação, digitalização, acessibilidade e disseminação de acervo;


Importante mencionar que, além do FDD, há também outras formas de captação importantes, como o Fundo Nacional de Cultura, além de parcerias institucionais e apoio mútuo em buscas de soluções. Essa pauta precisa ser retomada pelo Comitê de Governança Digital no exercício 2023.

7.4) o fortalecimento da BNDigital, dos Laboratórios de Digitalização, Preservação e Restauração voltadas às propostas do Centro de Processamento e Preservação, integrada com a temática de outros projetos e eventos da FBN planejados para o exercício seguinte, entre outros.

O assunto constou do Relatório de Auditoria Interna 05/2019, e precisa ser mantida, pois foi sem êxito até o momento.

“Recomendação nº 001 (Constatação) – Designar atribuição, a Colegiado permanente pré-existente ou a ser constituído, para desenvolvimento de Programação Anual Prévia da BN Digital com o fim de nortear atividades dos Laboratórios de Digitalização, Preservação e Restauração voltadas às propostas dessa Coordenação (nos termos do Art. 72 parágrafos único, da Portaria MinC nº 74, de 03/08/2018). A referida previsão, de caráter orientativo e integrada com a temática de outros projetos e eventos da FBN planejados para o exercício seguinte, deve contemplar temas de interesse público, com impacto sobre a sociedade e que possam fomentar parcerias com outros órgãos públicos. ”

Foram apresentados projetos importantes da instituição, voltadas a fortalecer e manter a qualificação do Laboratório de Digitalização da FBN, elegíveis para captação por meio do Fundo Nacional de Cultura (FNC), mas que não lograram êxito no efetivo apoio de recursos. A FBN precisa superar a obsolescência de alguns equipamentos que atendem o setor. Isso requer apoio financeiro para a aquisição de tecnologias para o desenvolvimento e a promoção de serviços digitais, que constituem prioridades da instituição. Acrescentamos também a necessidade de captação de recursos financeiros para os projetos que visam aprimorar os sistemas de segurança e backup da instituição.

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

8) verificação das atividades da Comissão Permanente de Preservação Digital da FBN e da implementação da Política de Preservação Digital;


Inicialmente, deve ser verificada a necessidade de atualização da designação dos membros da Comissão Permanente de Preservação Digital, tendo em vista a exoneração de membros e nova designação de equipe. Esta Comissão tem uma finalidade importante, de ser a responsável pela revisão, atualização e gestão da política de preservação digital da Fundação Biblioteca Nacional, e, dessa forma, os assuntos tratados podem subsidiar medidas pelo Comitê de Governança Digital, para a tomada de decisão pela Alta Administração, em nível mais estratégico.

9) monitoramento do Plano de Ação para Digitalização dos acervos raros e de valor histórico do acervo de obras raras ou de elevado valor histórico: as ações a serem tomadas e os prazos para implementação (item 9.2.1.2.do Acórdão nº 1439/2021/TCU-Plenário);

O Tribunal de Contas da União considerou o Plano de Ação apresentado pela FBN como atendido, conforme o Acórdão nº 194/2023 - TCU – Plenário, remanescendo, dessa forma, o seu monitoramento pelo Comitê de Governança Digital para cumprir as metas definidas até o final do período dos dois anos, e dar continuidade nos trabalhos, a partir dos critérios estabelecidos, inclusive com mais detalhamento do que vem sendo realizado e as oportunidades de melhoria no processo. Destacamos que o Plano de ação (doc. SEI 0064550) foi elaborado em outubro de 2021 pelas equipes do Centro de Processamento e Preservação (CPP) e do Centro de Coleções e Serviços aos Leitores (CCSL), apresentando uma descrição do acervo da Biblioteca Nacional, e dando maior atenção para as obras que são consideradas raras, além de trazer toda a construção das medidas de digitação implementadas.

10) monitoramento da implantação dos objetivos previstos no Decreto nº 10332/2020, entre outros assuntos.

