GAPs e Recomendações Processos

Pilar	GAP	Recomendação	Artefato
APO06.01 Gerenciar finanças e contabilidade	As classificações orçamentárias são realizadas de forma empírica, sem um processo documentado.	Criar e documentar um esquema de classificação orçamentária.	Esquema de Classificação de Custos de TI.
	Ausência de um processo definido e documentado para controle de entrada, saída e controle orçamentário. Não há uma definição clara sobre os papéis e responsabilidades acerca da análise e reporte da gestão financeira.	Mapear e documentar o processo de controle orçamentário, incluindo periodicidade de reportes (incluindo, se possível, uma matriz RACI).	Documento do Processo de Controle Orçamentário.
APO06.02 Priorizar a alocação de recursos	Falta de um procedimento documentado para verificação de opções entre comprar ativos/serviços ou contratação de uso de ativos/serviços.	Elaborar um processo para que se verifique entre a opção de compra ou locação do ativo, assim como desenvolver internamente um serviço ou contratá-lo externamente, a cada solicitação de compra de ativo ou serviço.	Documentação do Processo de Requisição de Compra/Serviço.
	Inexistência de um processo documentado para priorização orçamentária.	Estabelecer um processo para priorização orçamentária, assim como para estabelecer comunicações de decisões orçamentárias.	Priorização de Iniciativas Orçamentárias
APO06.03 Criar e manter orçamentos	Na criação do orçamento, não há uma documentação de quais componentes considerar. Estes são elencados de forma empírica.	Criar uma documentação contendo os componentes a considerar na elaboração do orçamento.	Documentação do Processo de Criação de Orçamento
	Não é elaborada uma documentação acerca da lógica considerada para criação do orçamento, o que dificulta a justificativa de contingências.	Criar um procedimento para elaborar um documento que registre a lógica realizada para criação do orçamento.	
APO06.05 Gerenciar custos	Não há um processo para coleta de dados relevantes para identificar desvios no orçamento quanto ao real praticado, tendências do custo de serviços e ROI do investimento, quando aplicável.	Definir, documentar e implementar um processo para coleta e verificação de dados relevantes para mensurar possíveis desvios no orçamento quanto ao real praticado, tendências do custo de serviços e mensurar ROI do investimento, quando aplicável.	Documentação do Processo de Coleta de Dados de Custo
APO09.01 Identificar os serviços de TI	Não é realizado um estudo para estimar a demanda futura e tendência para confirmar a capacidade dos serviços.	Mapear, documentar e implementar um processo para realização de um estudo que possibilite estimar a demanda futura de serviços de TI para poder confirmar a capacidade dos serviços oferecidos.	Análise de Tendência da demanda de serviços de TI.
	Não há um 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.	Mapear e documentar um processo para análise dos serviços atuais de TI e seus SLAs, verificando se está alinhado com a necessidade do negócio. Este processo deverá ser realizado em uma rotina definida.	Documentação do Processo de Análise dos Serviços e SLA. Lacunas identificadas entre a necessidade do negócio e os serviços de TI e SLAs ofertados.
APO09.02 Catálogo de serviços habilitados para TI	A publicação dos serviços e seus SLAs no catálogo de serviços é realizado esporadicamente, de forma empírica.	Criar uma recorrência para atualização do catálogo de serviços e SLAs, documentada em forma de processo.	Documentação do Processo de Atualização do Catálogo de Serviços

Pilar	GAP	Recomendação	Artefato
APO09.03 Definir e preparar acordos de serviço	A definição do SLA necessário para o serviço realizado e/ou contratado é realizada de forma empírica, sem um processo definido e documentado.	Mapear e documentar um processo para definição dos SLAs necessários para os serviços a serem realizados e/ou contratados.	Documentação do Processo de definição do Nível de Acordo de Serviço.
APO12.01 Coletar Dados	Não existe um método documentado para coleta, classificação e análise de risco.	Estabelecer, documentar e manter um método para coleta, classificação e análise de dados relacionados a riscos de TI.	Documento do Processo de Gestão de Riscos
		Registrar dados relevantes e significativos relacionados a riscos de TI no ambiente operacional interno e externo da empresa.	Documento do Processo de Gestão de Riscos
APO12.03 Manter um perfil de risco	Não há documentação dos riscos, segregados por categoria, linha de negócio e área funcional.	Agregar e documentar cenários de risco atuais por categoria, linha de negócio e área funcional	Risco documentado. Cenários por linha de negócios e função.
