PROJETO BASE ADEQUAÇÃO LGPD – YUP CHAT

PREPARAÇÃO				
Seq	Ref.Legal	Assunto	Macro Atividade - Projeto LGPD	Descrição
1.1.1	DPMS	Abertura do Projeto	Reunião abertura do projeto	Reunião para apresentação do projeto, definição e aprovação do cronograma (macro) de atividades. Será definido início e fim do projeto, bem como a distribuição de fases.
1.1.2	DPMS	Alta Gestão	Gerenciar compromisso da Alta Gestão	Assinar termo de compromisso para abertura do projeto de execução.
1.1.3	ISO27701 / LGPD	Organização da Segurança da Informação	Definir o Encarregado (DPO) ou área Encarregada para responder	A organização deverá designar uma pessoa ou uma área com o preparo necessário para responder formalmente diante do órgão regulador a respeito de qualquer incidente envolvendo Dados Pessoais. Recomenda-se que o encarregado reporte-se diretamente ao nível gerencial apropriado a fim de assegurar uma efetiva gestão de riscos de privacidade
1.1.5	DPMS	Comitê	Gerenciar partes interessadas (Comitês de Negócio e Terceiros)	Constituir comitê que conduzirá o projeto na instituição.
1.1.6	DPMS	Papeis e Responsabilidades	Estabelecer Papeis e Responsabilidades	Definir papéis e responsabilidades dos membros do comitê
1.2.1	ISO27701	Organização da Segurança da Informação	Definir um programa de conscientização em Segurança da Informação	Deve ser definido um programa de conscientização interna em Segurança da Informação, que leve em conta os aspectos de Proteção de Dados Pessoais
1.2.2	DPMS	Oficina Inicial	Oficinas de Conscientização	Encontro com funcionários, de todas as áreas, para apresentação dos conceitos de privacidade de dados pessoais. Recomenda-se a exposição de informações de fácil assimilação. O objetivo desse encontro é iniciar o processo de mudança de cultura. É importante estimular a participação ativa dos presentes, induzindo perguntas que provoquem a reflexão sobre o tema.
1.3.1	DPMS	Áreas de Processamento	Definição de áreas de processamento de dados	Registrar/identificar as áreas, setores/departamentos que processam dados pessoais na instituição.
1.3.2	DPMS	Titulares	Identificação de Titulares	Registrar/identificar as categorias de "titulares" que confiam dados à instituição. Classificar titulares favorece a tomada de decisão. Clientes, fornecedores ou funcionários, são alguns exemplos. É importante que, ao classificar, defina-se de forma clara a identificação/descrição do titular.

1.3.3	DPMS	Atividades	Identificação de Atividades	Registrar as atividades executadas pela instituição que processam dados pessoais. Essa identificação deverá indicar quem, quando e como a atividade é executada, as trocas de informações, prevendo origem e determinando destino, e ainda o tempo de processamento e a forma de descarte da informação. NOTA: Informar se a atividade processa dado de criança.

1.3.4	DPMS	Leis e Regulamentos	Reunir Leis e Regulamentos	Após identificar as atividades de tratamento de dados pessoais, com auxílio do departamento jurídico e/ou departamento de qualidade, registre todas as leis, resoluções e portarias que autorizam ou regulam a atividade de processamento de dados.
1.3.5	DPMS	Invetário de Dados	Estabelecer Fluxo e Inventário de Dados	Definia o fluxo dos dados em sua instituição, se valendo do método BPM, organizando entradas, armazenamento, consulta e processamento como transformação, extração e eliminação.
1.3.6	DPMS	Fluxo de Dados	Macro-Fluxo de Dados por área	Registrar entrada e saída do dado, indicando sua origem e seu destino, interno ou externo ao controlador. Se externo, apontar destinação como "Operador" ou "Novo Controlador".
1.3.7	LGPD	Inventariar/classificar ativos e sistemas	Para manter um maior controle sobre as configurações de segurança deve-se determinar e identificar os ativos de informação da Organização e classificar.	Inventariar e classificar ativos de forma que estes possam ser mantidos e atualizados conforme necessidade, contemplando: - Lista de ativos da Organização - Responsáveis e custodiantes de cada ativo inventariado- Classificação dos ativos
1.3.8	ISO27701	Organização da Segurança da Informação	Classificação da Informação	Todas as informações produzidas na organização, inclusive àquelas que incluam dados pessoais devem ser devidamente classificadas e rotuladas

1.3.9	LGPD	Classificação da informação	A informação deve ser classificada com base nos requisitos legais, valor, importância e sensibilidade em caso de divulgação ou modificação não autorizada.	Recomenda-se que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. Promover conscientização sobre a área de segurança da informação e promover acordos entre as áreas da Organização na aplicação e classificação da informação; Um exemplo de critérios para classificação da informação pode ser: - Pública ou Externa: Pode ser utilizado por todos sem restrição. Geralmente possui uma formatação, linguagem e conteúdo comercial ou promocional voltado mais para os clientes. - Interna: Acesso à os funcionários, colaboradores, acionistas. Normas, procedimentos, formulários que a Organização não possui interesse em divulgar em que o acesso por parte de pessoas externas pode causar algum tipo de dano à imagem, porém não tão impactante quanto às informações restrito/confidenciais. - Restrita/Confidencial: Acesso controlado em que apenas pessoas autorizadas devem ter acesso. Contratos, plano estratégico, informações fiscais, informações de clientes, entre outras. O acesso indevido pode causar riscos de imagem, financeiro, operacional, criminal, cíveis, entre outros riscos.

1.3.10	LGPD	Período de retenção de registos	Definir práticas para retenção de registos (Nota: a conservação dos dados deve ser efetuada apenas durante o período em que os mesmos são necessários relativamente à finalidade)	Definir práticas para retenção de registos (Nota: a conservação dos dados deve ser efetuada apenas durante o período em que os mesmos são necessários relativamente à finalidade)

1.3.11	LGPD	Inventário dados (RAT)	Um inventário dos dados pessoais deve ser realizado	Inventário de dados pessoais, com o objetivo de identificar questões como: Finalidade Descrição do tratamento Departamento/área responsável pela recolha/tratamento Base legal Proveniência/meios de obtenção dos dados pessoais Categorias de dados pessoais Modo de conservação dos dados pessoais (sistemas informáticos e/ou arquivo em papel) Decisões automatizadas Subcontratantes com acesso aos dados Grupo dentro da organização que possuem acesso aos dados pessoais Terceiros localizados dentro dos limites definidos com acesso aos dados Terceiros localizados fora dos limites definidos com acesso aos dados Prazo de conservação dos dados Medidas técnicas e organizativas adotadas para proteger os dados
1.3.12	DPMS	Dicionário de Dados - Software	Identificar e documentar estrutura de armazenamento de dados	Solicitar aos fornecedores de software o envio do dicionário de dados. NOTA: Carta aos fornecedores.
1.3.13	LGPD	Definir Identidades (Funções)	Para se tornar parte da “comunidade” organizacional, identidades devem ser registradas e criado o seu respectivo perfil. Em essência, o registro torna uma identidade “conhecida” para a organização como uma pessoa, objeto ou entidade que pode exigir acesso aos ativos da organização e que pode ter que ser autenticado e autorizado a usar privilégios de acesso.	Criar um processo de criação e organização de identidades de forma a definir os limites de "comunidade" de pessoas, objetos e entidades, de acordo com as seguintes diretrizes, por exemplo: - Uma fonte de informação sobre identidades e seus acessos que seja única e consistente;- Uma baseline para que mudanças à identidades possam ser monitoradas, identificadas e gerenciadas; - O escopo para o monitoramento do controle de acesso e análise para identificar identidades que não são necessárias bem como revisão e alinhamento dos privilégios de acesso de acordo com o alinhamento com o negócio; - A agregação de identidades de pessoas, objetos ou entidades onde são necessárias múltiplas identidades.

1.4.1	DPMS	Estrutura de Governança	Estabelecer a Estrutura de Governança	Definir a organização de tomada de decisão para uso dos dados e gestão de pessoas e processos na instituição. A apresentação nessa fase é resumida, utilize modelo organograma.
1.4.2	DPMS	Auditoria Preliminar	Auditorias Iniciais	Avalie as atividades realizadas pelos departamentos, as funções envolvidas e determine riscos, e ações de redução ou eliminação da vulnerabilidade.

1.4.3	DPMS	Análise de Privacidade	Conduzir a análise da Privacidade	Execute avaliação de cultura de privacidade. Seu resultado deve ser avaliado em relação às atividades de processamento de dados pessoais, desdobrando em ações de melhoria em cada área, equipe e pessoa da instituição.
1.4.4	LGPD	Auditoria interna com foco em Segurança e Proteção de Dados	Auditorias internas devem ser realizadas com o objetivo de validar: - Cumprimento da conformidade da lei- Impacto da privacidade e princípios de privacy by design nos projetos - Verificação dos requisitos de Proteção de Dados	Auditorias internas devem ser realizadas com o objetivo de validar: - Cumprimento da conformidade da lei - Impacto da privacidade e princípios de privacy by design nos projetos - Verificação dos requisitos de Proteção de Dados
1.4.5	ISO27701	Gestão de Riscos	Definir planos de ação para redução e tratamentos dos riscos	Definir as medidas compensatórias que contemplem a redução e/ou tratamento dos riscos
1.4.6	DPMS	Análise de Cenário de Segurança	Conduzir a análise da Segurança	Execute avaliação de segurança. Seu resultado deve ser avaliado em relação às atividades de processamento de dados pessoais, desdobrando em ações de melhoria em cada área, equipe e pessoa da instituição.