Com o retorno do Ministério da Cultura, é conveniente e oportuno buscar seu apoio para viabilizar a implantação das demais metas pactuadas no Plano de Transformação Digital, e obter a participação e contribuições, no âmbito da competência ministerial, no processo de tomada de decisão, com fins de alcançar os objetivos

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

estratégicos, geração de valor público e cumprimento da sua missão institucional. Outra vantagem, é evitar duplicidade de esforços e composição de soluções em temas que guardem transversalidade. Nas reuniões do Comitê de Governança, é importante que se avaliem quais os objetivos previstos no Decreto nº 10332/2020 estão pendentes, para que se possa, conforme o caso, fazer novas repactuações no PTD.

2.2 CONSTATAÇÃO 01: NECESSIDADE DE IMPLEMENTAÇÃO DAS MEDIDAS URGENTES DO EIXO IV - SEGURANÇA E PRIVACIDADE – PTD

Das atividades programadas no Eixo IV do Plano de Transformação Digital, foram realizadas apenas as seguintes:


- Elaboração e publicação da Política de Segurança da Informação (POSIN)
- Designação do Gestor de Segurança da Informação, titular e suplente, por meio de ato normativo aprovado pela autoridade máxima do órgão
- Instituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR
- Instituição do Comitê de Segurança da Informação

A Lei Geral de Proteção de Dados dispõe que o órgão deverá estabelecer medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão

“Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; ”

“Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. ”

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

Atualmente a FBN oferece serviços digitais que carecem de que sejam periodicamente revisitados os protocolos de segurança.

A FBN precisa retomar as ações para cumprir o Eixo IV – Segurança e Privacidade no que compete principalmente à adoção de medidas de prevenção e segurança, a fim de evitar a ocorrência de novos incidentes, visto que, em abril de 2021, a instituição foi vítima de ataque hacker, comprometendo alguns arquivos do acervo digital.

Entre as medidas de segurança e privacidade, temos:

Medidas Básicas


1. Controle de Conformidade de Privacidade.
2. Controle de Conformidade de Segurança.

Medidas Urgentes

1. Controle de Backup.
2. Controle de Gestão de Acessos.
3. Controle de Gestão de Vulnerabilidades.
4. Controle de Inventário de Ativos.
5. Controle de Auditoria.

Práticas para o Controle de Backup: Acórdão 1.109/2021 – Plenário Tribunal de Contas da União (TCU):

1. conformidade do backup realizado dos sistemas com **a política de backup**;
2. realização de testes de restauração periodicamente;
3. solução de backup estar situada em ambiente isolado ao ambiente com os dados originais;
4. existência de mecanismo de segurança (firewall, IPS, etc.) entre a rede do backup e a rede do ambiente original,
5. capacidade para solução abarcar integralmente o backup de todo o ambiente dos sistemas (considerando a adoção de uma estratégia mínima de backup);
6. contrato vigente de suporte e garantia para a solução de backup;

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

7. procedimentos criptografados dos backups, em casos que convém manter a confidencialidade;
8. retenção dos backups por tempo suficiente para atendimento às legislações relacionadas aos requisitos de negócio.

A FBN carece de política de backup, de modo a documentar de quais dados serão feitos os *backups*, as suas respectivas periodicidades, tipos, quantidades de cópias, locais armazenamento, tempos de retenção e outros requisitos de segurança (processo SEI nº 01430.000304/2020-21 - documento 0048791).


Convém, também, intensificar a periodicidade da realização dos testes de restauração dos servidores.

No que se refere ao armazenamento dos arquivos de backups da FBN, verificar os serviços de hospedagem na “nuvem” (cloud services), de forma que estejam bem protegidos, evitando que estejam armazenados somente na própria sede da organização

Além disso, a FBN deve procurar mitigar a ocorrência de incidentes de segurança relacionados ao local e ambiente de armazenamento das cópias de segurança, para que não esteja desprotegido (processo n. 01430.000304/2020-21 - documento 0048791)

No Controle de Gestão de Acessos, as seguintes práticas são esperadas:

1. Dar conhecimento à unidade de TI imediatamente, para fins de realizar a revogação dos acessos ao ambiente computacional, nas situações abaixo:
 - a) quando um servidor ou estagiário se desliga do órgão,
 - b) quando um terceirizado se desliga de contrato não gerido pela TI, e
 - c) quando um terceirizado se desliga de contrato gerido pela TI;
2. Estabelecer um processo automatizado para desabilitar contas inativas após determinado período de inatividade;
3. Aplicar a prática de privilégio mínimo nas estações de trabalho dos usuários;
4. Constituir múltiplo fator de autenticação habilitado para os usuários, e administradores na rede do órgão e na autenticação para acesso aos sistemas;
5. Aplicar os sistemas internos de gerenciamento da infraestrutura de TIC que possuem múltiplo fator de autenticação habilitado;

