omnisblue

PLANO DE AÇÃO DA ÁREA DE NEGÓCIO TECNOLOGIA DA INFORMAÇÃO (TI)

Hospital São Marcos (HSM) | Omnisblue

Apresentação DO PROJETO

De acordo com as definições do Escopo do Projeto e Plano de Projeto aprovados pelo HSM, o projeto em execução realiza ***atividades de consultoria especializada para apoio à implementação de programa de adequação a Lei Geral de Proteção de Dados (Lei Federal n 13.709/2018) através do uso de ferramentas de gerenciamento de privacidade nas áreas de negócio do HSM.***

Objetivos do documento

- Documentar o resultado obtido após conclusão da etapa de Preparação do projeto de adequação à LGPD em execução na área do Tecnologia da informação (TI)
- Direcionar os colaboradores da área de negócio em relação às atividades que precisam ser concluídas para avançamos o projeto na etapa de Engajamento e Adequação à LGPD.

Fundamentos legais

As análises e definições presentes neste documento estão fundamentadas na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18), nos parâmetros definidos pela norma ISO/IEC 27.001 e pelas estratégias definidas no framework de adequação à LGPD de propriedade da Omnisblue, apresentado para o time do controlador em detalhes durante o *Workshop geral sobre LGPD* já realizado no projeto.

Todas as ações sugeridas aqui têm como origem as informações fornecidas pelo responsável da área de negócio do Controlador durante a etapa de Preparação/Diagnóstico da Adequação à LGPD e essas informações estão todas inventariadas no ambiente *Privacy & Compliance Project (PCP)* do Controlador.

É imperativo que o Controlador e seus representantes tomem ciência das informações presentes na plataforma de governança de privacidade implementada (PCP) e, em caso de distorção em relação à realidade operacional de suas rotinas, alerte a Omnisblue, uma vez que as informações ali contidas foram fruto de levantamento e narrativas apresentadas pelos próprios representantes do Controlador.

Resumo do projeto até aqui

O projeto de adequação à LGPD se iniciou com a elaboração do Plano de Projeto conhecido e firmado entre as partes e teve sua primeira ação mais palpável observável por todos os stakeholders com o *Workshop geral sobre LGPD*.

A partir do alinhamento teórico entre as partes, foram realizadas diversas atividades de levantamento entre o time de especialistas da Omnisblue e os colaboradores do cliente (internos ou terceiros) onde foram levantados os aspectos operacionais, tecnológicos e jurídicos do Controlador relacionado às suas áreas de negócio.

Parte desse levantamento tratou de analisar riscos operacionais associados às medidas administrativas e técnicas de segurança da informação atualmente em uso pelo controlador em cada área específica de negócio.

Para a área tratada aqui, esses levantamentos produziram os seguintes quantitativos inventariados:

- **05 processos de negócio**
- **13 rotinas de tratamento de dados pessoais**
- **13 riscos de segurança e privacidade**
- **11 atividades de adequação a serem executadas nas etapas de Engajamento e Adequação**
    - Aspectos operacionais e administrativos: 06 ações
    - Aspectos tecnológicos: 05 ações

Todas as informações inventariadas, e disponibilizadas no ambiente de produção do *Privacy & Compliance Project (PCP)*, foram na sequência analisadas pelos especialistas da Omnisblue e, a partir dessa análise, foram elencados os *Riscos de Privacidade e Proteção de Dados Pessoais* específicos da área aqui tratada e, a partir desses riscos, foram definidas as *Atividades de adequação* específicas da área pendentes e parte integrante do ciclo de adequação do Controlador à Lei Geral de Proteção de Dados dentro dos limites de escopo do projeto.

A seguir detalhamos então os *Riscos* e as *Atividades* específicos da área que endereçam ações que devem ser realizadas e monitoradas pelos responsáveis de negócio do controlador, com suporte da Omnisblue a partir daqui.