1.4.7	LGPD	Analisar Vulnerabilidades	Através da análise de vulnerabilidade, a organização procura entender a ameaça potencial que pode explorar a vulnerabilidade identificada. A estrutura da vulnerabilidade, o que ela pode fazer, como é explorada, os efeitos potenciais. Deve ser cuidadosamente considerada no contexto dos ativos e serviços potencialmente afetados. Um processo para analisar vulnerabilidades deve ser definido, através de soluções automatizadas e análises manuais. As informações obtidas pela análise das vulnerabilidades compõem a gestão de risco da Organização e auxilia na Segurança e Proteção de Dados.	Definir um procedimento de análise de vulnerabilidades que faça com que a Organização entenda as ameaças que elas representam, ao entender suas estruturas e formas de exploração, bem como os efeitos que elas causarão no ambiente tecnológico e na imagem da Organização. A análise de vulnerabilidades deve incluir atividades como: - Entender relação entre ameaças e exposição por conta das vulnerabilidades identificadas;- Revisar documentações para identificar a existência da mesma vulnerabilidade no passado, bem como quais ações foram tomadas para a mitigação; - Identificar e entender as causas-raiz das vulnerabilidades; - Priorizar, categorizar as vulnerabilidades e definir responsável para que ações apropriadas sejam tomadas para reduzir ou eliminar o impacto; - Comunicar com a área de gestão de riscos quando há necessidade de implantar uma estratégia diferenciada para mitigação.
1.4.8	LGPD	Identificar Vulnerabilidades	A identificação e análise de vulnerabilidades são elementos essenciais da Gestão de Vulnerabilidades antes que elas sejam exploradas. As informações aprendidas através da identificação de vulnerabilidades são contextualizadas usando informações de risco.	Definir um processo de identificação de vulnerabilidades no ambiente da Organização, que pode incluir diferentes técnicas, como por exemplo: - Avaliações internas por vulnerabilidades utilizando ferramentas automatizadas e análises manuais; - Realização de avaliações externas de vulnerabilidades utilizando ferramentas automatizadas e análises manuais; - A revisão dos resultados de auditorias internas e externas; - A revisão periódica dos catálogos de vulnerabilidades do mercado (ex: CERT, MITRE, etc); - A subscrição em serviços de notificação por vulnerabilidades dos fabricantes; - A subscrição em mailings que divulgam novas vulnerabilidades; - A revisão de relatórios de vulnerabilidades e grupos de notícias feitos pela indústria de Cyber Segurança.
1.4.9	DPMS	Teste de Segurança	Implementar e operar programas automatizados de segurança da informação*	Contratar empresa especializada em análise de vulnerabilidades para execução de testes controlados de invasão no serviço de tecnologia. O relatório deverá orientar a construção de novas tarefas e ações.

1.4.10	LGPD	Testes de invasão	Realizar Teste de Invasão no escopo	Recomenda-se que seja realizado um teste de invasão, para garantir que dados pessoais sejam comprometidos
1.4.11	ISO27701	Gestão de Identidades e Acessos	Provisionamento de acesso para usuários	A organização deve possuir processos ou procedimentos para provisionar o acesso para usuários aos recursos que processem Dados Pessoais (por exemplo, todo acesso a recursos que processem Dados Pessoais deve ser aprovado pelo gestor da área; não reemitir logins e senhas, etc.)
1.4.12	ISO27701	Gestão de Riscos	Conduzir avaliação dos riscos em Segurança da Informação e Privacidade de Dados	Conduzir, dentro do período fixo ou condição válida, avaliações de riscos relacionados à Segurança da Informação e Privacidade de Dados. NOTA: Contrate um pentest.
1.4.13	ISO27701	Gestão de Identidades e Acessos	Análise Crítica dos Acessos	A organização deve adotar, de forma periódica, a revisão dos acessos a todos os seus recursos tecnológicos e a todos os seus recursos que possam processar Dados Pessoais
1.4.14	ISO27701	Gestão de Terceiros	Identificar Segurança da Informação nos Fornecedores	A organização deve validar e verificar periodicamente se seus fornecedores atendem a requisitos mínimos de Segurança da Informação
1.4.15	LGPD	Auditorias externas com foco em Segurança e Proteção de Dados	Auditorias/assessments por entidades externas devem ser realizadas	Auditorias/assessments por entidades externas devem ser realizadas, com o objetivo de validar a conformidade com a lei
1.4.16	DPMS	Análise de Impacto Preliminar	Realizar a Análise de Impacto	Identifique e relacione as atividades que possuem troca de informações com terceiro, e já execute a avaliação de impacto do processamento de dados.
1.5.1	LGPD	Atribuir papéis às Identidades (Segregação de Funções)	Os papéis definem uma função em particular que é associada a uma identidade. Os usuários, particularmente, podem ter mais de um papel na Organização, em conjunto com suas tarefas de trabalho, podendo ser, por exemplo, administradores de um sistema de pagamento enquanto tem acesso autorizado à área de call center. Uma identidade tipicamente pode ter mais de um papel atrelado, baseado nas tarefas de trabalho e nos comportamentos da identidade.	Definir e associar as identidades aos usuários, objetos e entidades da Organização, bem como provém a aprovação para a criação e associação de um papel a uma identidade. Papéis criados podem ser idênticos a um papel pré-estabelecido em uma aplicação ou outra tecnologia (como um sistema de controle de acesso físico), mas também podem ser mais descritivos com relação à posição e responsabilidades de trabalho da identidade relacionada. Convém que os papéis definidos sejam autorizados e justificados pelos owners das identidades.

1.5.2	DPMS	Treinamento Privacidade	Elaborar Programa de Privacidade (Programa de Treinamentos)	A partir da avaliação de privacidade, e seus resultados, defina programa de treinamento reforçando pontos fortes e tratando pontos frágeis.

1.5.3	LGPD	Sensibilização, educação e treinamento em Segurança da Informação e Proteção de Dados	Todos os colaboradores da organização e, quando relevante, os prestadores de serviço devem ser destinatários de ações de sensibilização, educação e formação, no contexto do tema da Proteção de Dados e Segurança da Informação devem ser realizados	Recomenda-se que um programa de sensibilização em Segurança da Informação e Proteção de Dados seja definido baseado em: a) Tornar os funcionários e, onde relevante, partes externas, conscientes das suas responsabilidades para a segurança da informação e os meios pelos quais essas responsabilidades são realizadas. b) Alinhado com as políticas e procedimentos relevantes de segurança da informação da organização, levando em consideração as informações da organização a serem protegidas e os controles a serem implementados para proteger a informação. c) Atividades de sensibilização, tais como, campanhas (por exemplo, dia da segurança da informação) e a publicação de boletins ou folhetos. d) Atividades do programa de sensibilização sejam planejadas ao longo do tempo, preferencialmente de forma regular, de tal modo que as atividades sejam repetidas e contemplem novos funcionários e partes externas. e) Atualizado regularmente. Treinamento e educação em Segurança da Informação e Proteção de Dados também contemple aspectos gerais, como: a) declaração do comprometimento da direção com a segurança da informação em toda a organização; b) a necessidade de tornar conhecido e estar em conformidade com as obrigações e regras de segurança da informação aplicáveis, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos. c) responsabilidade pessoal por seus próprios atos e omissões, e compromissos gerais para manter seguro ou para proteger a informação que pertença a organização e partes externas. d) procedimentos de segurança da informação básicos (tais como, notificação de incidente de segurança da informação) e controles básicos (tais como, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa). e) pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança da informação, incluindo materiais de treinamento e educação em segurança da informação. f) abordando o tema da Proteção de Dados. g) direcionado a colaboradores com responsabilidades ao nível Proteção de Dados (incluindo áreas operacionais ex: call center, segurança, marketing, etc.). Exemplos de atividades do programa de sensibilização: a) Auditoria de senhas, com o objetivo de demonstrar, de forma prática, o uso de senhas fracas

1.5.4	ISO27701	Organização da Segurança da Informação	Conscientizar, treinar e educar em Segurança da Informação	dentro da Organização. Devem ser aplicados, de forma regular, treinamentos e ações de conscientização aos funcionários, sempre levando em consideração a Segurança da Informação e a Proteção de Dados Pessoais
1.6.1	DPMS	Plano de Ação	Revisar projeto base	Revisar projeto base, incluindo ações referentes aos diagnósticos e levantamentos observados (aquisição de software, hardware, revisão de contratos, etc)
1.6.2	DPMS	Orçamento	Compor Orçamento	Desenvolver orçamento do projeto final para autorização.

ORGANIZAÇÃO				
Seq	Ref.Legal	Assunto	Macro Atividade - Projeto LGPD	Descrição
2.1.1	DPMS	Evolvimento Alta Gestão	Gerenciar envolvimento da Alta Gestão	Definir ações de participação ativa da alta gestão nos projetos e atividades do projeto, como treinamentoe, eventos etc.
2.1.2	DPMS	Comunicação	Gerenciar comunicações regulares	Definir calendário de publicações referentes ao projeto e a importância da participação de todos.
2.2.1	DPMS	Classificação de Dados	Sistema de Classificação de Dados (Níveis mínimos, controles e interesses dos titulares)	Definir como os dados serão classificados na instituição, para anonimização, exclusão ou minimização.
2.2.2	DPMS	Requisitos Jurídicos do Negócio	Gerenciar DP&P (Leis e Requisitos de Negócio) e Governança	A partir da reunião de leis e regulamentos, vinculadas as cada atividade, avaliar se o tratamento com o dado pessoal observa a legislação e promover adaptações e correções conforme e legislação. Essas informações de tratamento e adaptações devem compor documentação própria, de registro, vinculadas à atividade para consulta futura e dapatações quando a legislação mudar.