	Não há uma documentação acerca de quais serviços de TI e infraestrutura são críticos para operação do negócio e riscos relacionados.	Determinar e concordar sobre quais serviços de TI e recursos de infraestrutura de TI são essenciais para sustentar a operação de negócio e processos. Analisar as dependências e identificar os elos fracos. Documentar em um catálogo de serviços críticos.	Serviços críticos de TI para sustentação do negócio.
APO12.05 Definir um portfólio de ações de gerenciamento de riscos.	Não há documentação sobre as atividades de controle de riscos.	Manter uma documentação das atividades de controle que estão em vigor para mitigar o risco e que permitam que o risco seja assumido de acordo com apetite do risco e tolerância. Classifique as atividades de controle e mapeie-as para cenários de risco de TI específicos.	Documentação das atividades de controle do risco.
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Não há um processo de gestão de mudança definido e implementado na CPRM. Todas as mudanças são realizadas de forma empírica e pontual.	Aprovar formalmente as requisições de mudança pelos proprietários do processo de negócio afetado. Para as mudanças priorizadas como baixo risco deverão ser pré-aprovadas como mudança padrão.	Documento de Requisição de Mudança.
		Criar uma categorização padrão para as mudanças. Ex: Infraestrutura, Sistema Operacional, Sistemas Aplicativos, etc.	Lista de Categorias de Mudança.
		Definir uma formalização padrão para o requerimento de mudança, incluindo o solicitante e o aprovador.	Documento de Requisição de Mudança.
		Mapear, definir e implementar um processo para gestão de mudança. Certificar que toda e qualquer mudança seja realizada através do processo de gestão de mudança.	Documento do Processo de Gestão de Mudança.
		Planejar e comunicar a execução da mudança.	Comunicado da Mudança.
		Priorizar toda e qualquer mudança, identificando também aquelas que são emergenciais.	N/A
		Avaliar, declarar e aprovar preliminarmente as mudanças emergenciais através de um documento padronizado, registrando-as.	Registro de Mudança Emergencial.

Pilar	GAP	Recomendação	Artefato
BAI06.02 Gerenciar mudanças de emergência	Mudanças só são classificadas como emergenciais quando é solicitado pela liderança.	Definir o que constitui uma mudança emergencial. Avaliar quais riscos estão sendo mitigados através da mudança, e qual a probabilidade dos mesmos ocorrerem caso a mudança não seja realizada de forma imediata.	Definição de Mudança Emergencial.
BAI06.04 Fechar e documentar as alterações	Não há registro histórico das mudanças realizadas.	Criar um registro de toda e qualquer mudança realizada, contendo informações do que foi realizado, quais configurações foram alteradase, etc. Manter este registro por um tempo determinado.	Documentação da Mudança.
		Definir qual o tempo necessário para manter o histórico da mudança.	N/A
BAI09.01 Identificar e registar o ativo corrente	Não existe um processo documentado para gestão de Ativos. O inventário não é completo e não é realizado de forma automática ou semi-automática.	Criar, documentar e implementar um processo para gestão dos ativos.	Documento do Processo de Gestão de Ativos
		Inventariar todos os ativos de Hardware e Software através de ferramentas autônomas ou semi-autônomas.	Inventário de Ativos
		Verificar e documentar periodicamente os requisitos legais, regulatórios ou contratuais para a aquisição/uso do ativo.	Resultado de Adequação de Ativos
		Verificar e documentar periodicamente se os ativos estão adequados ao propósito e em boas condições de uso.	
BAI09.02 Gerenciar ativos críticos	A identificação dos ativos críticos é realizada apenas de forma empírica, sem documentação.	Criar, documentar e implementar um processo para identificação e classificação dos ativos críticos.	Documento do Processo de Gestão de Ativos
	Não há um procedimento documentado para comunicação aos usuários acerca de inatividade ou degradação de desempenho dos ativos em caso de manutenção preventiva.	Criar, documentar e implementar um processo formal para comunicação aos usuários acerca de manutenções preventivas e seus impactos nos serviços.	Comunicação de manutenção planejada e tempo de inatividade.