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

6. Aplicar os sistemas externos, em nuvem, para gerenciamento da infraestrutura de TIC que possuem múltiplo fator de autenticação habilitado;
7. Criar complexidade de senhas implementada nas contas dos usuários;
8. Adotar um processo formal para concessão de acesso à VPN para usuários;
9. Aplicar assinatura de um termo de responsabilidade para que os usuários obtenha acesso à VPN;
10. Aplicar o acesso à VPN possui múltiplo fator de autenticação habilitado;
11. A instalação e atualização de antivírus é exigida para que os usuários acessem o ambiente pela VPN;
12. Existir um processo automatizado para verificação da saúde operacional das estações de trabalho de usuários em trabalho remoto que acessam o ambiente pela VPN.

Práticas para Gestão de Vulnerabilidades

1. Possuir janelas periódicas de atualização de patches de sistemas operacionais:
 - 1.1. Nas estações de trabalho dos usuários,
 - 1.2. Nos servidores;
2. Realizar varreduras de vulnerabilidades periodicamente;
3. Possuir uma rotina automatizada de atualização de aplicativos de prateleira;
4. Possuir uma rotina automatizada de atualização dos sistemas internos de gerenciamento da infraestrutura de TIC;
5. Tratar rapidamente as vulnerabilidades identificadas nos sistemas;
6. Possuir um software centralizado para gerenciamento de patches e atualização de:
 - 7.1. Sistemas operacionais das estações de trabalho dos usuários,
 - 6.2. Sistemas operacionais Windows Server,
 - 6.3. Sistemas operacionais Linux nos servidores.


O Programa de Privacidade e Segurança da Informação (PPSI) objetiva elevar o grau de maturidade dos órgãos e das entidades do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) em termos de proteção de dados pessoais e ações de segurança da informação.



Conforme o art. 3º, inciso I, item “d” da Estratégia de Governo Digital (EGD), instituída pelo Decreto 10.332/2020, o Eixo 4 – Segurança e Privacidade está alinhado com as metas estabelecidas no âmbito do Programa de Privacidade e Segurança da Informação (PPSI) da Secretaria de Governo Digital (SGD).

Seguem, abaixo, sugestões de guias e modelos do Programa de Privacidade e Segurança da Informação (PPSI) que podem ser usados para a privacidade, a segurança da informação e a proteção de dados:

- **Framework de Privacidade e Segurança da Informação:** propõe às instituições públicas diretrizes para auxiliar a identificação, o acompanhamento e o preenchimento das lacunas de privacidade e segurança da informação existentes na organização.
- **Modelo de Política de Backup:** tem por enfoque prover diretrizes para política de backup e restauração de dados digitais.
- **Modelo de Política de Gestão de Ativos:** tem por objetivo prover diretrizes para a gestão de ativos.
- **Modelo de Política de Controle de Acesso:** tem por finalidade prover diretrizes para o controle de acesso.
- **Modelo de Política de Gestão de Registros (Logs) de Auditoria:** tem por objetivo prover diretrizes para a gestão de registros de auditoria.
- **Guia de Gerenciamento de Vulnerabilidades e Modelo de Política de Gerenciamento de Vulnerabilidades:** abordam a construção de processos repetitivos de ciclos de gerenciamento das vulnerabilidades em proteção e segurança de dados da instituição.
- **Programa de Governança em Privacidade:** apresenta os principais pontos da LGPD, fornecendo os subsídios para a criação de um programa institucional de gerenciamento de privacidade.
- **Inventário de Dados Pessoais:** incentiva a adoção de inventários de todas as operações de tratamento de dados pessoais e suas respectivas avaliações, sob a ótica dos princípios da LGPD.
- **Termo de Uso e Política de Privacidade:** orienta a elaboração de Termos de Uso e Políticas de Privacidade vinculados à utilização de serviços públicos prestados por meio de aplicações (sites, sistemas ou aplicativos para dispositivos móveis) e fornecidos por órgãos e entidades da administração pública.
- **Avaliação de Riscos:** orienta a identificação e a mensuração de riscos de segurança e privacidade, mitigando-os com a utilização dos controles mais indicados.
- **Requisitos e Obrigações quanto à Segurança da Informação e à Privacidade:** orienta a adequação do processo de contratação para contemplar os

| | | |
|---|-------------------------------|----------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO


requisitos mais importantes de segurança e privacidade dos dados, conforme a Instrução Normativa SGD nº 31, de 23 de março de 2021.

- **Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** orienta a elaboração de documento de comunicação e transparência que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como propõe medidas, salvaguardas e mecanismos de mitigação.
- **Guia de Segurança em Aplicações Web:** auxilia os profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação.
- **Guia de Resposta a Incidentes de Segurança:** apresenta boas práticas para que as instituições e os profissionais de segurança da informação realizem o tratamento de incidentes cibernéticos, com enfoque em incidentes que envolvam dados pessoais.
- **Guia de Requisitos Mínimos de Segurança e Privacidade para APIs:** apresenta, para as instituições e os profissionais de segurança da informação, as boas práticas a serem aplicadas para proteção dos dados pessoais quando do uso de Interface de Programação de Aplicações (*Application Programming Interface* - API).
- **Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis:** fornece orientações básicas e auxilia os profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, nas distintas etapas do desenvolvimento da aplicação.
- **Guia de Boas Práticas - LGPD:** fruto de debates internos ao Ministério da Economia e de contribuições técnicas de órgãos e entidades externas, consolidados no âmbito do Comitê Central de Governança de Dados, foi aprovado e disponibilizado por intermédio da Resolução CCGD nº 4, de 14 de abril de 2020. Fonte: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd>

Considerando a necessidade de implementação das medidas urgentes do EIXO IV - SEGURANÇA E PRIVACIDADE – PTD, apresentamos a Recomendação 01 abaixo.

3 CONCLUSÃO

Concluimos que a Fundação Biblioteca Nacional avançou com a reestruturação estatutária e regimental com a criação da Coordenação de Tecnologia de Informação, e atingiu o cumprimento parcial do Decreto nº 10.332/2020, acompanhados pelo Comitê de Governança Digital, tendo como benefícios, a aprovação do Plano de Transformação Digital (PTD), do Plano Diretor de Tecnologia Informação e Comunicação (PDTIC), da

| | | |
|---|---------------------------------------|--------------------------------------|
|  FUNDAÇÃO BIBLIOTECA NACIONAL | RELATÓRIO DE AUDITORIA | ORIGEM: AUDITORIA INTERNA |
| | | DATA: 27/03/2023 |

RESERVADO

Política de Segurança da Informação (POSIN), a realização de medidas básicas do Eixo IV do PTD, com a designação do Gestor de Segurança da Informação, a instituição de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR e do Comitê de Segurança da Informação, e, na atualização da sua Carta de Serviços, em que contou com a disponibilidade do serviço "Solicitar bolsa de pesquisa da Biblioteca Nacional" por meio de formulário digital, e o destaque na transformação digital dos serviços do Escritório de Direitos Autorais.

A FBN conseguiu avançar, sobretudo, no segundo semestre de 2022, a partir da rotina de reuniões do Comitê de Governança Digital da FBN, mas ressaltamos que as pautas precisam ser retomadas no exercício de 2023, cabendo destacar a necessidade de se avançar na implementação do Depósito Legal Digital.

Considerando a necessidade de aprimoramento da gestão de riscos, e as medidas já elencadas no EIXO IV - SEGURANÇA E PRIVACIDADE do PTD, recomendamos:

RECOMENDAÇÃO 01: Priorizar as medidas contidas no EIXO IV - SEGURANÇA E PRIVACIDADE –previstas no PTD, junto ao Ministério da Economia e ao Ministério da Cultura, em especial as medidas urgentes, relacionadas aos controles de backup, de gestão de acessos e vulnerabilidade, de inventário de ativos e de auditoria, bem como na adoção de controles adequados para mitigar riscos que possam comprometer a proteção dos dados pessoais.

Rio de Janeiro, 27 de março de 2023.


GLÁUCIO CAVALCANTI TAK-MING
Auditor-Chefe
Fundação Biblioteca Nacional