2.2.3	LGPD	Identificar e priorizar serviços críticos para o Negócio	Os serviços críticos da organização devem ser identificados como uma linha de base para identificar a extensão e os tipos de Planos de Continuidade de Negócio a serem desenvolvidos e implementados. A falha em identificar e priorizar esses serviços pode resultar no desenvolvimento de planos de continuidade de serviço desnecessários ou ineficazes e aumenta os custos de gerenciamento de resiliência operacional para a organização.	Identificar e priorizar os serviços que garantem a continuidade do negócio Identificar e analisar as dependências internas e externas Mapear registros e banco de dados críticos
2.2.4	DPMS	Gestão de Terceiros	Avaliação de Risco – Áreas de Negócio e Plano de Gerenciamento de Terceiros	Avaliar as atividades com troca de dados com terceiro. Desdobrar revisão de contratos e termos de confidencialidade.

2.2.5	LGPD	Estabelecer critérios de Riscos e escopo(AIPD/RIPD)	A definição da tolerância (limite) de risco traça uma linha sob os riscos identificados e define quais os riscos devem ser tratados e quais o negócio da Organização considera aceitáveis. A definição destes limites ajuda na priorização do tratamento dos riscos.	Definir a tolerância de risco operacional aceitados pelo negócio da Organização; Definir os requisitos necessários para a realização do processo de Gestão de Riscos de Cyber Segurança; Categorizar os riscos incluindo as áreas de impacto de cada tipo de risco; Criar critérios para um melhor entendimento dos riscos e os impactos, de forma que possam ser medidos corretamente.

2.2.6	LGPD	Definir Gestão de Riscos(AIPD/RIPD)	A Gestão de Riscos de Cyber Segurança é crítico para o negócio da Organização, por entender seu ambiente e controlar os riscos em que está exposto, onde neste caso os riscos a serem analisados estão relacionados ao âmbito de Cyber Segurança. É essencial que esta estratégia seja definida de forma a direcionar os gastos, esforços e estratégias de segurança para o negócio. O processo de Gestão de Riscos de Cyber Segurança é composto por políticas, procedimentos, metodologia e equipe especializada.	Identificar componentes/recursos necessários para realizar a Gestão de Riscos de Cyber Segurança Identificar pontos de melhorias nos skills dos colaboradores e quais treinamentos são necessários para a realização do processo. Endereçar ações para a Gestão de Riscos de Cyber Segurança como: - Definir metodologia de Análise de Riscos de Cyber Segurança, contendo: - Lista de ativos; - Mapeamento das ameaças (Ambientes externos e internos a Organização); - Identificação das vulnerabilidades; - Definir taxonomia dos riscos, de forma a facilitar a mitigação dos mesmos.
2.2.7	LGPD	Identificar Riscos(AIPD/RIPD)	O nível e a extensão dos riscos aos quais a organização está sujeita afetam diretamente a resiliência operacional da organização.	Definir todas as ferramentas e técnicas que deverão ser utilizadas na contenção dos ricos organizacionais; Criar uma lista dos riscos operacionais baseados nas categorias dos ativos; Atualizar os parâmetros de risco periodicamente; Listar os riscos operacionais divididos por serviço. Definir programa de atividades identificadas, no âmbito do novo regulamento de proteção de dados, com o objetivo claro de assegurar a realização de um assessment sobre os riscos associados ao tema da privacidade

2.2.8	LGPD	Analisar Riscos (AIPD/RIPD)	A análise de risco é realizada pela organização para determinar a importância relativa de cada risco identificado e é usada para facilitar as atividades de disposição e mitigação de risco da organização. A análise de risco ajuda a organização a colocar os riscos identificados no contexto dos fatores de risco da organização (tolerâncias, apetite e critérios de medição), o que facilita ainda mais o planejamento de mitigação.	Atualizar o impacto causado por cada risco identificado na parametrização dos riscos; Listar todos os riscos identificados, com suas devidas categorizações e priorização previamente definidas; Listar os riscos identificados com a respectiva disposição; Listar os riscos que terão prioridade na mitigação.
2.2.9	LGPD	Realização do RIPD	PIA (Privacy Impact Assessment) deve ser definido, aplicado e gerenciado	Procedimento para a realização do PIA (Privacy Impact Assessment) deve ser definido, verificando a necessidade de contemplar o envolvimento de entidades externas Um PIA deve ser aplicado sempre quando houver: - Um novo programa, sistema ou processo, que estiverem no âmbito da lei - Alteração de programas, sistemas ou processos, que estiverem no âmbito da lei Planos de ações devem ser definidos com base nos problemas identificados no PIA Se aplicável, os resultados obtidos no PIA (incluindo issues), devem ser comunicados às entidades reguladoras e a entidades externas - Efetuar um DPIA aquando da introdução de novos programas, sistemas ou processos, se os mesmos representaram risco para os direitos, liberdades e garantias dos titulares dos dados. - Definir um procedimento para a realização de um DPIA (Data Privacy Impact Assessment) para as atividades identificadas com risco elevado. - Definir um procedimento para identificar e tratar os problemas encontrados aquando da realização do DPIA

2.3.1	LGPD	Definir responsáveis e custodiantes	Contas genéricas normalmente são contas de administradores de sistemas ou contas de teste e normalmente são compartilhadas entre os membros da equipe que devem ter acesso aos sistemas relacionados. A falta de controle nestas contas pode acarretar o compartilhamento indevido entre funcionários e acessos não autorizados, por conta da impossibilidade de ligar os últimos acessos à usuários específicos.	Definir controles para o correto manuseio de contas genéricas. Tipicamente, o owner do sistema ou do ativo deve ser o responsável pelas contas genéricas, devendo zelar pela confidencialidade e evitar o compartilhamento e uso indevido. Registrar, armazenar e controlar todas as contas vinculadas a uma só identidade, seja ela conta de sistema, genérica ou pessoal.
2.3.2	LGPD	Controlar Identidades	Em alguns casos, informações pessoais como telefone, endereço, documentos de identificação são inclusas nos perfis de acesso e estão sujeitas à acessos não autorizados. O controle de acesso à estas informações são necessárias para manter a confidencialidade das mesmas, mantendo a Segurança e Proteção de Dados dos sujeitos e da Organização, garantindo conformidade com regulamentações	Definir procedimento de controle de acesso às informações contidas nos perfis de identidades de forma a garantir a Segurança e Proteção de Dados da Organização e de seus colaboradores
2.4.1	DPMS	Plano de Ação	Revisar projeto base	Revisar projeto base, incluindo ações referentes aos diagnósticos e levantamentos observados (aquisição de software, hardware, revisão de contratos, etc)
2.4.2	DPMS	Orçamento	Atualizar Orçamento	Desenvolver orçamento do projeto final para autorização.

IMPLEMENTAÇÃO				
Seq	Ref.Legal	Assunto	Macro Atividade - Projeto LGPD	Descrição

3.1.1	ISO27701	Organização da Segurança da Informação	Política para Classificação da Informação	A organização deve estabelecer e publicar uma Política que oriente seus funcionários sobre a maneira correta de se classificar uma informação diante de seu conteúdo e relevância para o negócio
3.1.2	LGPD	Política de Segurança da Informação	Um conjunto de políticas para a segurança da informação deve ser definido, aprovado pela gestão, publicado e comunicado aos colaboradores e partes externas relevantes.	Recomenda-se que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. Políticas de segurança geral de informação devem ser definidas, onde recomendamos pelo menos o seguinte conteúdo: a) Objetivo b) Abrangência c) Histórico de revisões d) Resumo Executivo e) Definições f) Sanções g) Papéis e responsabilidades h) Classificação da Informação i) Controle de acesso (Físico e Lógico) j) Códigos maliciosos/Ransomwares l) Desenvolvimento/Manutenção de Sistemas m) Dispositivos Móveis n) Uso de Correio Eletrônico o) Uso de Internet p) Programa de Conscientização q) Proteção e privacidade da informação de identificação pessoal r) Segurança Física s) Senhas t) Terceirização/Fornecedores u) Tópicos orientados aos usuários finais: 1) uso aceitável dos ativos; 2) mesa Limpa e Tela Limpa; 3) transferência de informações; 4) dispositivos móveis e trabalho remoto; 5) restrições sobre o uso e instalação de software. v) Tratamento de Incidentes de Segurança da Informação Para dar base a política geral, as seguintes normas específicas recomenda-se ser criadas a) Norma de Acesso Remoto; b) Norma de Controlo de Acesso Lógico; c) Norma de Classificação da Informação; d) Norma de Gestão de Backup e Restore; e) Norma de Gestão de Continuidade de Negócio; f) Norma de Gestão de Incidentes de Segurança da Informação; g) Norma de Gestão de Terceiros; h) Norma de Retenção de Logs; i) Norma de Restrição de Uso de Software; j) Norma de Uso do Correio Eletrônico; l) Norma de Uso de Equipamentos Portáteis; m) Norma de Uso de Internet.

