Inventário de Aplicações

ID	Pilar	Tecnia	Título	Data	Duração Investimento	Prioridade Ganhos Financeiros	Prioridade Ganhos de Operação	Estimativa de Custo	Problemática	Usuário	Risco de TI	Risco de Negócio	Recomendação
001	Sistemas	ERP	ERP - Mapeamento de Processos e levantamento de Requisitos	MD	10	Baixa	Média	Baixa	R$ 400.000,00	N/A	Utilização de sistemas departamentais sem integração e alto volume de controles manuais.	N/A	N/A	Apoiar as áreas Administrativas na contratação de consultoria técnica especializada para mapeamento de processos e levantamento de requisitos funcionais e não funcionais para implantação de sistema ERP
002	Sistemas	ERP	ERP - Seleção da Solução	MD	8	Baixa	Média	Baixa	R$ 300.000,00	001	Utilização de sistemas departamentais sem integração e alto volume de controles manuais.	N/A	N/A	Apoiar as áreas Administrativas na contratação de consultoria técnica especializada no serviço de solução ERP caso adequado às necessidades do MDB, visto que o RFP e "Roadmap Claro" para seleção de fornecedor e implantação da solução.
003	Sistemas	ERP	ERP - Implantação do Sistema	MD	48	Baixa	Alta	Alta	R$	002	Utilização de sistemas departamentais sem integração e alto volume de controles manuais.	Maior vulnerabilidade a ataques cibernéticos. Alta complexidade para customização dos sistemas;	Ineficiência operacional. Horas cansadas por intervenções manuais. Alta complexidade para customização de apoio, informações gerenciais desperdiçadas.	Apoiar as áreas Administrativas na contratação de consultoria técnica especializada para implantação de sistema ERP selecionado, gerência da mudança cultural e organizacional, gerenciamento do programa e controle de qualidade das entregas.
004	Governança	Liderança	Processo Processos de Prospecção de Soluções de TI	MD	48	Baixa	Alta	Alta	R$	002	Gestão do relacionamento com o negócio ineficiente.	Ineficácia das operações de TI	Não atendimento das necessidades gerais TI	Estabelecer processo processo de prospecção de soluções de TI para atendimento de necessidades do negócio, respaldando os pontos focais de cada área do empresa, definindo suas responsabilidades, frequência e forma de atuação.
005	Governança	Liderança	Política de Equipamentos Pessoais	MD	6	Média	Média	Alta	R$	N/A	Inexistência de padronização dos equipamentos.	Suporte a diversos modelos de equipamentos pessoais, descentralizados	N/A	Estabelecer política padrão do equipamento de tecnologia e divulgar para toda companhia.
006	Governança	Liderança	Processo Master of Buy para aquisição de softwares.	MD	4	Média	Alta	Alta	R$	N/A	Processo decisórios para aquisição de softwares ineficientes.	Maior enfoque na contratação de ferramentas autônomas no mercado	Contratos e custo excessivos na aquisição de soluções sistêmicas.	Estabelecer diretrizes e procedimentos para aquisição de novos softwares e/ou desenvolvimento dos sistemas para atendimento das demandas do negócio. Processo Master of Buy
007	Governança	Comitês	Estabelecimento de Comitês de TI	MD	6	Baixa	Alta	Alta	R$	N/A	Ausência de comitês de TI.	Desalinhamento estratégico de TI com o negócio	N/A	Estabelecer Comitês que endereçam as pautas de Governança de TI, Projetos e Inovação de TI, observando suas responsabilidades e atribuições específicas, conforme proposta do Anexo 1 e 2 e 3 e cada unidade deverá ser participada por um comitês específicos.
008	Governança	Planejamento	Governança de Tecnologia	MD	2	Alta	Alta	Alta	R$ 60.000,00	N/A	Ausência de estratégia para aquisição de serviços de TI terceirizados.	Contratações ad-hoc de terceiros.	Ineficiência no atendimento de demandas pela TI	Definir estratégia de terceirização de fornecedores, considerando os custos de serviços e as responsabilidades que devem ser transferidas ao 1º equipe interna de TI ou equipadas a terceiros.
009	Governança	Monitoramento e Controle	Análise do Desempenho de TI	MD	2	Alta	Alta	Alta	R$ 60.000,00	N/A	Ausência de métricas definidas para a acompanhamento operacional de TI, não suficientes para a volta geral do desempenho.	Dificuldade de monitorar o desempenho de TI	N/A	Estabelecer KPI's e Dashboard para monitoramento e controle e acompanhamento e evolução de TI.
010	Governança	Monitoramento e Controle	Gestão de Prestadores	MD	2	Média	Alta	Alta	R$ 60.000,00	N/A	Processos estabelecidos entre TI e fornecedores possuem prestadores previstos, porém não foram identificadas práticas nem processos formais para aplicação das prestadores previstos, quando aplicáveis.	Desgastes de relacionamento pelos fornecedores pela falta de aplicação de prestadores previstos em contrato.	Ineficiência no atendimento das demandas pela TI	Estabelecer processo de monitoramento do serviço contratado, e, no caso/cenário de falha por atividade prestadores previstos em contrato, acionar departamento jurídico e avaliar sua aplicabilidade.
