ÍNDICE DE REVISÕES

REVISÃO	STATUS	DESCRIÇÃO
0	AP	Elaboração inicial do documento.
A	REV	Inclusão do tópico de testes na seção 3.2.11. Retirada de diversos tópicos das seções 3.2.2, 3.2.5 e 3.2.8

PA - PARA APROVAÇÃO	CA - CANCELADO	PR - PRELIMINAR
PI - PARA INFORMAÇÃO	AP - APROVADO	LI - LIBERADO

REVISÃO	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G
DATA	13/04/2022	03/08/2023						
ELABORAÇÃO	CARLOS C.	MARIANA O.						
ANÁLISE CRÍTICA	ADRIANA S.	MARCELA /JULIO						
PADRONIZAÇÃO	ADRIANA S.	ADRIANA S.						
APROVAÇÃO	PAULO M.	BRUNO B.						

Sumário

1. ATA DE APROVAÇÃO

A ata de aprovação desta política encontra-se devidamente assinada e arquivada na plataforma UniVoce, no Curso Adequações LGPD, disponível a todos os colaboradores da empresa.

URL de Acesso: https://univoce.com.br/course/view.php?id=46

2. ABRANGÊNCIA

Abrangência interna e externa, para todos os colaboradores, clientes, fornecedores, parceiros e demais utentes que queiram conhecer esta Política.

3. POLÍTICA

3.1 Introdução

3.1.1 A Política de Segurança no Desenvolvimento de Software é um complemento da Política de Segurança da Informação da empresa e está baseada na metodologia de controles da ABNT NBR ISO/IEC 27002:2013 proposta no Guia de Avaliação de Riscos de Segurança e Privacidade publicado pela Secretaria de Governo Digital (SGD);

3.1.2 Essa política deverá ser seguida pelos desenvolvedores de software da empresa a partir da data de sua aprovação.

3.1.3 Essa política está fundada nos princípios do *Privacy by Design* e do *Security by Design*, que propõem que as empresas adotem procedimentos de desenvolvimento para respeitar os direitos de privacidade e segurança da informação nos produtos e serviços que oferecem.

3.2 São medidas necessárias para o cumprimento dessa política no que diz respeito a:

3.2.1 Garantir a continuidade do negócio:

- A empresa adotará mecanismos e procedimentos para reduzir os riscos de ocorrência de ataques de negação de serviço;
- A empresa elaborará um plano de continuidade de negócio que estabeleça procedimentos a serem seguidos durante a ocorrência de situações adversas.

3.2.2 Garantir a adoção de controles criptográficos:

- O compartilhamento ou a transferência de dados pessoais nos softwares desenvolvidos pela empresa ocorrerá por meio de canais criptográficos que garantam a segurança das informações em tráfego.

3.2.3 Garantir a adoção de medidas que possibilitem realizar o controle de acesso aos softwares:

- Os sistemas serão desenvolvidos de forma a possibilitar aos clientes a definição de diversos padrões de permissão (edição e visualização, somente visualização, etc.) para que os clientes possam gerenciar os acessos aos softwares oferecidos pela empresa;
- Os softwares produzidos pela empresa deverão garantir um padrão mínimo de segurança nas senhas de acesso (por exemplo, a senha deve ter, no mínimo, 8 caracteres, letras maiúsculas, caracteres especiais e números);

- As credenciais de acesso aos softwares desenvolvidos e comercializados pela empresa deverão estar gravadas em recursos de tecnologia da informação protegidos por criptografia;
- Os softwares produzidos pela empresa deverão garantir que as credenciais de acesso sejam transmitidas de forma segura e protegida;
- Nos softwares produzidos pela empresa, deverão existir mecanismos de recuperação de senha que permitam a recuperação de maneira segura, sem que a aplicação forneça a senha definitiva;
- Nos softwares produzidos pela empresa, deverão existir mecanismos que permitam o encerramento (expiração) da sessão após um período determinado de inatividade.

3.2.4 Garantir a existência de cópias de segurança dos dados tratados no sistema:

- Os softwares produzidos pela empresa terão a frequência de realização de backups definida pela empresa, em acordo aos contratos firmados com os clientes;
- Para proteger os clientes contra a perda total das informações armazenadas nos sistemas produzidos pela empresa, as cópias de segurança deverão ser mantidas em localidades remotas e a uma distância suficiente para garantir sua integridade e disponibilidade, caso algum incidente venha a ocorrer no sistema;
- Poderão ser realizadas cópias de segurança dos logs;
- Para garantir a integridade dos dados armazenados, os softwares produzidos pela empresa deverão possuir mecanismos para identificar se ocorreram alterações não autorizadas.

3.2.5 Garantir o desenvolvimento seguro dos softwares:

- Para garantir o desenvolvimento seguro dos softwares produzidos pela empresa, deverão ser seguidas as diretrizes dessa política e de outros procedimentos já adotados na empresa para essa finalidade;
- Os softwares deverão ser produzidos tendo como regra a observação do princípio do Security by Design, que significa que os requisitos de segurança deverão ser respeitados e observados desde o início do desenvolvimento dos softwares, prevendo toda possibilidade de riscos aos quais a aplicação pode estar sujeita;
- A empresa procurará revisar periodicamente as medidas de segurança aplicadas nos softwares que realizam o tratamento de dados pessoais.