3.1.3	ISO27701	Organização da Segurança da Informação	Definir os objetivos de Segurança da Informação e Privacidade de Dados	Definir os objetivos que a organização deseja atingir ao estabelecer a contínua gestão da Segurança da Informação e da Privacidade de Dados. Tais objetivos podem ser definidos em Políticas de Segurança da Informação
3.1.4	ISO27701	Políticas de Segurança da Informação	Definir Política de Privacidade de Dados Pessoais	Definir uma Política que estabeleça diretrizes quanto à forma de coleta, finalidade e forma de processamento de Dados Pessoais que possa vigorar de forma interna na organização
3.1.5	ISO27701	Políticas de Segurança da Informação	Definir Política local para Retenção de Dados Pessoais	Definir uma Política que estabeleça diretrizes quanto ao tempo de retenção de dados pessoais, mesmo após o fim do processamento
3.1.6	ISO27701	Políticas de Segurança da Informação	Definir Política de Segurança da Informação para uso e validade local	Definir o conjunto de diretrizes de alto nível para garantir que os princípios da Segurança da Informação (CID - Confidencialidade, Integridade e Disponibilidade) sejam preservados a fim de evitar a exposição a riscos
3.1.7	ISO27701	Políticas de Segurança da Informação	Comunicar as Políticas de Segurança da Informação	A organização deve comunicar formalmente as suas Políticas de Segurança da Informação e Privacidade de Dados para todas as partes interessadas
3.1.8	ISO27701	Organização da Segurança da Informação	Política de Tela e Mesa Limpa	A organização deve estabelecer e divulgar internamente uma Política que contenha diretrizes de Tela e Mesa Limpa, restringindo, por exemplo, a exposição de material físico que contenha Dados Pessoais ao mínimo necessário para atender ao propósito do tratamento identificado
3.1.9	ISO27701	Gestão de Identidades e Acessos	Definir uma Política de Controle de Acesso	A organização deve possuir uma Política de Controle de Acesso que leve em consideração as diretrizes vigentes para acesso aos principais recursos (físicos ou lógicos) que processem Dados Pessoais
3.1.10	ISO27701	Gestão de Identidades e Acessos	Definir uma Política de Senhas	Deve ser definida e aplicada aos recursos de Tecnologia da Informação, processadores de Dados Pessoais ou não, uma Política de Senhas que regule quanto à definição de senhas robustas
3.1.11	ISO27701	Gestão de Segurança Física e do Ambiente	Definir Políticas para a Segurança Física	A Organização deve criar políticas e procedimentos dos controles da Segurança Física dos ambientes. A política de gestão de segurança física define os controles necessários para assegurar todos os ambientes da Organização de forma a minimizar riscos de perda ou vazamento de informações ocasionadas por acesso indevido e/ou por erro humano
3.1.12	ISO27701	Gestão de Desenvolvimento Seguro	Política de Desenvolvimento Seguro	A organização, caso aplicável, deve estabelecer uma Política de Desenvolvimento Seguro que contribua ativamente para os aspectos de privacy by design e privacy by default

3.1.13	LGPD	Destruição segura dos dados em meios físicos e digitais	Definir políticas / procedimentos para proceder a uma destruição segura dos dados em meios físicos e digitais (HDs, pen drives, papeis, etc)	Definir políticas / procedimentos para proceder a uma destruição segura dos dados em meios físicos e digitais (HDs, pen drives, papeis, etc)

3.1.14	LGPD	Dados Pessoais de crianças e menores de idade - Política e procedimento	Definir política e procedimento de recolha e utilização de dados pessoais de crianças e menores. Indicando as condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação	Definir política e procedimento de recolha e utilização de dados pessoais de crianças e menores
3.1.15	LGPD	Política de Privacidade de Dados	Deve ser definida uma política de privacidade e/ou de proteção de dados pessoais na organização	Definir política clara, seguindo os seguintes princípios: Relativa ao propósito pelo qual os dados são recolhidos, e adequada ao ciclo de vida dos dados. Definir o "uso secundário" de dados pessoais, onde será descrito a utilização dos dados pessoais para outros fins para além dos que foram definidos inicialmente Definir e manter uma política de privacidade de dados transversal a toda a organização. Atualizar a Política de Privacidade em todas as plataformas da organização por forma a garantir claramente as práticas relativas a este tema e sua conformidade com a lei Definir termos como: - Privacidade: direito em manter o domínio sobre o nosso corpo, casa, propriedade, pensamentos, sentimentos, segredos e identidade. - Dados pessoais: toda a informação relativa a uma pessoa singular que a possa tornar num indivíduo identificável. - Dados pessoais sensíveis, entre outros.
3.1.16	DPMS	Política de Segurança	Política e Controle de Segurança de Dados	Definir a política de segurança e controle de dados pessoais na instituição
3.1.17	DPMS	Gestão de Uso de Dados	Prática para Gestão do Uso de Dados Pessoais	Executar treinamento referente às políticas de segurança.

3.1.18	ISO27701	Organização da Segurança da Informação	Estabelecer uma Política que regule o uso de dispositivos móveis	A organização deve estabelecer uma Política que regule o uso de dispositivos móveis para fins profissionais e relativos ao negócio, entendendo a importância de assegurar que o uso dos mesmos não conduza a um comprometimento dos dados pessoais

3.1.19	LGPD	Definir a Gestão de Identidades	Uma identidade documenta a existência de uma pessoa, objeto ou entidade que requer acesso a ativos organizacionais, como informações, tecnologia e instalações, para cumprir seu papel na execução de serviços. Gestão de Identidades em uma organização exige que as pessoas, objetos e entidades sejam identificados, perfilados e registrados (através de um perfil de identidade).	Definir políticas e procedimentos para requisição, aprovação, concessão e revogação de acesso a pessoas, objetos e entidades Identificar componentes/recursos necessários para realizar a Gestão de Identidades Identificar pontos de melhorias nos skills dos colaboradores e quais treinamentos são necessários para a realização do processo.
3.1.20	DPMS	Política Transparente	Aviso de Privacidade, Plano de Segurança e Aviso ao Titular	Descrever a política de uso e segurança de dados, em linguagem simples e acessível, e disponibilizá-la em ambiente virtual e físico para acesso ao titular.
3.2.1	DPMS	Armazenamento	Registro de Banco de Dados	Definir controle de cadastros e sistemas de armazenamento. Mapear bases estruturadas, com rico dicionário de dados pessoais armazenados na instituição. Exigir dos prestadores/fornecedores o envio do dicionário dos sistemas.
3.2.2	ISO27701	Gestão de Dados	Estabelecer método seguro para transferência de Dados Pessoais e Informações	Deve ser estabelecido um canal único e seguro para realizar a transferência de Dados Pessoais e Informações
3.2.3	LGPD	Proteção no Database	Bases de dados, contendo dados pessoais, deve estar de acordo com referenciais normativos/melhores práticas de segurança da informação (ex. ISO 27001, NIST, CERT, SANS)	Bases de dados contendo dados pessoais devem era protegidos, com controles como: - Segmentação da rede, entre banco de dados e aplicação; - Aplicação de baseline de segurança; - Controle de acesso, não permitir que qualquer pessoa tenha acesso ao Database; - Não permitir o uso de dados pessoais em databases de homologação e desenvolvimento;- Firewall de Database (se possível).

3.2.4	ISO27701	Gestão de Dados	Acordos de Confidencialidade e NãoDivulgação	Convém que a organização tenha estabelecido com seus funcionários, prestadores de serviço, fornecedores, parceiros e terceiros cláusulas contratuais e acordos de confidencialidade entre as partes interessadas
3.2.4	ISO27701	Gestão de Terceiros	Acordos de Confidencialidade com Fornecedores	A organização deve garantir que, ao firmar seus contratos com fornecedores que processem Dados Pessoais, bem como com todos os fornecedores de tecnologia, cláusulas de confidencialidade estejam inseridas entre os contratos e aditivos firmados entre as partes interessadas

3.2.5	DPMS	Transferência Internacional	Transferência de Dados (Internacionais)	Avaliar existência de troca internacional de dados. Observar operadores e terceiros. Desdobrar avaliação de requisitos de segurança e contratos de garantia.
3.2.6	LGPD	Transferências internacionais de dados pessoais (Dados transfronteiriços)	Os dados pessoais podem ser tratados dentro dos limites definidos pela lei, quando esses dados são transferidos para um local fora desse limite, seja através de um ambiente cloud, sistema de terceiro ou para outra empresa do mesmo grupo corporativo, deve ser aplicado as medidas necessárias para garantir que essa transferência esteja em conformidade com a lei, assim como garantindo a segurança da informação e proteção dos dados pessoais.	Para garantir a proteção de dados na transferência recomendamos os seguintes pontos: - Celebrar um acordo entre as empresas - Implementar controles técnicos no ambiente terceiro, para garantir a proteção dos dados;- Definir regras corporativas (BCR); - Solicitar consentimento, como forma de legitimar a transferência de dados; - Solicitar aprovações da autoridade supervisora, como forma de legitimar a transferência de dados, caso seja necessário.
3.2.7	LGPD	Anonimização dos dados	Anonimização dos dados pessoais na base de dados	Os dados pessoais que não precisam ser identificados devem ser anonimizados, como por exemplo uma pesquisa de satisfação dos clientes
3.3.1	ISO27701	Segurança das Operações	Uso de Criptografia	A organização deve garantir que os canais de comunicação por onde podem transitar dados pessoais, ou que os recursos (sistemas, pastas de rede, dispositivos removíveis) que possam estar processando dados pessoais, recebam a criptografia adequada
3.3.2	ISO27701	Segurança das Operações	Transferência Física de Mídias	Caso a organização adote a cultura de transferir arquivos contendo Dados Pessoais através de dispositivos removíveis, convém que estes possuam a proteção adequada (por exemplo, criptografia, ser um dispositivo homologado e autorizado pela organização)