	O risco de falha ou a necessidade de substituição de um ativo crítico não é analisado e documentado.	Analisar periodicamente o risco e impacto caso haja falha em um ativo crítico, documentando em um Mapa de Riscos dos Ativos Críticos.	Mapa de Risco de Ativos Críticos.
BAI09.03 Gerir o ciclo de vida dos ativos	O processo de compra/aquisição de um ativo não é documentado.	Documentar o processo de compra/aquisição de ativos.	Documento do Processo de Aquisição de Ativos
		Documentar o processo de teste, validação e registro do ativo após a aquisição.	
BAI09.05 Gerir licenças	A gestão de licenças é realizada de forma descentralizada, ou seja, a licença de um software pode ser adquirida e controlada por outros departamentos.	Criar e implementar uma política para centralização da gestão de licenças de software no departamento de TI, a partir do processo de Gestão de Ativos.	Política de Gestão de Licenças de Software.
BAI10.02 Estabelecer e manter um repositório de configuração e linha de base	Não há um processo definido e documentado para gestão da configuração.	Criar, documentar e implementar um processo para gestão da configuração.	Documento do Processo de Gestão da Configuração.
	Só existe o repositório de itens de configuração para equipamentos de rede (Switch, Firewall)	Identificar e registrar os itens de configuração de todos os ativos e suas respectivas linhas base.	Repositório de Configuração e Linhas Base.

Pilar	GAP	Recomendação	Artefato
BAI10.03 Manter e controlar itens de configuração	Não há registro das modificações realizadas nos itens de configuração.	Identificar regularmente todas as alterações nos Itens de Configuração e atualizar o repositório.	Repositório de Configuração e Linhas Base atualizado.
BAI10.04 Produzir relatórios de status e configuração		Identificar a mudança de status dos Itens de Configuração e atualizar a Linha Base.	
BAI11.01 Manter uma abordagem padrão para gerenciamento de projetos.	Não existe programa de treinamento para gerenciamento de projetos.	Fornecer treinamento adequado em gerenciamento de projetos e considerar a certificação para gerentes de projeto.	Programa de Treinamento em Gestão de Projetos.
BAI11.02 Iniciar e implementar um projeto.	Quando um projeto é iniciado, não é assegurado que as partes interessadas e/ou patrocinadores (negócio) concordem e aceitem os requisitos do projeto, incluindo a definição dos critérios de sucesso (aceitação) do projeto e indicadores-chave de desempenho (KPIs).	Assegurar que as partes interessadas e patrocinadores concordem e aceitem os requisitos do projeto, definição do critério de aceitação e indicadores chave de desempenho.	Documentos de Iniciação do Projeto.
BAI11.06 Gerenciar o risco do projeto.	Não há um processo de gestão de riscos nos projetos.	Atribuir a pessoa devidamente qualificada a responsabilidade pela execução do processo de gerenciamento de riscos do projeto e garantir que isso seja incorporado às práticas de desenvolvimento da solução. Considere alocar essa função para uma equipe independente, especialmente se for necessário um ponto de vista objetivo ou se um projeto for considerado crítico.	Processo de gestão de riscos.
DSS01.01 Realizar procedimentos operacionais	Não há documentação acerca dos procedimentos operacionais da TI.	Criar uma documentação dos procedimentos operacionais da TI.	Procedimentos Operacionais.
	Não há planejamento das atividades operacionais.	Elaborar um planejamento de todas as atividades operacionais e sua execução.	Planejamento de Atividades
DSS01.03 Monitoriar a infraestrutura de TI	Não há registros de eventos ocorridos na infraestrutura de TI.	Registrar todos os eventos ocorridos na infraestrutura de TI, considerando os riscos associados ao evento.	Registro de Eventos
DSS01.04 Gerenciar o ambiente	Não há uma política de utilização dos equipamentos ou ambientes de TI com objetivo de prevenir danos aos equipamentos e/ou instalações.	Criar uma política com o objetivo de prevenir danos aos equipamentos e ambientes de TI, por exemplo: proibir o armazenamento de artigos de papelaria ou quaisquer outros objetos que representem risco de incêndio nas salas de informática, proibir o consumo de bebidas durante a utilização de equipamentos, etc.	Política de Utilização de Equipamentos e Ambientes de TI.