011	Processos	Controle Orçamentário	Processo de Controle Orçamentario	MD	6	Média	Alta	Alta	R$ 60.000,00	N/A	Ausência de processo definido e documentado para controle de verba, saída e acompanhamento. Não há definição clara sobre as papéis e responsabilidades acerca da análise e reporte das gestão financeira.	Gestão Orçamentaria Ineficiente	N/A	Mapear e documentar o processo de controle orçamentário, incluindo documentação de etapas de classificação orçamentaria, reporte RAC e periodicidade de reportes.
012	Processos	Alocação de Recursos	Processo Orçamentario	MD	2	Alta	Alta	Alta	R$ 60.000,00	009	Inexistência de um processo documentado para priorização orçamentária.	Gestão Orçamentaria Ineficiente	N/A	Estabelecer um processo para priorização orçamentaria, saber como para estabelecer consumo/gastos de recursos orçamentarios.
013	Processos	Alocação de Recursos	Processo de Compra ou Locação de Ativos	MD	2	Alta	Alta	Alta	R$ 60.000,00	006	Falta de um procedimento documentado para verificação de aqdquecimento comprar ativos/serviços ou contratação de uso de ativos/serviços.	Gestão Orçamentaria Ineficiente	N/A	Mapear um processo para que se verifique entre a opção de compra ou locação de ativos, saber como determinar internamente um serviço ou contratá-lo externamente, a cada solicitação de compra de ativo ou serviço.
014	Processos	Elaboração Orçamentaria	Elaboração Orçamentaria	MD	2	Alta	Alta	Média	R$	009	Ausência de um processo, não há uma documentação de quais componentes considerar.	Gestão Orçamentaria Ineficiente	N/A	Criar uma documentação contendo os componentes a considerar na elaboração do orçamento, respondendo o quê, quando e como.
015	Processos	Dados Orçamentarios	Gestão de Dados Orçamentarios	MD	2	Alta	Alta	Média	R$	009	Não há um processo para coleta de dados relevantes para identificar desvios no orçamento quanto aos real gastos/ganhos, considerando do custo de serviços RDI de investimento, quando aplicável.	Gestão Orçamentaria Ineficiente	N/A	Definir, documentar e implementar um processo para coleta e verificação dos dados relevantes para identificar desvios do orçamento quanto aos real gastos/ganhos, considerando do custo de serviços e investimento RDI do investimento, quando aplicável.
016	Processos	Acordos de Serviços Gerenciados	AP0208 - Estabelecer processo Acordos de Serviços Gerenciados	MD	6	Média	Alta	Alta	R$ 80.000,00	N/A	Não há processo definido para análise, em uma linha de tempo, dos serviços atuais de TI e seus SLAs, para identificar lacunas entre o esperado pelo negócio e o realizado.	Ineficiência na prestação dos serviços para negócio	N/A	Estabelecer processo Acordos de Serviço Gerenciados para: - Avaliar dos serviços atuais de TI e seus SLAs, verificando se está alinhado com as necessidades do negócio; - Identificar lacunas entre o esperado e demanda futura de serviços de TI, para que se possa antecipar a capacidade dos serviços oferecidos; - Definição dos SLAs necessários para os serviços a serem realizados e/ou contratados, assim como a definição dos KPI's para o atendimento deles, quando aplicável.
017	Processos	Acordos de Serviços Gerenciados	AP0209 - Atualização do Catálogo de Serviços de TI	MA	2	Média	Alta	Alta	R$	N/A	Não há processo definido para atualização periódica do Catálogo de Serviços de TI	N/A	N/A	Estabelecer processo para revisão periódica do Catálogo de Serviços de TI para atendimento às necessidades do negócio.
018	Processos	Riscos Gerenciados	AP0212 - Estabelecer processo Riscos Gerenciados	MD	6	Média	Média	Média	R$ 80.000,00	N/A	Não há processo definido e implementado para gestão de riscos de TI.	Ineficiência de identificação, documentação e classificação dos riscos de TI.	N/A	Estabelecer processo de gestão de riscos de TI para: - Documentar e manter um método para coleta, classificação e análise de dados relacionados a riscos de TI; - Registrar dados relevantes e específicos do ambiente operacional interno e externo do MDB que possam estar relacionados a riscos; - Criar o Mapa de Riscos de TI, agregando e documentando cenários de riscos atuais por categoria, linha de negócio e área funcional.
019	Processos	Ativos Gerenciados	AP0219 - Estabelecer processo de Gestão de Ativos de TI	MD	6	Média	Alta	Alta	R$ 80.000,00	N/A	Não existe um processo documentado e implementado para gestão de Ativos.	Ausência de controle dos ativos da empresa	Fuga de Capital e multas por descumprimento de requisitos legais para licenciamento de softwares.	Estabelecer processo de Gestão de Ativos de TI para: - Identificar o inventário de ativos tecnológicos, requisitos legais e regulatórios, ativos críticos, risco e impacto na linha de um ativo, salvaguarda ativos ou propósito; - Formalização do processo de compra de Ativos de TI; - Centralizar a gestão de licenças de software no departamento de TI; - Realizar estudo para escolha de ferramenta autônoma semi-autônoma de inventário de ativos tecnológicos no mês e realizar sua implementação.
020	Processos	Mudanças de TI Gerenciados	AP0216 - Estabelecer processo de Gestão de Mudança de TI	MD	6	Média	Média	Alta	R$	017	Não há processo de Gestão de Mudanças de TI	Mudanças de TI não documentadas e/ou programadas.	Instabilidade dos serviços de TI	Estabelecer processo Gestão de Mudança para: - Definir que toda mudança seja realizada pelo processo de Gestão de Mudança, com requerimento e aprovação formal, de forma a garantir o controle, planejamento e comunicação; - Gerar um registro de todo e qualquer mudança realizada, contendo informações de que foi realizado, quais configurações foram alteradas e etc. Manter este registro por um tempo determinado.
021	Processos	Configurações Gerenciados	AP0210 - Estabelecer processo Gestão de Configurações	MD	4	Média	Média	Alta	R$	017	Não há processo definido para gerenciada configuração.	Falta de padrão na configuração dos ativos	N/A	Estabelecer processo para gestão da configuração dos ativos, definindo e documentando os linha base necessárias.
022	Processos	Operações Gerenciados	20001 - Estabelecer Procedimento Operacional de TI	MD	4	Média	Média	Alta	R$	N/A	Não há procedimento operacional de TI definido e documentado.	Ausência de padronização operacional.	N/A	Estabelecer documentação referente aos procedimentos operacionais de TI, contendo pelo menos de tarefas e atividades operacionais e sua execução, incluindo ações de rotina e checagens de ativos, quando aplicável. Registrar todos os eventos ocorridos no infraestrutura de TI, considerando os dados processados.
023	Processos	Requisições de Serviços e Incidentes Gerenciados	20002 - Estabelecer processo de gestão de Requisições de Serviço e Incidentes	MD	4	Média	Alta	Alta	R$	020	Não existe um processo definido para atendimento às requisições de serviços e incidentes.	Ausência de fluxo de ticket e de ciência e base de conhecimento.	N/A	Estabelecer processo de atendimento às requisições de serviços e incidentes, classificando-a e implementando uma base de conhecimento para otimizar a solução de problemas/incidentes já conhecidos. Manter um documento PADs para problemas/incidentes conhecidos e suas respectivas soluções.
029	Sistemas	Desenvolvimento	Ciclo Disciplina de Desenvolvimento	MD	6	Média	Alta	Alta	R$	N/A	Existe uma cultura de desenvolvimento interno no SIB e/ou demandas de negócio para sistemas de tecnologia, sem a sistematização/governança de TI.	Equipe/ação nicos tecnológicos e de segurança devido ao desenvolvimento não mantenedores pela TI.	Sensagem nos, adaptar ou desenvolvimento (customizações) de soluções que contem no desenvolvimento de soluções, sem o devido controle e governança, gerando custos e riscos de segurança e/ou operacionais e/ou econômicos e/ou prejuízos. A TI deve's estabelecer normas e guidlies para utilização dessa metodologia adotada pelos áreas de negócio.
030	Sistemas	Hospedagem	Hospedagem de Sistemas Em Premise	MD	0	Baixa	Baixa	Alta	R$	N/A	90% dos aplicações estão/estão pesquisam sua hospedagem On Premise (rack/ou em data center interno/quarto utilizado/etc).	Indisponibilidade/erros caos ocasionando na a gerência não passam a enxergar/ver/ouvir/sentir.	Indisponibilidade de sistemas/serviços tecnológicos	Migrar as aplicações On Premise para Cloud, conforme os equipamentos chegam ao final do ciclo de vida.
031	Sistemas	Obsolescência de Tecnologia	Banco de Dados	MD	6	Média	Média	Média	R$	N/A	Existem 3 aplicações que utilizam banco de dados que são/que são/hospedados em servidores/com sistema operacional Windows Server 2008 R2, considerada obsoleta e fora seu ciclo de vida terminado em janeiro/2020. Adicionalmente, existem 7 aplicações que utilizam banco de dados que são/hospedados em servidores/com sistema operacional com término de seu ciclo de vida programado para junho/2019: RH61 e o RH62. 7 x	Vulnerabilidades e invasíveis/ou de suporte técnico em versões de bancos de Dados consideradas obsoletas	Indisponibilidade em serviço e sistemas de TI que utilizam base de dados.	Atualizar a versão dos bancos de dados para a mais recente: Oracle 19c, PostgreSQL 15.2 e SQL Server 2019
027	Sistemas	Obsolescência de Tecnologia	Sistema Operacional dos servidores de Banco de Dados	MD	6	Média	Média	Média	R$	N/A	Existem 3 aplicações que utilizam banco de dados que são/que são/hospedados em servidores/com sistema operacional Windows Server 2008 R2, considerada obsoleta e fora seu ciclo de vida terminado em janeiro/2020. Adicionalmente, existem 7 aplicações que utilizam banco de dados que são/hospedados em servidores/com sistema operacional com término de seu ciclo de vida programado para junho/2019: RH61 e o RH62. 7 x	Vulnerabilidades e invasíveis/ou de suporte técnico em versões de Sistemas Operacionais obsoletas.	Indisponibilidade em serviço e sistemas de TI que utilizam base de dados.	Atualizar o sistema operacional dos servidores de banco de dados mencionados para as versões: Windows Server 2022 e RH61 8.