3.3.3	ISO27701	Segurança das Operações	Descarte de Mídias	Os dispositivos removíveis que possam processar dados pessoais devem receber tratamento adequado quando em caso de descarte, garantindo que a deleção lógica de todos os arquivos seja realizada antes do descarte
3.3.4	ISO27701	Segurança das Operações	Política de Backup	A organização deve estabelecer diretrizes para realização de cópias de segurança
3.3.5	ISO27701	Segurança das Operações	Rotinas definidas para Backup e Restore	A organização deve definir a periodicidade na qual serão realizados os backups e as respectivas situações que exigem o restore de uma cópia de segurança
3.3.6	ISO27701	Segurança das Operações	Execução de Backup	A organização deve executar as rotinas de backup conforme definido em Política de Backup para todos os recursos, incluindo os que processam Dados Pessoais

3.4.1	LGPD	Definir Gestão de Segurança Física	A Organização deve criar políticas e procedimentos dos controles da Segurança Física dos ambientes. A política de gestão de segurança física define os controles necessários para assegurar todos os ambientes da Organização de forma a minimizar riscos de acesso indevido e acidentes.	Elaborar plano de Gestão de Segurança Física contendo todas as atividades necessárias, bem como as ferramentas e técnicas para a realização dos procedimentos envolvidos; Definir lista dos ambientes da Organização e categorização da criticidade; Estabelecer, registrar e criar documentações de segurança física para os ambientes da Organização; Identificar componentes/recursos necessários para realizar a Gestão de Segurança Física. Identificar pontos de melhorias nos skills dos colaboradores e quais treinamentos são necessários para a realização do processo.
3.4.2	ISO27701	Gestão de Segurança Física e do Ambiente	Proteger as instalações físicas	Os ativos das instalações são um dos ativos mais tangíveis e visíveis da organização. Eles fornecem uma presença física à organização e são o ponto de interseção para pessoas, processos e tecnologias que alimentam os serviços organizacionais. Assim, a disponibilidade de instalações é importante para a viabilidade dos serviços organizacionais.
3.4.2	LGPD	Segurança no ambiente corporativo	Controles para garantir a Segurança da Informação no ambiente corporativo devem ser implementados	Recomenda-se que sejam implementados controles para garantir a Segurança da Informação no ambiente corporativo, tais como: Segmentação da rede Restringir o acesso do utilizador as configurações do Desktop Bloqueio de dispositivos USB em Desktops Uso de software de identificação de códigos maliciosos (Endpoint Protection) Restrição de acesso administrativo no Desktop pelo utilizador Criptografia de disco do(s) Desktop(s) Bloqueio de acesso de dispositivos indevidos via porta UTP (ex: port security)

3.4.3	ISO27701	Gestão de Segurança Física e do Ambiente	Definir regras para disponibilização de acesso físico	Devem ser definidas e aplicadas regras para o acesso físico às instalações, ao Datacenter (caso aplicável) e ao arquivo físico da empresa, visando minimizar riscos de perda ou vazamento de informações ocasionadas por acesso indevido e/ou por erro humano
3.4.4	LGPD	Segmentação do ambiente de testes e produção	O ambiente de testes e de produção devem ser segmentados e dados reais não podem ser utilizados no ambiente de testes, assim como o acesso ao ambiente de testes deve ser restrito.	O ambiente de testes e de produção devem ser segmentados e dados reais não podem ser utilizados no ambiente de testes, assim como o acesso ao ambiente de testes deve ser restrito.

3.4.4	LGPD	Proteger ativos de instalações	Os ativos das instalações são um dos ativos mais tangíveis e visíveis da organização. Eles fornecem uma presença física à organização e são o ponto de interseção para pessoas, processos e tecnologias que alimentam os serviços organizacionais. Assim, a disponibilidade de instalações é importante para a viabilidade dos serviços organizacionais.	Implementar controles de segurança física, como por exemplo: - Implantar um processo de controle de acesso na entrada do edifício; - Posicionar seguranças próximos às catracas para monitorar a entrada e saída de funcionários;- Instalar câmeras de segurança em todos os andares da Organização, de forma que todo o complexo seja monitorado; - Instalar controles de acesso a todos os andares do prédio de forma a proteger os ativos e informações da Organização; - Conscientizar os funcionários a sempre utilizarem o crachá à mostra enquanto estiverem na Organização; - Implementar controle de acesso biométrico em ambientes críticos;
3.4.5	DPMS	Interfaceamento	Atividades de Integração (Interfaceamentos)	Avaliar equipamentos e integração de banco de dados. Revisar contratos e garantias de segurança.
3.5.1	LGPD	Definir a Gestão de Configuração Segura	Os ativos da organização devem ser identificados, priorizados, documentados e inventariados. O processo de Gestão de Configuração é composto por políticas, procedimentos, soluções tecnológicas e equipe especializada.	Identificar componentes/recursos necessários para realizar a Gestão de Configuração de Cyber Segurança Identificar pontos de melhorias nos skills dos colaboradores e quais treinamentos são necessários para a realização do processo.
3.5.2	ISO27701	Gestão de Rede e Serviços de Rede	Gerenciar a Segurança nos Serviços de Rede	Serviços de rede, tais como diretórios e e-mail, devem ser gerenciados a fim de garantir que informações são armazenadas, transferidas ou trafegadas com a maior segurança possível

3.5.3	ISO27701	Gestão de Rede e Serviços de Rede	Segregar as redes corporativas	Convém que a organização segrege sua grande rede em outras redes menores, a fim de melhor gerenciar o tráfego de informações. Também é recomendado que exista uma rede exclusiva para uso de convidados, na qual não haja o tráfego de informações sensíveis
3.5.4	ISO27701	Gestão de Rede e Serviços de Rede	Implementar controles de Segurança da Informação na rede corporativa	A organização deve garantir que sua infraestrutura de rede possui a proteção adequada contra ataques direcionados ou interceptações e autenticações indevidas, a fim de assegurar que os dados transitados pela rede corporativa permaneçam confidenciais, íntegros e disponíveis somente para quem deve acessá-los
3.5.5	LGPD	Comunicação segura entre cliente e servidor	Dados pessoais dos titulares podem ser capturados por terceiros, sem uma devida implementação de protocolo de criptografia na comunicação entre o cliente e o servidor.	Recomenda-se a implementação de protocolo de criptografia na comunicação entre o cliente e o servidor, evitando que essa informação seja capturada por terceiros, podendo ser: - Aplicações web, deve ser implementado o HTTPS e habilitar a flag HSTS. - Aplicações cliente servidor, deve ser implementado a criptografia na comunicação dos dados entre estes meios. - Serviços em Cloud, por ex: Office 365, implementar a criptografia dos e-mails.

3.5.6	LGPD	Acessos restritos	Em alguns casos, dados pessoais como nome, telefone, documentos de identificação estão sujeitas à acessos não autorizados. O controle de acesso à estas informações são necessárias para manter a confidencialidade das mesmas, mantendo a Segurança e Proteção de Dados dos sujeitos e da Organização, garantindo conformidade com regulamentações	Recomenda-se que a aplicação implemente os seguintes controles, tanto para os titulares quanto para os administradores dos sistemas: - Autenticação / Autorização; - Atribuir papéis às Identidades (Segregação de Função);- Gerenciamento de Sessão segura.
3.5.7	LGPD	Armazenamento e tratamento seguro do User e Password no sistema	Dados pessoais como o user e a password devem ser armazenados de forma segura e utilizando algoritmos de hash forte. Evitando que estas informações sejam capturadas e acessos indevidos com credenciais válidas sejam realizadas.	Dados pessoais como o user e a password devem ser armazenados de forma segura e utilizando algoritmos de hash forte (SHA-256 ou superior). Evitando que estas informações sejam capturadas e acessos indevidos com credenciais válidas sejam realizadas. Possuir a funcionalidade de segundo fator de autenticação (2FA)

3.6.1	LGPD	Consentimento sobre o uso do Cookie	Implementar controle no portal como um pop-up com a explicação sucinta e clara sobre o propósito da utilização do(s) cookie(s) que a aplicação web utiliza.	Existem 2 tipos diferentes de cookies: - Session cookie: Este cookie é excluindo quando se fecha o browser - Persistent cookie: Este cookie permanece no dispositivo por um período pré definidoQuanto ao domínio ao qual pertence, existem: - First-party cookies: Mesmo domínio do web server. - Third-party cookies Domínio externo, ex Google AnalyticsPara cada um desses cookies deve-se seguir as seguintes regras: - First party session cookies: NÃO precisa do consentimento. - First party persistent cookies: Necessita do consentimento, só deve ser usado quando realmente necessário, com período de expiração de 1 ano no máximo - Todos third party session and persistent cookies: Necessita de consentimento. Este tipo de cookie deve ser evitado no portal, pois dados pessoais podem ser transferidos para países terceiros (Transferência internacional de dados). Deve ser exibido uma barra onde deixe claro os cookies que estão sendo utilizados pela aplicação e solicitar o consentimento do utilizador para os cookies que não são tecnicamente essenciais No link abaixo é demonstrado que o titular aceita todos os cookies ou nega todos os cookies que não são essenciais, não sendo necessário escolher quais cookies quer habilitar ou não, existem alguns sites que para forçar o usuário a escolher uma das opções deixa esse banner grande, atrapalhando a visão do mesmo no site, caso ele não aceite uma das opções. http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm
3.7.1	ISO27701	Gestão de Riscos	Reduzir e/ou tratar riscos	Aplicar as medidas compensatórias que contemplem a redução e/ou tratamento dos riscos