Cabe ressaltar que, além desses riscos e ações específicas da área, o projeto ainda contará com a produção de um *Plano de Ação Global* para o controlador, que irá analisar riscos gerais e listar outras atividades que atenderão não só a área de negócio aqui tratada, como também todas as demais unidades de negócio do controlador.

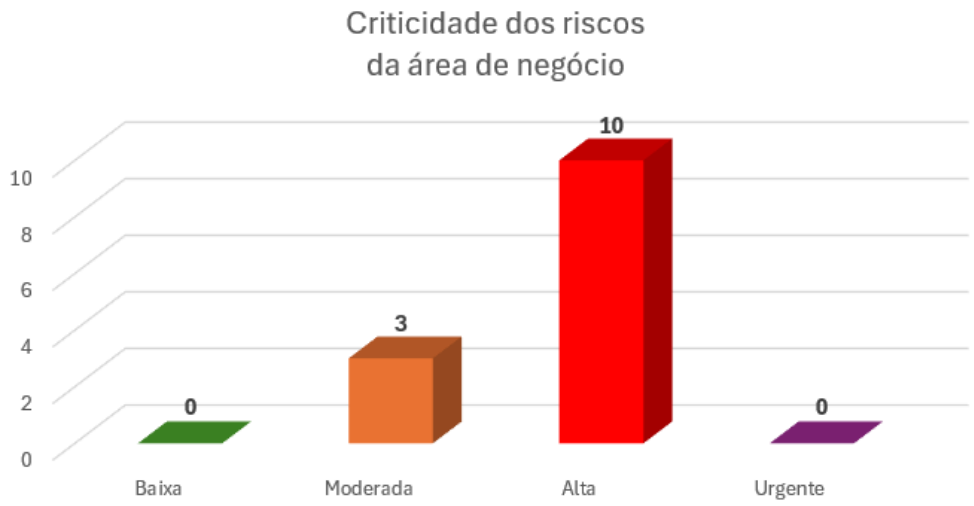
Por fim, vale destacar que os riscos e atividades aqui tratados tiveram como foco a operação e uso de dados pessoais sob a ótica das medidas administrativas e técnicas de segurança, e não sobre o fluxo em si da informação, algo que será ainda tratado nas próximas etapas do projeto.

Visão geral dos riscos de privacidade e proteção de dados

Os riscos encontrados, inventariados e com suas respectivas estratégias definidas foram classificados de acordo com sua criticidade que é automaticamente observada de acordo com a seguinte matriz de classificação de impacto *versus* probabilidade:

Probabilidade	Impacto: Baixo	Impacto: Médio	Impacto: Alto
100%	Alta	Urgente	Urgente
90%	Moderada	Urgente	Urgente
80%	Moderada	Alta	Urgente
70%	Moderada	Alta	Urgente
60%	Moderada	Alta	Alta
50%	Baixa	Alta	Alta
40%	Baixa	Moderada	Alta
30%	Baixa	Moderada	Moderada
20%	Baixa	Baixa	Moderada
10%	Baixa	Baixa	Moderada

Esses riscos podem ser analisados em detalhe no ambiente PCP do Controlador, na funcionalidade “Riscos” e a distribuição de suas respectivas criticidades, para a área aqui tratada, pode ser compreendida de acordo com o gráfico a seguir:



As atividades de adequação detalhadas a seguir tratam, inclusive, das ações a serem realizadas para executar as estratégias de gestão e mitigação de todos os riscos esses riscos associados à área de negócio.

A lista de riscos de privacidade deve ser compreendida como algo que evolui ao longo do tempo, onde novos riscos serão descobertos, encerrados, disparados ou terão seus atributos modificados de acordo com eventos internos ou externos ao Controlador. A gestão desses riscos, muito além das atividades definidas neste plano, deve ser tarefa contínua, a ser realizada

pelo DPO do Controlador durante a fase de Operação do ciclo de vida do Sistema de Gestão de Privacidade e Proteção de Dados (SGPD).