ID	Pilar	Tema	Título	Data	Duração Semana	Prioridade Grupo Financeiro	Prioridade Compatibilidade	Prioridade Grupo de Operação	Estimativa de Custo	Problemática	Usuários	Risco de TI	Risco de Negócio	Recomendação
G28	Sistemas	Obsolescência de Tecnologia	Sistema Operacional dos servidores de Replicação	MD	6	Média	Média	Média	R$	N/A	Grupos de usuários com permissões de acesso indevidas. Sistema operacional obsoleto (Windows Server 2008 R2, RHEL 6, Oracle Linux 6.0). Que deixam seus dados de cada terminal bem guardados (EBS) ocasionou DOS8 e mar/2017, respectivamente. Ademais, existem 3d aplicações que dão hospedadas em servidores com sistema operacional sujo cobre de vida está próximo de sua finalização. RHEL 7 e sucessores.	Vulnerabilidade a invulnerabilidade de suporte técnico e em servidores de bitcoins. Operacionais obsoletos.	Indisponibilidade em aplicações de TI.	Atualizar o sistema operacional dos servidores de banco de dados mencionados para as versões: Windows Server 2012 e RHEL 8.
G29	Sistemas	Dados	Heterogeneidade Dados Técnicos/Ontológicos armazenados	MD	12	Baixa	Baixa	Alta	R$ 720.000,00	N/A	Os dados dos sensores/equipamentos são armazenados em base de dados distintas, sem padrão específicos que os dados que representam as características das sondas, o que dificulta a interpretação da informação pelos analistas Bioes.	Inteligência no armazenamento de dados	Interpretação/acesso ao de dados técnicos.	Revisar Projeto de Estruturação de Dados, para que os dados possam ser classificados e organizados de maneira padrão, mutuando suas unidades de medida e nomenclaturas para descrição de suas características, de acordo com os conceitos de MDM (Master Data Management).
G30	Sistemas	Aplicações	Software de Gestão para área MCTIR (Minerais)	MD	4	Média	Média	Alta	R$	G01	Como MCTIR não possui um sistema que agiar na gestão de Minerais. O sistema Pergamum é utilizado para de controle específico para operacionalizar. Não é suficiente para agiar todos os processos de bens, requisito relevado pela minería, gerando grande trabalho em controlar controlar os bens em planilhas Excel.	N/A	Sobrecarga no cadastro de itens de Minerais e em controle de bens	Colocar o módulo de Gestão de Ativos/Patrimônio do sistema ERP e ser implementado ou inserir em uma solução que atenda por completo todos os requisitos funcional definido pela área usuária em substituição as soluções atuais.
G31	Infraestrutura	Serviços	Cloud - Fundação	MS	4	Média	Média	Média	R$ 170.000,00	N/A	Serviços e atividades de TI desenvolvidas, Estrutura de clouds desprotegidas/abertas e vulnerabilidade em ambiente cloud.	Acesso indevido as aplicações/ou ambiente Cauda sendo trafegados pela internet em acesso/ruptura de serviços da cloud.	Exposição de informações sensíveis via internet	Implementar o conceito de landing zone (detalhadores diagrama) em todos os serviços de cloud. Implementar firewall no ambiente cloud e melhorar/adequar para aumento de segurança e utilizadade nas vulnabilidade. Implementar configuração Private Endpoints para que o tráfego seja via backbone, não via internet, ou troca de informações entre objetos para serviços não críticos e sem exposição de dados. Utilizar a configuração Private Service Endpoints para que o tráfego seja via rede interna do fornecedor, não via backbone ou internet, na troca de informações entre objetos para serviços críticos e sensíveis para segurança de dados.
G32	Infraestrutura	Serviços	Cloud - Consolo Private	MS	12	Baixa	Baixa	Baixa	R$ 20.000,00	N/A	Ausência de consolo ponto a ponto com fornecedor de cloud.	Dados sendo trafegados pela internet ou acesso ao recurso de cloud	Exposição de informações sensíveis via internet	Estabelecer consolo dedicado e private com fornecedor de cloud para acesso seguro aos seus serviços e dados.