3.7.2	LGPD	Definir Gestão de Vulnerabilidades	O planejamento é conduzido estabelecendo e mantendo uma estratégia para identificar, analisar e gerenciar as vulnerabilidades no ambiente organizacional. A estratégia de Gestão de Vulnerabilidades aborda as ações específicas e o processo de gerenciamento usados para aplicar e controlar as atividades de Gestão de Vulnerabilidades dentro da organização. Isso inclui o escopo do ambiente organizacional a ser verificado quanto a possíveis vulnerabilidades, o desenvolvimento de critérios para categorizar as vulnerabilidades e os parâmetros usados para identificar, analisar e recomendações para solucionar as vulnerabilidades.	Identificar componentes/recursos necessários para realizar a Gestão de Vulnerabilidades. Identificar pontos de melhorias nos skills dos colaboradores e quais treinamentos são necessários para a realização do processo. Endereçar ações para a Gestão de Vulnerabilidades como: - Definir escopo para realizar a Gestão das Vulnerabilidades (TI, Processos e Pessoas) - Identificar pontos de melhorias nos skills dos colaboradores e quais treinamentos são necessários para a realização da análise e mitigação das vulnerabilidades; - Identificar pontos de melhorias nas ferramentas/soluções para realizar a identificação, análise e Gestão das Vulnerabilidades; - Definir política de Gestão de Vulnerabilidades e procedimentos necessários; - Identificar a relação de técnicas e ferramentas necessárias para identificação, análise, mitigação, monitoramento e comunicação de vulnerabilidades; - Definir critérios de categorização da vulnerabilidade;- Identificar custos associados ao processo; - Mapear stakeholders do processo.
3.7.3	LGPD	Mitigar e gerenciar Riscos	Quando as consequências do risco excedem a tolerância de risco da organização, classificado como risco inaceitável, a organização deve agir para mitigar os riscos.	Elaborar um plano de mitigação de riscos que leve em consideração a classificação e o impacto de cada risco identificado. Criar uma lista dos responsáveis definidos por endereçar e tratar os riscos identificados. Manter a lista de riscos sempre atualizada com o status de cada risco identificado.

3.7.4	LGPD	Corrigir inconsistências	A falta de gerenciamento de acessos é uma grande fonte de riscos e vulnerabilidades para a Organização. A revisão periódica de acessos e identidades é um controle detectivo e compensatório que ajuda a Organização a manter o controle de acessos e comunidade de identidades viável e precisa e tem o intuito de identificar entradas inválidas, duplicadas ou que sofreram mudanças não documentadas pelo processo de mudanças.	Definir procedimento de: - Revisão periódica das identidades; - Corrigir as inconsistências Planos de ações que podem ser gerados: - Criar novos perfis de identidade (No caso onde uma ou mais colaboradores compartilham o mesmo perfil de identidade, devendo, no entanto, ter autorização da linha de negócio relacionada); - Realizar mudanças nos perfis de identidade existentes para corrigir inconsistências em informações cadastradas; - Eliminar ou bloquear perfis de identidade duplicados; - Bloquear perfis de identidade que não representam uma pessoa, objeto ou entidade na Organização.
3.7.5	LGPD	Criptografia de discos do Desktop e dispositivos externos	Criptografar disco do(s) Desktop(s) e dispositivos corporativos externos (Notebooks, Pen drive, HDs externos, etc)	Criptografar disco do(s) Desktop(s) e dispositivos corporativos externos (Notebooks, Pen drive, HDs externos, etc)
3.8.1	ISO27701	Gestão de Desenvolvimento Seguro	Segregação de ambientes	Devem ser segregados os ambientes de desenvolvimento, homologação e produção, a fim de garantir a disponibilidade e integridade do sistema desenvolvido ou até mesmo de um recurso de processamento de informações mesmo durante testes, atualizações e correções
3.8.2	ISO27701	Gestão de Desenvolvimento Seguro	Proteger os dados para testes	A organização deve garantir que os testes em sistemas são realizados apenas com Dados Pessoais ou Informações sintéticas. Onde o uso de Dados Pessoais ou informações sintéticas não puder ser evitado, convém que sejam implementadas as mesmas medidas técnicas e organizacionais vigentes em Ambiente de Produção.
3.8.3	ISO27701	Gestão de Identidades e Acessos	Registrar logs e eventos	Convém que as bases de processamento de Dados Pessoais contenham o recurso de rastreabilidade de ações implementado, a fim de identificar as atividades realizadas por um usuário ou por um determinado grupo de usuários

3.8.4	LGPD	Monitorar e gerenciar mudanças de Acesso/ Identidades	Mudanças no ambiente da Organização devem ser refletidas com precisão no inventário de perfis de acesso e identidade em tempo hábil, caso contrário o inventário não irá refletir o nível e acesso atualmente autorizado aos ativos da Organização e podem não ser confiáveis como sendo o baseline para o a proteção destes ativos.	Monitorar e identificar inconsistências entre identidades e pessoas, objetos ou entidades relacionadas, por exemplo: - Quando há adição de novos funcionários; - Quando há mudanças nas responsabilidades dos usuários, devido a mudança de departamento, promoção/demoção ou mudanças nas descrições do cargo; - Mudanças na estrutura da Organização ou dos serviços; - Adição ou finalização de parcerias de negócio.
3.8.5	LGPD	Controles de segurança da informação e proteção dos dados na aplicação	Requisitos de Proteção de Dados devem ser implementados no desenho, desenvolvimento de novos produtos, assim como os sistemas já existentes	Controles de segurança da informação e proteção de dados devem ser implementados no desenho, desenvolvimento de novos produtos, assim como nos sistemas já existentes Recomenda-se que a aplicação implemente os seguintes controles: - Arquitetura de Segurança; - Comunicação segura, entre cliente e servidor; - Controle de acesso seguro; - Configuração segura do servidor/serviço; - Integrações externas seguras; - Trilhas de Auditoria (Log); - Tratamento de Erros (Exceções); - Validação dos dados entradas, do lado do servidor.
3.10.1	DPMS	Documentação	Documentação de Proteção de dados – Evidências	O comité deverá reunir em um único relatório, as atividades desenvolvidas, incluindo anexos, lista de presenças, contratos e simulações, etc
3.11.1	DPMS	Plano de Ação	Revisar projeto base	Revisar projeto base, incluindo ações referentes aos diagnósticos e levantamentos observados (aquisição de software, hardware, revisão de contratos, etc)
3.11.2	DPMS	Orçamento	Atualizar Orçamento	Desenvolver orçamento do projeto final para autorização.

GOVERNANÇA				
Seq	Ref.Legal	Assunto	Macro Atividade - Projeto LGPD	Descrição
4.1.1	DPMS	Proteção de Dados - Partes Envolvidas	Relatório de Proteção de Dados e Privacidade – Partes envolvidas	Listar, em relatório, titulares, dados, uso de dados, funções e uso dos dados. A informação resultado desse relatório deverá compor o plano de governça de dados, e deverá ser publicado.

4.2.1	DPMS	Comunicação com Titular	Plano de Solicitações, Reclamações e Retificação	Desenvolver estrutura de comunicação com o titular para recepção, gestão e resposta de solicitações
4.2.2	LGPD	Pedido de acesso a dados pessoais	Definir procedimento para responder a pedidos de acesso a dados pessoais	Procedimento para responder a pedidos de acesso a dados pessoais, deve conter uma matriz com: - Sistemas; - Responsáveis; - Plano de comunicação; - Prazos de resposta
4.2.3	LGPD	Direito ao Esquecimento - Processo	Definição do processo do Direito ao Esquecimento, que deve ser respeitado por toda a organização	Definir processo que será seguido para as solicitações de Direito ao Esquecimento, contemplando: - Exclusão; - Restrição; - Objeção. Onde deverá ser definindo uma matriz contemplando: - Sistemas; - Responsáveis; - Dados tratados; - Plano de comunicação; - Prazos Este processo deve ser automatizado, na medida do possível, e bem definido, para evitar o risco de erro humano na execução do direito ao esquecimento.
4.2.4	LGPD	Direito ao esquecimento - Funcionalidades do sistema	Sistemas precisam estar preparados para solicitações de direito ao esquecimento, porém o mesmo não pode apagar 100% dos dados do titular, para necessidades legais, como faturamento, esses dados não podem ser apagados.	Recomenda-se o uso de blacklists com os titulares que solicitem o direito ao esquecimento. Onde permita que os dados sejam apagados no sistema, a menos que esses dados possuam necessidades legais.

4.3.1	LGPD	Controle de consentimento sobre o processamento dos dados pessoais	Definir controle para obter o consentimento de recolha e utilização de dados pessoais De acordo com a definição da palavra consentimento, sendo a manifestação de vontade livre, específica, informada e explícita, mediante declaração de aceitação por parte do titular dos dados, em como o mesmo consente no tratamento dos dados pessoais que lhe dizem respeito.	Implementar controle de aceite do processamento dos dados pessoais, pelos titulares, nos cadastros onde são recolhidos dados pessoais. assim como armazenar o mesmo de forma segura no Database. As mensagens devem ser customizáveis conforme a necessidade da Organização.
4.3.2	LGPD	Autorização para cadastro de dados de menores de idade	De acordo com a lei em relação aos serviços da sociedade da informação, todo cadastro de menor de idade, deve ser solicitado autorização de um adulto ou responsável maior de idade.	Para todo cadastro de menor de idade, deve ser solicitado autorização de um adulto ou responsável maior de idade. A maioridade se diferencia em cada país, o sistema deve permitir customizar este parâmetro, para definir a maioridade por país.