DSS01.05 Gerenciar instalações	Inexistência de um padrão do uso de cabeamento de rede lógica de dados e telefonia, sendo a rede não estruturada.	Estruturar a rede lógica de dados e telefonia conforme preconiza a NBR 14565.	Rede Lógica de Dados e Telefonia estruturada.
	Não há redundância para os links de comunicação e fontes de energia.	Implementar uma redundância de links de comunicação e fontes de energia.	Definição das redundâncias necessárias para os serviços críticos.
	Não há um processo que defina uma periodicidade nos testes das fontes de energia (nobreaks e afins).	Definir e documentar um processo de checagem regular das fontes de energia.	Procedimentos Operacionais.
	O capital humano da companhia não recebe treinamentos contra incêndios, evacuação e resgate.	Definir e implementar, em conjunto com a CIPA, uma periodicidade para treinamentos contra incêndios e evacuação.	Treinamentos de Prevenção de Incêndio.

Pilar	GAP	Recomendação	Artefato
DSS02.02 Registrar, classificar e priorizar as requisições e incidentes	Não existe um processo definido para atendimento as requisições de serviços e incidentes.	Criar, definir e implementar um processo de atendimento as requisições de serviços e incidentes, com classificação do serviço/incidente.	Documento do Processo de Atendimento as Requisições de Serviço e incidentes.
DSS02.04 Investigar, diagnosticar e alocar incidentes	As requisições de serviço não são registradas em uma base de conhecimento para que soluções já implementadas possam ser consultadas.	Implementar uma base de conhecimento, registrando as requisições de serviços/incidentes para otimizar a solução de problemas/incidentes já conhecidos.	Base de Conhecimento de Requisições de Serviço/incidentes.
DSS02.05 Resolver e recuperar os incidentes	Quando é dada uma solução temporária a uma requisição, esta informação não é registrada.	Registrar a informação de soluções temporárias às requisições de serviço/incidente.	Registro da informação de soluções temporárias.
DSS02.06 Encerrar requisições de serviços e incidentes	Após a resolução da requisição, o usuário não é consultado para saber se a solução foi satisfatória.	Definir e implementar um procedimento para que, no fechamento da requisição de serviço/incidente, o usuário solicitante seja contactado para informar se a solução foi satisfatória.	Documento do Processo de Atendimento as Requisições de Serviço e incidentes.
DSS02.07 Acompanhar o status e elaborar relatórios	Não há um processo definido para acompanhamento das requisições de serviço/incidentes.	Monitorar toda e qualquer requisição de serviço/incidente aberto, acompanhando suas variações e solicitar procedimentos para avançar para resolução.	
DSS05.01 Proteger contra Malware	A política de proteção contra Malware, incluindo o software endpoint, não possui documentação indicando os procedimentos e configurações.	Documentar a política de utilização de softwares de proteção contra Malware, incluindo sua versão, forma de configuração e atualização.	Política de Prevenção contra Malware.
	Não há filtragem de tráfego de internet e e-mails.	Implementar um filtro de conteúdo na borda que proteja contra links maliciosos e sites conhecidamente inseguros.	Implementação de Filtro de Conteúdo/anti-spam.
		Implementar um filtro na borda que proteja a navegação, downloads e e-mails contra Malwares, Spywares, Phishing e demais códigos maliciosos.	
DSS05.02 Gerenciar a segurança da rede e da conectividade	Apenas a rede Wi-Fi possui proteção contra acesso de dispositivos não autorizados. Esta proteção baseia-se em autenticação. Para a rede cabeada, não possui nenhuma proteção contra acesso não autorizado.	Implementar uma proteção contra acesso de dispositivos não autorizados tanto para rede Wi-fi quanto para a rede cabeada, como por exemplo: filtragem por MAC-Address. Certifique-se que esta implementação seja documentada em uma política.	Implementação de uma política contra acesso de dispositivos não autorizados na rede.
DSS05.02 Gerenciar a segurança da rede e da conectividade	Não há documentação para configuração segura dos equipamentos de rede.	Documentar todas as configurações de segurança dos dispositivos de rede.	Documento de configuração de dispositivos de rede.