G33	Infraestrutura	Serviços	Cloud - Adoção de Cultura PetrOpa	MD	12	Baixa	Baixa	Baixa	R$	N/A	Sendo financeiras realizada sem a adoção das melhores práticas de mercado.	Não manter o controle de custos de TI	N/A	Implementar PetrOpa de acordo com seus conceitos e considerando os pontos listados abaixo: Revisar Organização/Treinamento para área responsável e equipe de TI sobre os conceitos de PetrOpa, custos operacionais de TI e sua estrutura; Revisar e implementar o processo de gestão de mudanças; Utilizar métrica para controle do custo de TI, programas de recuperação, gamificação e educação em diversos canais para disseminar a cultura e ações no novo modo de trabalho;
G34	Infraestrutura	Dados	Azure - Licença P1	MD	6	Média	Baixa	Baixa	R$ 468.000,00	N/A	Impossibilidade de utilização do BID (single sign-on) para as aplicações, através do Azure AD.	N/A	N/A	Implementar funcionalidades da licença P1 do Azure nesses em vista o aumento da capacidade de monitoramento, resposta de acessos, proteção de vulnerabilidades, risco e acesso privilegiado. Implementar SBO. Implementar Acesso condicional baseado em risco. Criar processo de revisões de acesso. Configurar Conexões seguras de diretórios.
G35	Infraestrutura	Redes	Rede de Dados - Latência	MD	36	Baixa	Baixa	Baixa	N/A	N/A	Performance da Rede de Dados abaixo dos padrões e necessidades das aplicações.	N/A	N/A	Verificar latência dos regionais para a sede e centro e cloud gerando documento de controle; Realizar estudo de tempo e movimentos para analisar performance dos links e aplicações de negócio.
G36	Infraestrutura	Redes	Rede de Dados - Redundância de Links	MD	36	Média	Baixa	Baixa	R$ 360.000,00	N/A	Ausência de links redundantes nas unidades.	Indisponibilidade de conectividade de rede	Indisponibilidade de aplicações e serviços.	Realizar a contratação de link adicional para cada unidade, promovendo disponibilidade dos serviços de TI em caso de falha dos principais. Configurar a utilização dos links de dados no modo "Ativo-Ativo" (Balancear de carga).
G37	Infraestrutura	Redes	Rede de Dados - Compartilhamento de Backbone Internet	MS	2	Baixa	Baixa	Baixa	N/A	N/A	Ausência de informações sobre o compartilhamento de infraestrutura dos provedores de internet.	Indisponibilidade de conectividade em decorrência de backbone compar tilhado entre operadoras	Indisponibilidade de ambiente, recursos e aplicações de negócio	Obter a informação da seguinte forma: 1- Acesso a site da operadora para consulta de link e tráfego de inter-conexão, ou; 2- Acesso a site específico a operadora responsável por disponibilizar ou na mesma ocasião que a NOC está sendo acionada. Ocasiões que você está no ambiente ou qual você deveria obter o APN com o código 4G/3G, ou seja Bug Iner, ou campo search digitar o APN do provedor, para inter-PNL clicar no atos Graph ve ou para PNA clicar na atos Graph vé, cada atos mostra todas as rotas BGP que qual o provedor deve estar para acessar a internet.
G38	Infraestrutura	Redes	Rede de Dados - Fundação	MD	12	Baixa	Baixa	Baixa	62000	N/A	Custos elevados com links, gerenciamento de rotas não otimizado, subtrocação para acesso ao ativo de rede devem estabelecer e ausência de acesso alternativo ao ambiente.	Acesso indevido aos ativos de rede e indisponibilidade do ambiente.	Indisponibilidade de ambiente, recursos e aplicações de negócio.	Revisar BIP com operadoras de atendimento nacional para redução de custos e melhorias na prestação de serviços; Implementar configuração avançada no roteador BIP que tem como objetivo replicar rotas parâmetro para todos os roteadores da rede, reduzindo custos e melhorias; Implementar protocolo de segurança (IPsec/MD5) no TACACS para o gerenciamento da autorização e autenticação centralizada de acesso aos roteadores e switches; Desenvolver contratos e ou aditivos com as operadoras para reduzir custos e ou prestar; Implementar controle de endereçamento de rede que permita informações como: VLAN ID, redes, endereço IP e máscara de rede, para todos os ativos de rede;
G39	Infraestrutura	Redes	Rede de Dados - SD-WAN	MD	4	Baixa	Baixa	Baixa	R$ 300.000,00	N/A	Desnecessário de rotas, políticas, QoS e backbone internet desenvolvidas.	Ineficiência no gerenciamento do ambiente	N/A	Implementar solução de SD-WAN para a rede, centralizando o gerenciamento de políticas e tráfego nas bordas via APN, QSPR (ou portadores similares), criando um backbone próprio.
G40	Infraestrutura	Redes	Rede de Dados - Segmentação	MS	12	Baixa	Baixa	Baixa	N/A	N/A	Rede de dados não segmentada.	Alcance/ataque/hacker no ambiente	Exposição de informações sensíveis.	Implementar as VRFs por segmentação de rede (Equipamentos de roteadores); Utilizar recurso DHCP de acordo com a quantidade de dispositivos por departamento.
G41	Infraestrutura	Redes	Rede de Dados - Contratos	MD	6	Média	Baixa	Baixa	250000	N/A	Ausência de controle de extensão de garantia para equipamentos de rede com suporte ATIVO/EOS para equipamentos críticos ou que requer zeros. Suporte 8/5NBD para equipamentos com baixa criticidade.	Indisponibilidade de ambiente, recursos e aplicações de negócio	Indisponibilidade de ambiente, recursos e aplicações de negócio	Contratar extensão de garantia para equipamentos de rede com suporte ATIVO/EOS para equipamentos críticos ou que requer zeros. Suporte 8/5NBD para equipamentos com baixa criticidade.
G42	Infraestrutura	Dados	Serviços - Servidor de Arquivos	MS	36	Alta	Média	Média	R$ 1.100.000,00	N/A	Serviços de armazenamento desorganizado e sem consolidação.	Grupos de usuários com permissões de acesso indevidas	Acesso indevido a informações	Implementar uma solução física de servidor de arquivos corporativo; Revisar os grupos que deveriam ser movidos para nuvem cloud. Arquivos com tempo de vida maior que 3 anos deveriam ser arquivados em archive; Revisar o mapeamento de grupos e pastas em cada diretório; Implementar políticas no arquivos garantindo sua permissão através de snapshot ou backup/restore ou ferramenta cibersegs; Isolar os acessos para os grupos nas pastas privilegiadas mapeadas; Obs. Exemplo usando um ambiente com Azure: custo estimado para 6TB = Reserva 1 ano = U$ = >= R$ 1.258 Ano ou Reserva 3 anos = U$ = R$ 840 ou = U$ 588 Ano
G43	Infraestrutura	Dados	Segurança - Gestão de Administração	MS	4	Baixa	Baixa	Baixa	R$	N/A	Gerenciamento descentralizado de contas do administrador local do sistema operacional Windows.	Alcance/ataque/hacker no ambiente	Exposição de informações sensíveis.	Implementar Windows LAPS no ambiente e limitar a quantidade de contas com privilégios elevada, diferenciando uma solução de centralização e gerenciamento de senha para conta de administrador local das estações de trabalho. Revisar política referente ao tamanho da senha no ambiente e nome de conta do administrador (contas com privilégios de administrador alteradas no ou existentes de conta/senha de banners); Para ambiente cloud habilitar MFA nas contas privilegiadas e/ou colte de senhas. Tamanho de senhas para firewall, switches, roteadores e demais equipamentos de infraestrutura Revisar política de contas com acesso a dispositivos de rede interna limitando no mínimo 12 caracteres de tamanho; Definir através de política que contas com acesso a dispositivos de rede na DMZ ou externo tenham no mínimo 16 caracteres de tamanho e colte de senha ou certificado; Revisar da conta do administrador; Revisar a alteração do nome de conta padrão de administrador, como: administrador, root, admin, etc, para um nome de conta diferente e sem correlações; Definir a troca periódica de senhas para contas de administrador/usuários locais e ou domínio.
G44	Infraestrutura	Dados	Segurança - Implementar MDM	MS	12	Média	Baixa	Baixa	R$ 200.000,00	N/A	Ausência de gerenciamento de dispositivos móveis.	Acesso indevido as aplicações ou ambiente sem autenticação, com ou e microsserviços	Exposição de informações sensíveis.	Implementar solução de MDM (Mobile Device Management) para todas empresas, oferecendo maior segurança e produtividade para gerenciamento e dispositivos móveis na organização.
G45	Segurança Cibernética	Políticas	Política de proteção contra malware	MS	1	Média	Alta	Alta	R$	N/A	A política de proteção contra malware. Incluindo software endpoint, não possui documentação indicando a possibilidade/uso configurações.	Falta de proteção/ação a partir de comportamento/ataque	N/A	Implementar política de utilização de software de proteção contra malware, incluindo malware. Revisar as configurações atualizações.
G46	Segurança Cibernética	Segurança Lógica	Ausência de trilhas de entradas e saída de dados	MS	1	Média	Alta	Alta	R$	N/A	Não há filtragem de trilha de entrada e saída.	Exposição/ataque/hacker no ambiente e/ou Phishing, BYOD e outros	N/A	Implementar um filtro no banda que proteja a navegação, downloads e evadicionto Malwares, spyware e outros códigos nocivos, além de filtro de conteúdo que impeça o acesso a sites malosos e sites controlado/entre imagens.
G47	Segurança Cibernética	Segurança Lógica	Mecanismo de bloqueio de mídias	MD	4	Média	Média	Alta	R$	N/A	Não existe mecanismo de bloqueio de dispositivo.	Impossibilidade de bloqueio de ativos conectados a rede corporativa.	N/A	Implementar um mecanismo que possibilite bloquear todo e qualquer dispositivo conectado rede, superior ao momento em que o mesmo passar a utilizar mais autorizado.

ID	Pilar	Tema	Título	Data	Duração Investir	Prontidão Investir	Prontidão Gerenciar Operação	Estimativa de Custo	Problemática	Usuários	Risco de TI	Risco de Negócio	Recomendação
D07	Segurança Cibernética	Segurança Lógica	Verificação de Perfil de Acesso	M01	0	Alta	Média	Alta	RB	Os servidores são compartilhados entre perfis, mas ainda não são totalmente personalizados. Se alguém quebrar um funcionalidade, ele pode usar permissões de demais não autorizadas.	Controle de confidencialidade da informações	Acesso indevido a informações	Verificar periodicamente as permissões ativas e revogadas para cada usuário.