4.4.1	LGPD	Definir a Gestão de Incidentes de Segurança da Informação e Proteção de Dados	A organização deve estabelecer processos para identificar, analisar, responder e aprendendo com os Incidentes para evitar as consequências de riscos imprevistos e gerenciar essas consequências quando realizado. O processo de Gestão de Incidentes de Segurança e Proteção de Dados é também uma fonte de conhecimento que ser usada pela organização para melhorar planos e práticas de continuidade e estratégias para proteger e sustentação de serviços e ativos.	Identificar componentes/recursos necessários para realizar a Gestão de Incidentes de Segurança e Proteção de Dados. Identificar pontos de melhorias nos skills dos colaboradores e quais treinamentos são necessários para a realização do processo. Definir Política de Gestão de Incidente de Segurança e Proteção de Dados; As seguintes normas recomenda-se ser definidas: - Classificação da Informação; - Uso do Correio Eletrônico; - Integração com Terceiros; - Uso correto da Internet;- Acesso Remoto; - Retenção de Logs. Mapear: - Canais de entrada de Incidentes de Segurança e Proteção de Dados internos e externos; - Criar canais de entrada para comunicações de Incidentes(E-mail, SMS, tickets, etc.); - Interações com entidades externas (ex: Cert); - Leis, regulamentações e políticas referentes relevantes ao negócio da Organização, suportando o processo de resposta ao Incidente. Definir: - Campanhas de conscientização dos usuários devem ser realizadas; - Categorias de Incidentes; - Serviços que serão prestados pela equipe de Gestão de Incidentes de Segurança e Proteção de Dados; - Contratos com terceiros envolvidos na resposta ao Incidente.
4.4.2	DPMS	Resposta a Incidentes	Plano de resposta de violações, por categoria (incidente, notificação, logs, testes, correção, métricas)	Avaliar riscos e definir cenários de ocorrência de perda e/ou vazamento de dados. Para cada cenário, descrever o plano de resposta incidentes que deverá conter orientação para publicações em redes sociais, midias, comunicação com titular, com anpd e comunicações internas.
4.4.3	ISO27701	Gestão de Incidentes de Segurança da Informação	Definir um Procedimento de Gestão de Incidentes	A organização deve definir um procedimento formal de Gestão de Incidentes que inclua papéis, responsabilidades e procedimentos, seja para tratar de incidentes de Segurança da Informação ou incidentes que envolvam Dados Pessoais
4.4.4	ISO27701	Gestão de Incidentes de Segurança da Informação	Determinar níveis de atendimento e suporte	A organização deve determinar níveis específicos para resolução de um incidentes, direcionando assim, todas as tomadas de decisão de forma correta

4.4.5	LGPD	Detectar eventos de Segurança da Informação e Proteção de Dados	Incidentes se originam como eventos organizacionais. A organização poder monitorar e identificar eventos à medida que eles ocorrem, bem como determinar quando um evento ou uma série de eventos constitui um Incidente que requer uma resposta coordenada e planejada.	Tratar Eventos de Segurança e Proteção de Dados encaminhados pelos canais de entrada interno/externos; Elaborar procedimento de identificação e reporte de Eventos de Segurança e Proteção de Dados; Registrar Eventos/Incidentes de Segurança e Proteção de Dados deve ser realizado em uma ferramenta única e de forma segura; Registrar e atualizar todo o histórico dos Eventos de Segurança e Proteção de Dados; Definir procedimento de registro e atualização dos Eventos de Segurança e Proteção de Dados; Elaborar procedimento de coleta, documentação e preservação das evidências dos Eventos de Segurança e Proteção de Dados; Definir critérios de priorização de cada evento de Segurança e Proteção de Dados, divididos por categoria.
4.4.6	LGPD	Declarar Incidente de Segurança da Informação e Proteção de Dados	Declaração de Incidente de Segurança e Proteção de Dados define o ponto em que a organização estabeleceu que um Incidente ocorreu, está ocorrendo ou é iminente e terá que ser solucionado.	Definir critérios para declarar quando um Evento de Segurança se torna um Incidente Elaborar procedimento de revisão periódica da base de conhecimentos para correlacionamento de Incidentes em análise Manter atualizado o histórico dos Incidentes durante todo o ciclo de vida Definir critérios para análise de Incidentes Elaborar procedimento de análise do Incidente Definir ferramentas, técnicas e atividades relevantes para analisar os Incidentes
4.4.7	ISO27701	Gestão de Incidentes de Segurança da Informação	Formar base de conhecimento de incidentes	Convém que a organização registre e documente todos os incidentes já solucionados para servir como forma de Base de Conhecimento para futuras ocorrências semelhantes
4.4.8	ISO27701	Gestão de Incidentes de Segurança da Informação	Responder a Incidentes de Segurança da Informação ou com Dados Pessoais	Todos os incidentes reportados devem ser solucionados em tempo hábil. Quando um incidente envolver Dados Pessoais, uma análise crítica deve ser conduzida a fim de avaliar impactos e tempo de resposta.

4.4.9	LGPD	Responder e se recuperar de um Incidente Segurança da Informação e Proteção de Dados	A natureza de um Incidente declarado é que a organização já incorreu algum efeito, embora limitado, requer que a organização atue no Incidente.	Elaborar procedimento de escalonamento dos Incidentes entre equipes internas e externas Definir critérios de escalonamento dos Incidentes entre equipes internas e externas Integrar com a área de GCN (Gestão de Continuidade de Negócio) Definir procedimento de resposta para cada Incidente mapeado, baseado no ciclo de vida Mapear stakeholders e seus respectivos protocolos e canais de comunicação Definir procedimento de Incidentes de violação de dados pessoais Definir matriz de responsabilidade dos grupos solucionadores, por categoria do Incidente Criar matriz RACI com o devido SLA (Service Level Agreement) para cada grupo solucionador Definir procedimento de comunicação por Incidente, centralizado e atualizado Definir critérios de finalização dos Incidentes
4.5.1	LGPD	Priorizar ativos de instalações	A Organização possui diversos ativos e instalações críticas para o funcionamento dos negócios que devem ser listados e priorizados para que controles de segurança sejam implementados.	Listar todos os ativos e instalações críticas da Organização de forma que controles de segurança possam ser criados para gerenciar o risco destes ambientes; São considerados alguns exemplos de ambientes críticos para a Organização: - Prédios da Organização e seus ambientes internos e áreas comuns; - Fábricas; - Data centers; - Outros locais onde exista trânsito de funcionários e equipamentos. Identificar ativos que fazem parte do processo de Continuidade de Negócios ; Documentar em políticas e procedimentos todos os controles de segurança relacionados aos ativos da Organização, de forma a garantir que estes sejam seguidos e que possam ser gerenciados e atualizados.

4.5.2	LGPD	Gerenciar Vulnerabilidades	A organização deve desenvolver e implementar uma estratégia de resolução apropriada das vulnerabilidades para as quais a organização determinou que a exposição deve ser reduzido ou eliminado	Elaborar e implementar uma estratégia para gerenciar a exposição de vulnerabilidades em seu ambiente, de forma a reduzir ou eliminá-la, de forma a reduzir os riscos de Cyber Segurança inerentes à estas vulnerabilidades e garantir a Segurança e Proteção de Dados. Elaborar a estratégia levando em consideração os seguintes pontos: - Aplicar patches em softwares, sistemas e firmwares; - Desenvolver e implementar novos controles de proteção ou atualizar controles existentes; - Desenvolver e implementar novos panos de continuidade de serviços ou atualizar os existentes; - Garantir que todos os stakeholders do processo tenham ciências das vulnerabilidades;- Atualizar o repositório de vulnerabilidades com informações sobre a estratégia de gestão de vulnerabilidades; - Monitorar os status das vulnerabilidades abertas; - Analisar a eficiência das estratégias de Gestão de Vulnerabilidades para garantir que os objetivos foram alcançados.
4.5.3	LGPD	Gerenciar riscos de ativos de instalações	Avaliações de riscos devem considerar ameaças, vulnerabilidades e eventos que os ativos da Organização estão sujeitos e determinam os controles a ser melhorados ou implantados para a contenção de Incidentes.	Realizar avaliações de risco periódicas levando em consideração o ambiente físico da Organização e sua localização. Tipos de ameaças e vulnerabilidades incluem mas não se limitam a: - Eventos, não criminoso, realizado por pessoas ou naturais; - Eventos criminosos como roubos, acesso não autorizado ou sabotagem; - Mudanças políticas, sociais ou demográficas na localização da Organização;- Pessoas, incluindo as que possam ter conhecimento sobre o edifício.
4.7.1	ISO27701	Organização da Segurança da Informação	Processo Disciplinar	A organização deve estabelecer em seus processos disciplinares ações que contemplem as violações de políticas e normas de Segurança da Informação e Privacidade de Dados
4.7.2	LGPD	Geração de métricas relacionadas a Proteção dos Dados	Geração de métricas relacionadas a Proteção dos Dados	Métricas associadas ao tema da Proteção dos Dados devem ser definidas, tais como: Quantidade de não conformidades identificadas X tratamentos realizados Quantidade de vulnerabilidades identificadas que tem o risco de vazamento de dados pessoais Quantidade de incidentes de Segurança e Proteção dos Dados identificados X corrigidos Solicitações de esquecimento realizadas X atendidas

4.7.3	LGPD	Controlar mudanças de Configurações dos ativos	A aplicação de configurações pode criar impactar o funcionamento dos ativos, o baseline deve ser testado em um ambiente controlado antes de aplicada em ambiente de produção	Definir processo de mudança de configuração, contemplando: - Processo de mudança e aprovação - Lista de mudanças pré aprovadas - Processo de análise de impacto em segurança - Requisitos de teste - Restrições - Mudanças emergenciais - Revisões e atualizações - Processo de Rollback
4.7.4	DPMS	Treinamento Políticas	Plano de Treinamento	Treinar equipe da instituição na política de segurança de dados pessoais
4.8.1	DPMS	Entrega - Projeto	Procedimento de Aprovação e Entrega	Toda a documentação, especialmente políticas e governança, juntamente com atividades executadas, deverão ser apresentadas em reunião de entrega para conclusão do projeto.