DSS05.03 Gerenciar a segurança dos dispositivos (Notebook, desktop, dispositivos móveis, entre outros)	Não existe documentação que registre as configurações de instalação de Softwares Operacionais de forma segura.	Criar uma documentação que registre todas as configurações e procedimentos para instalar um Software Operacional, tanto para servidores quanto para desktops, de forma segura.	Documentação de Instalação e Configuração de Sistemas Operacionais.
	Não existe mecanismo de bloqueio de dispositivo.	Implementar um mecanismo que possibilite bloquear todo e qualquer dispositivo conectado à rede, a partir do momento em que o mesmo passe a não ser mais autorizado.	Mecanismo de Bloqueio de Hosts.

Pilar	GAP	Recomendação	Artefato
	Não há criptografia dos dados armazenados nas unidades de disco.	Implementar criptografia em todas as unidades de disco físicas. (tanto HDs quanto dispositivos móveis (Pendrive, HD Externo, etc.)	Implementação de Criptografia de disco
	Não há política adequada de descarte de equipamentos	Implementar uma política para descarte adequado dos equipamentos que chegaram ao fim de sua vida útil.	Política de Descarte de Equipamentos.
DSS05.04 Gerenciar os perfis de usuário e o registro de acesso	Os acessos são concedidos baseados em perfis, mas estes não são confirmados periodicamente. Ou seja, quando um funcionário entra, ele possui uma permissão e as demais são adicionadas.	Administrar as mudanças de perfil (criação, modificação e exclusão) de forma ágil, apenas com base em autorizações formais dadas pelo dono da informação.	Política de Perfil de Acesso
		Identificar de forma única todas as atividades de processamento de informação por cargos funcionais. Coordenar com as áreas de negócio para assegurar que todas as funções são sistematicamente definidas.	
		Segregar e reduzir ao mínimo o número necessário de acessos e gerenciar ativamente as contas de usuários permitidos.	
		Verificar periodicamente as permissões ativas e necessárias para cada usuário.	
DSS05.05 Gerenciar o acesso físico aos ativos de TI	Não há registros de visitantes em locais de TI.	Registrar e monitorar todos os locais de TI. Registrar todos os visitantes, incluindo fornecedores.	Política de registro de visitantes.
	Não há uma obrigatoriedade dos funcionários de TI andarem sempre com o crachá de identificação visível.	Implementar um código de conduta para que todos os funcionários frequentem os locais de TI com o crachá de identificação sempre visível.	Código de Conduta.
	Os locais sensíveis de TI não são protegidos por barreiras de segurança física.	Assegurar que os perfis de acesso se mantenham atualizados. Basear o acesso aos locais de TI (salas de servidores, edifícios) na função e responsabilidades do trabalho.	Controle Físico aos locais sensíveis de TI.
		Implementar em todos os locais sensíveis de TI barreiras físicas de segurança e monitoramento, tais como: Controle de acesso biométrico e Câmeras de Monitoramento e Segurança.	
DSS05.06 Gerenciar documentos sensíveis e dispositivos de saída.	A informação não é classificada.	Criar uma política para classificação da informação, conforme a necessidade do negócio.	Política de Classificação e proteção da informação.
		Estabelecer procedimentos para controlar o recebimento, utilização, eliminação e descarte de documentos sensíveis.	
		Estabelecer proteções físicas apropriadas sobre documentos sensíveis.	
		Estabelecer um inventário de documentos e informações sensíveis.	
		Restringir o acesso à informação baseado nos perfis de classificação.	

Pilar	GAP	Recomendação	Artefato
DSS05.07 Gerenciar vulnerabilidades e monitorar a infraestrutura para eventos relacionados a segurança.	Os registros de eventos e potencial incidentes não são revistos periodicamente.	Definir e implementar um processo para revisão contínua dos eventos e potenciais incidentes.	Documento do Processo de revisão de eventos e potenciais incidentes.
	Os Tickets de incidentes de segurança não são abertos em tempo hábil, e não são registrados para histórico.	Assegurar que os tickets de incidentes relacionados com a segurança sejam criados em tempo hábil quando a supervisão identificar potenciais incidentes.	Atendimento e registro de tickets relacionados à segurança.
		Registar os eventos relacionados com a segurança e armazenar os registos. Definir um período apropriado para este armazenamento.	