D05	Segurança Cibernética	Segurança Lógica	Classificação de Informação	M02	4	Alta	Alta	R$ 80.000,00	N/A	Não há identificação nenhum processo definido para classificação da informação do BDB.	Controle de confidencialidade da informações	Acesso indevido a informações que deveriam ser confidenciais ou restritas, por não estarem classificadas devidamente.	Estabelecer, implementar e monitorar um processo para classificação da informação, a ser executado pelo(s) dono(s) da mesma.
D03	Segurança Cibernética	Segurança Lógica	Política de Backup	M1	2	Alta	Alta	Média	R$	Não há uma política de backup definida. Repetir de existência rotinas de backup com armazenamento online e offline, não há uma política definida (mínimas e responsabilidades, recuperação e como será armazenada cópia de segurança.	Realizar rotinas de backup de forma empírica comprometer sua eficácia.	N/A	Estabelecer, implementar e monitorar uma política de backup de dados.
D01	Segurança Cibernética	Segurança Lógica	Criptografia de Dados	M3	4	Média	Média	Alta	RB	A atual solução anti-malware utilizada pelo BDB não contempla a criptografia dos dados armazenados nos servidores. (Computadores, Pendrives, HDs externos, etc)	A não utilização da criptografia de dados nos arquivos, principalmente aquelles que são coletados(HDs externos, Laptops, Pendrives, etc), aumenta a exposição ao risco de roubo de informações confidenciais das organização, pois qualquer um que tenha acesso ao dispositivo será capaz à informação.	N/A	Utilizar solução anti-malware que contemple a criptografia nos unidades de armazenamento ou solução específica de criptografia de dados.
D02	Segurança Cibernética	Segurança Lógica	Licença de uso das soluções Anti-Malware e Firewall	M1	0	Média	Alta	Alta	RB	A licença de uso das soluções anti-malware do Firewall está com data próxima de expiração e ainda não foram renovadas.	Perda imediata das soluções de proteção contra malware na borda do perímetro, aumentando exponencialmente o risco de ataques cibernéticos.	Indisponibilidade dos serviços e possível perda de informação caso ocorra um ataque cibernético.	Renovar a licença das soluções anti-malware do firewall antes do seu vencimento.
D03	Segurança Cibernética	Segurança Lógica	Servidor de Arquivos	M3	2	Alta	Alta	Alta	RB	D17	Sistema servidores de arquivos instalados nas áreas sem o conhecimento da TI e fora das políticas de segurança e backup.	Perda de arquivos por não haver backup e risco de ataques via código malicioso.	N/A	Identificar, através de protocolos de compartilhamento de arquivos, máquinas instaladas como servidores de arquivos sem o conhecimento da TI e adequar aos padrões existentes.
D04	Segurança Cibernética	Segurança Física	Controles de Acesso	M2	0	Alta	Alta	Alta	RB	Inexistencia de acesso ao prédio não restritivos, possibilitando acesso e saída sem crítica sistêmica.	N/A	Perda da eficiência do controle de acesso, não registrando acesso de pessoas na local com horário de entrada e na saída, além da possibilidade de acesso de pessoas não autorizadas na ausência temporária de um funcionário no local.	Estabelecer, implementar e monitorar um processo para controle de acesso ao prédio e situação da catraca de acesso para permitir a entrada/saída da unidade apenas para pessoas autorizadas, registrando data e hora dos eventos.
D05	Segurança Cibernética	Segurança Física	Acesso à sala de CPTV	M3	0	Alta	Alta	Alta	RB	Não há controle de acesso físico na sala de CPTV.	N/A	Entrada de qualquer pessoa na sala de controle CPTV, podendo acessar ponto de informações de registro das imagens isolamento e/ou interconectamento.	Estabelecer, implementar e monitorar um processo para administração de controle de acesso a implementação de um controle de acesso físico na sala onde ficam armazenadas os equipamentos/equipções das imagens de circuito interno de TV (CPTV).
D06	Segurança Cibernética	Segurança Física	Acesso Físico nas Unidades Regionais	M3	0	Alta	Alta	Alta	RB	Não há controle de acesso físico nas unidades regionais.	Pontos de pessoas não autorizadas a acessarem dados de TI, podendo ocasionar riscos de informações e/ou ataques cibernéticos	Pessoas de pessoas não autorizadas a disponibilizar das unidades regionais, comprometendo a confidencialidade das informações de negócio.	Estabelecer, implementar e monitorar um processo para controle de acesso às unidades regionais a implementação de um controle de acesso físico, dando ênfase em salas que possuem equipamentos de TI.
D07	Segurança Cibernética	Segurança Física	Auditoria de Câmeras em salas restritas	M3	0	Alta	Alta	Alta	RB	Inexistência de TI (Datacenter de produção e Datacenter de backup) não possuem câmeras de monitoramento na parte interna.	Ações restritivas dentro das salas não poderão ser auditadas.	N/A	Estabelecer, implementar e monitorar um processo para administração da circuito interno de TV (CPTV) a instalação de câmeras de segurança, monitorar das salas de equipamentos de TI com acesso restrito.
D08	Segurança Cibernética	Segurança Física	Datacenter de backup	M1	0	Alta	Alta	Alta	RB	A sala do Datacenter de backup possui uma planta de vidro para o ser pública.	Risco de vandalismo, com facilidade de quebrar o vidro e largar substâncias que podem causar incêndios dentro da sala.	N/A	Estabelecer, implementar e monitorar um processo para administração da circuito interno de TV (CPTV) a instalação de câmeras de segurança, monitorar das salas de equipamentos de TI com acesso restrito.
D09	Segurança Cibernética	Segurança Física	Chave do Datacenter de backup	M2	0	Alta	Alta	Alta	RB	Manter de posse/ controle de aumos/chaveiros, a sala pode ser aberta por uma chave que fica armazenada na portaria e pode ser entregue para uma força de pessoas.	Acesso remoto a sala do Datacenter de backup por pessoas não autorizadas.	N/A	Estabelecer, implementar e monitorar um processo para controle de acesso ao prédio, a regulamentação do funcionamento do acesso biométrico ao datacenter de backup e inutilizar o acesso via chave.
D01	Segurança Cibernética	Segurança Organizacional	Plano de Continuidade de Negócio	M3	0	Alta	Alta	Alta	RB	Não há Plano de Continuidade de Negócio corporativo definido.	N/A	A ausência de um Plano de Continuidade de Negócio corporativo expõe a organização a risco de interrupção de seus serviços em caso de desastres ou falha crítica.	Solicitar à área de Governança Corporativa a elaboração de um Plano de Continuidade do Negócio, apontando processos críticos e tempo de resposta da TI necessário para restabelecimento deste processo em caso de sinistros.
D02	Segurança Cibernética	Segurança Organizacional	Plano de Recuperação de Desastres	M3	0	Alta	Alta	Alta	RB	Não há Plano de Recuperação de Desastres definido.	Inoperabilidade de sistemas e/ou serviços comprometidos de forma prolongada, gerando perda de dados e/ou arquivos e/ou danos ao negócio.	Interrupção prolongada de seus serviços em caso de desastres ou falha crítica.	Solicitar à área de Governança Corporativa a elaboração de um Plano de Recuperação de Desastres, apontando processos críticos e tempo de resposta da TI necessário para restabelecimento deste processo em caso de sinistros.
D03	Segurança Cibernética	Segurança Organizacional	Treinamento em TI	M1	0	Alta	Alta	Alta	RB	Nesse período não foi treinamento anuais, realizados em parceria com a RYP, que abordam temas relacionados à segurança da informação.	Pessoas mais vulneráveis a ataques através da engenharia social.	N/A	Manter parcerias da área gestão e treinar adendo do pessoas aos treinamentos relacionados à segurança da informação.
D03	Segurança Cibernética	Política	Validação da Política de SI	M2	0	Alta	Alta	RB	N/A	A Política de Segurança da Informação criada para o BDB está aguardando aprovação pela área de Governança Corporativa e ainda não foi implementada.	Não ter uma Política de SI em vigor expõe a organização a riscos de ausencia de vulnerabilidade para ataques cibernéticos, pela falta de padrões/procedimentos/comportamento de seus usuários.	N/A	Solicitar à Governança Corporativa a aprovação, divulgação e implementação da Política de Segurança da Informação, que deverá ser revisada no período inteiro definido pela SSI.
D04	Segurança Cibernética	Política	Senhas de Administração	M3	0	Alta	Alta	Alta	RB	O tópico 37 da Política de Segurança da Informação versa que a senha de administração deverá ser compartilhada com o corpo técnico e com inexistência que realizam suporte técnico.	Risco de comprometimento da confidencialidade da senha com privilégios de Administrador, podendo ocasionar em acessos indevidos à rotina da organização.	N/A	Não compartilhar senhas. Definir senhas individuais do administrador para os usuários necessários.
D05	Segurança Cibernética	Política	Penalidades Previstas	M2	0	Alta	Alta	Alta	RB	O capítulo VI da Política de Segurança da Informação, que versa sobre as penalidades previstas para o descumprimento da política, está redigido de forma genérica, não especificando quais as ações penalizadas e/ou aplicadas para cada tipo de descumprimento.	Nesse adendo de normas da Política pode modificação de quais penalidades serão aplicadas em caso de descumprimento.	N/A	Especificar detalhadamente quais as penalidades serão aplicadas para cada tipo de descumprimento.
D01	Pessoas	Estruturas Organizacionais	Alteração na estrutura organizacional	M2	0	Médio	Médio	Alta	RB	N/A	N/A	N/A	Organizar as questões na estrutura organizacional de acordo com princípios de estrutura hiatus e essencialidade detalhado no capítulo Pessoas do PDTI.