AVALIAÇÃO				
Seq	Ref.Legal	Assunto	Macro Atividade - Projeto LGPD	Descrição
5.1.1	DPMS	Teste de Segurança	Auditoria com terceiros (pentests*)	Contratar empresa especializada em análise de vulnerabilidades para execução de testes controlados de invasão no serviço de tecnologia. O relatório deverá orientar a construção de novas tarefas e ações.
5.1.2	DPMS	Auditoria Interna	Auditoria Interna	A partir do mapa de dados, executar avaliação das atividades da instituição para garantir a manutenção das alterações do processo e da documentação.
5.2.1	DPMS	Relatório de Riscos e Resultados	Relatório de Riscos e Resultados	Descrever relatório da análise, informando forma da execução, riscos encontrados, e ações de tratamento.
5.2.2	DPMS	Executar Avaliação de Impacto	Executar Avaliação de Impacto	Acompanhar início de novas ativdiades, executando AIPD para cada novo cenário, promovendo adaptações para casos de vulnerabilidades
5.2.3	DPMS	Resolver Riscos	Resolver Riscos	Riscos e vulnerbilidades observdas na auditoria e simulações dever ser classificados, gerando novas ações.
5.2.4	ISO27701	Gestão de Riscos	Revisar metodologia de avaliação de riscos, bem como os planos de ação e tratamento dos riscos (Lições aprendidas)	A geração de métricas e documentação de mudanças no programa de conscientização da Organização garante uma forma de medir a evolução da maturidade do programa e a aderência da Organização em uma cultura de Segurança e Privacidade da Informação.
5.3.1	ISO27701	Políticas de Segurança da Informação	Revisar as Políticas de Segurança da Informação	A organização deve estabelecer um período para realizar a revisão de suas Políticas de Segurança da Informação ou revisá-las sempre que houver mudanças significativas no negócio
5.3.2	DPMS	Monitorar Leis e Regulamentos	Monitorar Leis e Regulamentos	Acompanhar mudanças legislativas, promovendo atualização na documentação, na políticas, alinhando treinamento para ajuste de conduta.
5.3.3	DPMS	Benchmarking	Benchmarking	Realizar visita a instituições do mesmo porte e negócio para avaliar gestão de segurança da informação e compartilhar experiência

5.4.1	LGPD	Revisar Gestão de Identidades (Lições aprendidas)	Um processo de gestão de mudanças efetiva de acessos e identidades requer um processo de monitoramento do ambiente e identificação de adição, mudança e deleção de perfis. A geração de métricas permite identificar pontos de mudança no processo de Gestão de Identidades. As mudanças possibilitam que o processo seja atualizado periodicamente e garante uma melhoria contínua.	Definir métricas, como estes exemplos: - Porcentagem de identidades solicitadas que foram recusadas - Porcentagem de identidades criadas, que após análise detalhada foram bloqueadas, devidos a algum erro humano - Porcentagem de identidades que estão de férias ou inválidas - Porcentagem de identidades pertencentes a contas de serviços - Porcentagem de identidades pertencentes a entidades externas - Porcentagem de identidades que tiveram suas senhas divulgados de forma lícita ou ilícita.

5.4.2	LGPD	Revisar Gestão de Segurança Física (Lições aprendidas)	Os relatórios de risco geram insumos para a melhoria contínua do projeto e devem documentar as saídas das análises de forma a colaborar com a melhoria do processo.	Listar resultados da análise de risco para cada tipo de ativo Identificar as categorias e prioridades dos riscos Definir planos de ação para mitigar os riscos identificados Definir métricas, como estes exemplos: - Porcentagem de ativos organizacionais inventariados - Porcentagem de ativos com/sem responsáveis definidos - Porcentagem de ativos críticos para o negócio - Porcentagem de ativos que não atentem os requisitos de resiliência
5.4.3	LGPD	Revisar Gestão de Vulnerabilidades (Lições aprendidas)	Realizar análise da causa raiz das vulnerabilidades identificadas e gerar métricas para melhorar o processo de Gestão de Vulnerabilidades	Realizar análise de causa raiz das vulnerabilidades identificadas Definir métricas, como estes exemplos: - Porcentagem de vulnerabilidades que necessita de uma análise de causa raiz; - Quantidade de vulnerabilidades identificadas X Quantidade de vulnerabilidades mitigadas; - Porcentagem de vulnerabilidades por criticidade; - Porcentagem de vulnerabilidades por categoria; - Porcentagem de vulnerabilidades por status de tratamento; - Tempo médio de mitigação das vulnerabilidades por criticidade.

5.4.4	LGPD	Revisar Gestão de Configuração dos ativos (Lições aprendidas)	A geração de métricas permite identificar pontos de mudança no processo de Gestão de Configuração de Segurança. As mudanças possibilitam que o processo seja atualizado periodicamente e garante uma melhoria contínua.	Definir estratégia de monitoramento, contemplando: - Ferramentas e métodos de avaliação; - Tolerância a riscos; - Cronograma de testes periódicos; - Revisão de resultados; - Retestes e acompanhamento de correções; - Revisão de baseline ou documentação de exceções.Definir métricas, como estes exemplos: - Porcentagem de ativos inventariados - Porcentagem de ativos com baselines implementados X não implementados - Porcentagem de ativos que foi realizado rollback - Porcentagem de baselines atualizados
5.4.5	ISO27701	Gestão de Riscos	Definir periodicidade para execução de avaliação dos riscos em Segurança da Informação e Privacidade de Dados	Estabelecer um período fixo ou condição válida para conduzir as avaliações de riscos relacionados à Segurança da Informação, bem como as avaliações de impacto à Privacidade (DPIA). Espera-se que a organização tenha uma metodologia direcionada a esta atividade.
5.4.7	DPMS	Avaliação não programada	Avaliação não programada	Executar testes e simulações para verificar vulnerabilidades na conduta.

5.4.8	LGPD	Revisar Gestão de Incidentes Segurança da Informação e Proteção de Dados (Lições aprendidas)	Um dos aspectos mais importantes da Gestão de Incidentes de Segurança e Proteção de Dados é a capacidade de entender por que um Incidente ocorreu e o que pode o impacto para a organização. Do ponto de vista de Gestão de Risco, usando lições aprendidas para melhorar controles e estratégias de proteção e otimizar essas estratégias com planejamento de continuidade e resposta eficaz desloca a atenção da organização de um modo de resposta para um modo preventivo.	Avaliar causa raiz dos Incidentes de Segurança e Proteção de Dados reportados Definir integração entre as áreas de Gestão de Problemas e Gestão de Incidentes de Segurança e Proteção de Dados Analisar e controlar Eventos de Segurança e Proteção de Dados anormais (Incidentes, problemas e erros) Definir métricas, como estes exemplos: - Porcentagem de indisponibilidade (tempo operacional) que serviços e ativos de alta criticidade ficaram fora de operação devido a Incidentes de Segurança e Proteção de Dados; - Porcentagem de Incidentes de Segurança e Proteção de Dados que exploraram vulnerabilidades existentes com soluções conhecidas, patches ou correções temporárias; - Número e porcentagem de Eventos e Incidentes de Segurança e Proteção de Dados tratados em um período específico e que foram contidos em um período específico; - Aumento em porcentagem no volume de Eventos e Incidentes de Segurança e Proteção de Dados em um período específico; - Porcentagem de Incidentes de Segurança e Proteção de Dados que requereram envolvimento da aplicação da lei; - Número de Eventos e Incidentes de Segurança e Proteção de Dados que foram registrados, mas não fechados; - Número e porcentagem de recorrências de específicos Eventos e Incidentes de Segurança e Proteção de Dados. - Reclamações/incidentes no contexto da Proteção de Dados

5.4.9	LGPD	Revisar Gestão de Riscos (Lições aprendidas)	Lições aprendidas na identificação, avaliação e mitigação de riscos afeta diretamente as estratégias existentes para proteger e sustentar ativos e serviços, que podem se beneficiar do processo de Gestão de Riscos. Para usar as informações de risco para gerenciar a resiliência operacional, a organização deve usar diretamente as informações de risco como insumo para validar a eficácia das estratégias atuais de proteção e sustentação e para melhorar essas estratégias com base no entendimento do risco.	Elaborar uma lista dos controles da gestão de risco que necessitam de revisão; Elaborar uma lista do plano de continuidade dos serviços que necessitam de revisão; Criar um plano de revisão dos planos de continuidade de serviço, contendo os responsáveis e a periodicidade de revisão; Definir, implantar e medir as métricas de Cyber Segurança para a elaboração dos resultados da gestão de risco e trazer possibilidades de melhoria. Definir métricas, como estes exemplos: - Porcentagem de ativos e serviços que foi impactado ou custo de comprometimento foi identificado; - Porcentagem de riscos identificados que possuem um plano de mitigação, com status definido; - Quantidade de riscos que não foram tratados; - Porcentagem de riscos que ultrapassaram a tolerância de riscos
5.4.10	LGPD	Avaliações de conformidade de fornecedores	Recomenda-se a avaliação anual dos fornecedores, com relação a requisitos de segurança da informação e proteção dos dados nos sistemas desenvolvidos e nos processos internos do fornecedor.	Recomenda-se a avaliação anual dos fornecedores, com relação a requisitos de segurança da informação e proteção dos dados nos sistemas desenvolvidos e nos processos internos do fornecedor
5.5.1	DPMS	Validação do Programa DPMS Implantado	Procedimento de Aprovação e Entrega	Toda a documentação, especialmente políticas e governança, juntamente com atividades executadas, deverão ser apresentadas em reunião de entrega para conclusão do projeto.