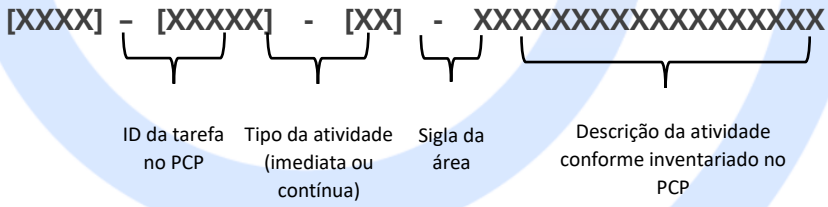
Visão geral das ações de adequação a serem realizadas na área

As análises sobre todas as informações inventariadas durante a etapa de **Preparação** geraram uma lista de ações/atividades a serem executadas a seguir no projeto.

Essas atividades foram cadastradas no ambiente PCP do Controlador na funcionalidade "Atividades e Ações" e podem ser classificadas de acordo com os aspectos de sua natureza técnica predominante, tal como segue:

- **Aspectos operacionais e administrativos**: Tratam de ações que alteram rotinas operacionais e administrativas do Controlador, adequando aspectos geralmente mais associados a papéis e responsabilidades, medidas administrativas e fluxo de informação e processos;
- **Aspectos tecnológicos**: Tratam de ações que alteram requisitos de Tecnologia da Informação do Controlador, adequando aspectos geralmente mais associados parâmetros de TI de Ativos de Informação eletrônicos e medidas técnicas de segurança;

A seguir listamos todas as atividades levantadas e planejadas para a área de negócio, dentro do escopo de ajustes de medidas administrativas e técnicas de segurança, agrupadas de acordo com sua classificação de seus aspectos conforme definidos acima, e utilizando o seguinte padrão:



O tipo da atividade define se a sugestão para a execução da ação é **imediata** (*a ser executada pela parte responsável ainda dentro do prazo e escopo do projeto atual*) ou se é **contínua** (*a ser executada pelo DPO do controlador em etapas complementares/futuras de gestão do SGPD*).

Aspectos operacionais e administrativos (06)

As atividades mais associadas aos aspectos operacionais e administrativos de adequação à LGPD que devem ser executadas para completar a adequação do Controlador dentro dos limites do projeto em questão são:

- **[Imediata] - [TI] - Implementar requisitos de compartilhamento de dados com terceiros na unidade/departamento**
  - *Resultado esperado*: Fazendo uso da nova política de segurança da informação do controlador, apresentar aos colaboradores da unidade/departamento as regras a serem seguidas para o compartilhamento de informações com terceiros, e conscientizar os colaboradores sobre a obrigatoriedade de aderência à essas diretrizes, sob pena de sanções administrativas.

- **[Contínua] - [TI] - Implementar política de uso de e-mails corporativos na unidade/departamento**
  - *Resultado esperado*: Apenas endereços de e-mails corporativos devem ser utilizados na unidade/departamento para fins de atividades de trabalho e envio e recebimento de dados pessoais.
    Fazendo uso da nova política de segurança da informação do controlador, entregar aos colaboradores uma conta de e-mail corporativa individual e não permitir o uso de e-mails pessoais para atividades de trabalho, sob pena de sanções administrativas.

- **[Contínua] - [TI] - Implementar/ajustar as rotinas de descarte de dados pessoais eletrônicos na unidade/departamento**
  - *Resultado esperado*: Fazendo uso da nova política de descartes de dados do controlador, compatibilizar as rotinas de exclusão e esquecimento de dados pessoais eletrônicos realizadas pela unidade/departamento de acordo com os requisitos pré-estabelecidos.

- **[Imediata] - [TI] - Implementar política de mesa limpa na unidade/departamento**
  - *Resultado esperado*: Fazendo uso da nova política de segurança do controlador, apresentar as regras de ""mesa limpa"" que devem ser observadas na unidade/departamento, garantindo segurança e disponibilidade ideal das informações físicas tratadas na área.

    Essas regras devem ser demonstradas aos colaboradores, bem como a obrigatoriedade de serem seguidas, sob pena de sanções administrativas.