3.2.6 Garantir a gestão da capacidade e redundância:

- Os softwares produzidos pela empresa deverão possuir mecanismos para monitoramento do uso de recursos, de forma que atendam às necessidades de capacidade futura e garantam o desempenho requerido nas aplicações;
- Os recursos de processamento da informação deverão possuir redundância suficiente para atender a requisitos de disponibilidade do sistema que venham a ser estipulados em contrato.

3.2.7 Garantir a gestão das mudanças:

- As mudanças realizadas nos softwares produzidos pela empresa deverão ser planejadas e testadas;
- Quando for necessária a realização de alguma mudança nos softwares produzidos pela empresa e a mudança não for motivada por urgência, deverão ser realizadas análises de potenciais riscos e consequências, priorizando os riscos relacionados à segurança da informação;
- As mudanças deverão ser comunicadas às partes interessadas. Sempre que envolverem riscos, principalmente relacionados à segurança da informação, deverão ser comunicadas ao cliente;

- Quando for identificada a existência de alguma vulnerabilidade em um sistema produzido pela empresa ela deverá ser comunicada via HelpDesk e classificada de acordo com os critérios abaixo:
  - Vulnerabilidade de baixo risco;
  - Vulnerabilidade de médio risco;
  - Vulnerabilidade de alto risco.
- De acordo com a classificação realizada no item anterior, os prazos para o tratamento das vulnerabilidades serão os seguintes:
  - Vulnerabilidade de baixo risco: deverá ser tratada em até 72 horas;
  - Vulnerabilidade de médio risco: deverá ser tratada em até 48 horas;
  - Vulnerabilidade de alto risco: deverá ser tratada em até 24 horas.
- Os prazos fixados no item anterior poderão ser estendidos mediante justificativa ou caso uma vulnerabilidade de maior risco apareça durante o processo de correção.

3.2.8 Garantir a gestão dos riscos envolvidos:

3.2.9 Garantir o registro de eventos, rastreabilidade e salvaguarda de logs:

- Os logs dos sistemas produzidos pela empresa deverão registrar a identificação dos usuários, incluindo os administradores e os que têm acesso privilegiado;
- Os logs dos sistemas desenvolvidos e comercializados pela empresa deverão registrar o endereço de IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso;
- Os logs dos sistemas desenvolvidos e comercializados pela empresa deverão registrar as ações executadas pelos usuários;
- Os logs dos sistemas desenvolvidos e comercializados pela empresa deverão registrar data e hora do evento ocorrido com alguma outra fonte de tempo sincronizada;
- Os logs dos sistemas desenvolvidos e comercializados pela empresa deverão ser protegidos contra edição e exclusão;
- Os logs dos sistemas desenvolvidos e comercializados pela empresa deverão ser protegidos contra acessos indevidos;
- Os sistemas desenvolvidos e comercializados pela empresa deverão permitir que as operações realizadas com dados pessoais sejam registradas e que seja possível a identificação de quem as realizou, além da data e hora da realização.

3.2.10 Garantir a efetiva resposta a incidentes:

- A empresa procurará adotar medidas para possibilitar a detecção, o tratamento e a resposta a incidentes de segurança ocorridos nos softwares de produção própria;
- Quando incidentes dessa natureza ocorrerem, deverão ser comunicados ao Comitê Gestor de Proteção de Dados Pessoais para deliberação sobre posterior comunicação ao cliente. Para isso, a empresa deverá manter atualizada a lista de contatos que, em caso de incidentes, devem ser comunicados, avisando-os sobre a dimensão do incidente e as medidas adotadas para sua mitigação;
- Quando, na ocorrência de algum incidente, for impossível preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, os responsáveis pelos softwares produzidos pela empresa deverão:

- Coletar e armazenar cópias dos arquivos afetados pelos incidentes, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação e outros que julgarem necessários, mantendo a estrutura do diretório original;
- Coletar e armazenar os ‘’metadados’’ desses arquivos, como data, hora de criação e permissões;
- Registrar em relatórios a impossibilidade de preservar as mídias afetadas, listando os procedimentos adotados para realizar esse procedimento.

3.2.11 O procedimento de anonimização de dados na realização de testes com dados pessoais deverá obedecer aos seguintes critérios:

- Os testes dos softwares de saúde e educação desenvolvidos pela A4PM deverão ser realizados em dois ambientes distintos: DESENVOLVIMENTO e HOMOLOGAÇÃO. Em ambos os ambientes, deverão ser utilizados dados fictícios para a realização dos testes.
- Mesmo que porventura seja usada uma base de dados real para povoar esses ambientes, os dados reais deverão passar por um processo de anonimização.
- O processo de anonimização será realizado pela utilização de duas funções de banco de dados, uma que gera uma combinação aleatória de nomes e sobrenomes. