POLÍLICA DE TRATAMENTO E USO DE DADOS

PERMANÊNCIA E TRANSFERÊNCIA COM PARCEIROS

A H2r trabalha com dados pessoais das empresas clientes sensíveis e passíveis de auditoria por parte de clientes e parceiros no referido à LGPD (Lei Geral de Proteção de Dados).

É tido como **Dados Pessoais** os seguintes identificadores:

Nome Completo	Endereço	Geoposicionamento
nomes de parentes próximos,	RG(Registro Geral)	CPF
Identificação biométrica	Identificação Facial	Numero de Passaporte
Números de Cartões de Crédito	Data de Nascimento(junto a outros dados)	

Assim descreve como politica interna:

1. TRANSMISSÃO E COMPARTILHAMENTO

1.1. Envio de e-mails

Todos os dados de Clientes devem utilizar a função Dados Sigilosos/Confidential, onde a mensagem tem rastreabilidade e prazo de deleção.

Revisão antes de envio, verificar se somente ao destinatário necessário com a rastreabilidade e prazo de deleção.

1.2. E-mail Marketing

A lista de Clientes não podem ser compartilhadas com outras ferramentas e somente pode ser transmitidos e-mails para clientes ou pessoas cadastradas em sistemas da Crescimentum com permissão de recebimento de mensagens pelo Marketing, passível de usuário e Gestor de explicações por e-mails enviados sem os devidos cuidados de retirada da lista quando solicitado pelo Cliente.

1.3. Dados com empresas terceirizadas

Os dados armazenados por empresas parceiras, devem conter o prazo de retenção do dado, devendo este assinar o TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS PESSOAIS.

As empresas representadas devem eleger o Data Protection Officer (DPO) e este se incumbirá de responder sobre o armazenamento, tempo de retenção, especificação de tratamento de dados e exclusão com o armazenamento de logs destas atividades.

2. RETENÇÃO DE DADOS

Dados sigilosos que necessitam de armazenamento, para a sua retenção os mesmos devem estar com armazenamento criptografado e/ou apelidos não identificáveis para os dados armazenados.

Para isso devem usar ferramentas de criptografia interna ao equipamento e/ou compartilhamento através da ferramenta de criptodados

Previsto como dados retidos e identificáveis o prazo do contrato em aplicação ou quando não mencionado a retenção no prazo de 60 dias por identificação.

3. TRATAMENTO DE DADOS INTERNOS

Quando os dados dos pessoais forem necessários tratamento para compilar/originar um novo documento, este novo documento composto deverá ter a ciência do cliente/pessoa afetada o tempo de resguardo destas informações e ao termino do projeto ter a notificações de exclusão de dados após 60 dias de término do projeto. Item a ser gerenciado pelo gestor de projeto no TEP (Termo De Encerramento De Projeto).

Tratamento de Dados para Business Inteligence, caberão aos analistas de dados o processamento de dados de modo a não ter identificação indiviual ao cliente sob o serviço prestado e sim a salvaguarda de que os dados foram tratados de forma generalizada para obter melhorias de processos e segmentação de dados.

4. SALVAGUARDA E SEGURANÇA DE DADOS

Backups devem ser realizados diariamente e em um ambiente não interno, isto é, aonde o servidor ou iteração humana seja dispensáveis para a execução e armazenamento e gerenciamento por tratamento de Logs de execução.

Crashtest devem ser realizados com a periodicidade máxima de de 28 dias corridos.

Disaster recover podem ser necessários como complemento ao Crash Test de modo a termos o tempo de recuperação total de sistemas e dados. E a sua viabilidade ou desprezo de informações.

5. POLITICA DE SENHAS

Senhas de identificação não podem ser armazenadas em arquivos internos da rede, bem como compartilhadas.

As mesmas devem seguir a alteração periodica, com restrição de uso interno e não iguais às demais senhas do usuário.

Prevenção e bloqueio de senhas com mais de 3 tentativas de acesso.

Sempre que possível, notificar por e-mail/SMS o que foi executado aos dados da pessoa.

6. PREVENÇÃO E USO DE DADOS

Revisão a este documento devem ser realizados semestralmente, juntamente com as evidências de execução das atividades de limpeza e armazenamento de dados.

7. DESENVOLVIMENTO DE SISTEMAS

As fases de inicio, desenvolvimento e testes devem ser executadas em banco de dados de testes com dados fictícios, até com revelação de dados de produção, mas nunca identificáveis e compartilhados com outros.

Em ambiente de produção os dados devem ficar em servidor/Ambiente separado ao front-end com portas de comunicação não rastreáveis e não as padrões : 1433, 3006, 5432

Servidores de Front-end, devem ter o usuário Administrador/Administrator desabilitado, porta de RDP não padrão (3389 e 22) e ICMP também desabilitado

8. TRATATAMENTO DE EXPOSIÇÃO

Estar preparado para mitigar o risco de exposição de dados é obrigação da empresa como confiança a nós empregado. Assim temos dois documentos em anexo que deve ser de conhecimento geral:

- Termo de confidencialidade (Anexo A)

- Template de Report de Incidente (Anexo B)

LEI 13.709/18 (partes mais importantes)

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

I - finalidade específica do tratamento;

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

III - identificação do controlador;

IV - informações de contato do controlador;

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

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS PESSOAIS (NDA)

Com o objetivo de atender da Lei de proteção de dados(LGPD - Lei 13.709/18), adotamos medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados. Também adotamos medidas para prevenir a ocorrência de danos em virtude do tratamento indevido dos dados pessoais dos nossos clientes.