- **[Imediata] - [TI] - Implementar política de impressão na unidade/departamento**
  - *Resultado esperado*: Fazendo uso da nova política de segurança do controlador, apresentar as regras de "compartilhamento de impressão" que devem ser observadas na unidade/departamento, garantindo segurança e disponibilidade ideal das informações físicas tratadas na área.

    Essas regras devem ser demonstradas aos colaboradores, bem como a obrigatoriedade de serem seguidas, sob pena de sanções administrativas.

- **[Contínua] - [TI] - Implementar/ajustar as rotinas de descarte de dados pessoais físicos na unidade/departamento**
    - *Resultado esperado*: Fazendo uso da nova política de descartes de dados do controlador, compatibilizar as rotinas de exclusão e esquecimento de dados pessoais físicos realizadas pela unidade/departamento de acordo com os requisitos pré-estabelecidos.

Aspectos tecnológicos (05)

As atividades mais associadas aos aspectos técnicos e tecnológicos de adequação à LGPD que devem ser executadas para completar a adequação do Controlador dentro dos limites do projeto em questão são:

- **[Contínua] - [TI] - Implementar bloqueio automático de telas por inatividade nos dispositivos corporativos**
    - *Resultado esperado*: Os dispositivos utilizados para acessar os ativos de informação eletrônicos em uso na unidade/departamento (desktops e notebooks) devem ser configurados de forma que eles realizem o travamento da tela de forma automática quando da inatividade do usuário após 5 (cinco) minutos.

- **[Contínua] - [TI] - Implementar criptografia de discos nos dispositivos corporativos**
    - *Resultado esperado*: Os dispositivos utilizados para acessar os ativos de informação eletrônicos em uso na unidade/departamento (desktops e notebooks) devem ser configurados de forma que seus discos possuam criptografia ativada, garantindo que apenas usuários com senhas possam acessar o conteúdo de seus discos.

      Para equipamentos Windows, utilizar, por exemplo, o BitLocker.

- **[Contínua] - [[TI] - Armazenar os ativos físicos em local com controle de acesso**
    - *Resultado esperado*: Os documentos (artefatos) físicos em uso na unidade/departamento devem ser armazenados em local seguro, com controle de acesso, garantindo que apenas colaboradores com devida permissão possam ter acesso a esses documentos.

      Sugere-se a movimentação desses arquivos em sala ou armário seguros, trancados com chave/cadeado e as chaves devem ser entregues apenas aos colaboradores com permissão para acessar os documentos, mediante assinatura de termo de responsabilidade.

- **[Imediata] - [TI] - Implementar monitoramento de câmeras nos ambientes onde são armazenados os ativos físicos**
    - *Resultado esperado*: Os documentos (artefatos) físicos em uso na unidade/departamento devem ser armazenados em local seguro, com monitoramento de câmera que garanta a possibilidade de se consultar histórico de acesso ao local.

Sugere-se que as imagens sejam armazenadas por um período de ao menos 30 (trinta) dias, e descartadas/substituídas após esse período.

Conclusão

As ações sugeridas neste Plano de Ação já foram cadastradas no PCP para controle e acompanhamento de seus resultados, e este documento deve ser conhecido por todos os stakeholders do Controlador, em especial os colaboradores da área de negócio em questão, e que porventura sejam envolvidos direta ou indiretamente na execução dessas ações.

Os prazos, as datas planejadas para a execução de cada atividade prevista neste Plano de Ação são de responsabilidade do HSM, mas esse planejamento pode ser realizado em conjunto com a Omnisblue, que inclusive manterá sua equipe disponível para suporte total aos temas.
O PCP, inclusive, pode ser utilizado para acompanhamento eletrônico do avanço das tratativas dessas atividades.

Como dito anteriormente, as ações e riscos aqui tratados se somam às demais atividades e riscos que serão levantados e documentados, estejam eles associadas às demais áreas de negócio do controlador ou associados ao escopo geral de gestão do órgão, e o time da Omnisblue segue à disposição para o suporte na implementação dessas ações.