Para assegurar que os nossos colaboradores, fornecedores e seus funcionários, estão igualmente empenhados, cientes e comprometidos com as exigências previstas na Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais, LGPD, conforme as regras descritas abaixo:

1ª - a manter sigilo, tanto escrito como verbal, ou, por qualquer outra forma, de todos os dados, informações científicas e técnicas e, sobre todos os materiais obtidos com sua participação, podendo incluir, mas não se limitando a: técnicas, desenhos, cópias, diagramas, modelos, fluxogramas, croquis, fotografias, programas de computador, discos, disquetes, pen drives, processos, projetos, dentre outros;

2ª - Fica vedado ao fornecedor. o compartilhamento de dados pessoais com terceiros, salvo se previamente autorizado pela EMPRESA e/ou Cliente ou que este seja fundamental para execução do contrato, cumprimento de dever legal ou regulatório, resguardados os direitos mencionados no art. 9° da Lei 13.709/18.

3ª - Não autorizamos, em nenhuma hipótese, a retenção de documentos físicos ou cópias, para fins diversos daqueles que se destinavam originalmente. Salvo para cumprimento de dever legal, regulatório, exercício regular de direitos, previsto em contrato ou com propósito de atender a processo judicial. administrativo ou arbitral.

4ª - O operador de dados obriga-se a informar a empresa, sobre ocorrências de vazamento de dados que afetem ou possam atingir, direta ou indiretamente seus clientes e para isso utilizar-se do TEMPLATE DE REPORTE DE INCIDENTE.

O **colaborador responderá solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas fornecidas pela política de dados da empresa**, hipótese em que o operador se equipara ao controlador de dados. salvo nos casos de exclusão previstos no art. 43 da Lei 13.709/18.

PARAGRAFO ÚNICO Caso o operador de dados, em razão do exercício indevido de atividade de tratamento de dados pessoais. causar a outrem, dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, será obrigado a repará-lo.

As medidas descritas acima, visam a proteção dos dados dos nossos clientes, assim como, são requisitos mínimos previstos na Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais, LGPD.

E, assim por estarem justo, acertados e informados assina o presente documento.

_____

Nome/Cargo /Empresa

TEMPLATE DE REPORTE DE INCIDENTE

Empresa	
Responsável de Contato (ou Encarregado/DPO)	
E-mail	
Telefone	
Data de detecção do incidente	
Data/Hora de comunicação ao responsável de Tratamento	
Estado do incidente	
Data de resolução	
Hora de resolução	
Tipo de incidente	Obs:

Natureza do incidente		Obs:
Descrição		Obs:
Causa do Incidente		Obs:
Consequências do Incidente		Obs:
Medidas de segurança prévias ao incidente		Obs:
Medidas corretivas/mitigadoras		Obs:
Número estimado de Titulares afetados		Obs:

Tipo de Titulares afetados		Obs:
Tipo de Dados Pessoais afetados		Obs:
Os Dados Pessoais afetados permitem a identificação direta dos Titulares?		Obs:
Inteligibilidade dos Dados Pessoais		Obs:
Recursos a subcontratantes (especificar)		Obs:
Existência de fluxos internacionais de Dados Pessoais fora do território brasileiro		Obs:
Outras informações relevantes		

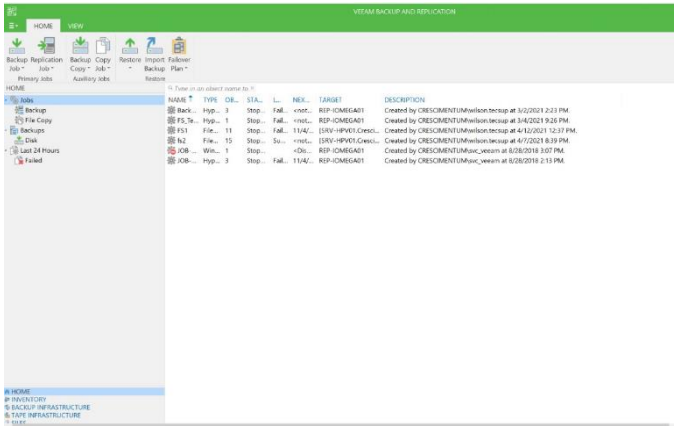
ESTRATÉGIA DE BACKUP

Para regras de Backups utilizamos a estratégia 3 – 2 -1 que compreeende:

3 cópias durante o dia, isto é, uma a cada 8 horas. Shadow Copy no Servidor de arquivos e de Banco de dados Estações de trabalho tem os seus dados armazenados em servidor Sharepoint Microsoft	2 cópias ao término do dia em um servidor espelhado e em um midia interna(Storage de dados)	1 cópia dos dados para a nuvem pelo Veem Backup. Estações de trabalho tem os seus dados individualmente armazenados em servidor Sharepoint Microsoft

DISASTER RECOVERY : Testados a cada 4 meses, por recuperação de máquina Virtual de servidor completa. Retenção de 30 dias.

CÓPIA EM NUVEM : Testados 1 vez ao mês a recuperação aleatória pelo Veeam Backup. Retenção de 30 dias.


VEEAM BACKUP AND REPLICATION
HOME
VIEW
Backup Job
Replication Job
Backup Copy
Copy Job
Restore
Import Backup
Failover Plan
Primary Jobs
Auxiliary Jobs
Restore
HOME
Jobs
Backup
File Copy
Backups
Disk
Last 24 Hours
Failed
NAME
TYPE
TARGET
DESCRIPTION
HOME
INVENTORY
BACKUP INFRASTRUCTURE
TAPE INFRASTRUCTURE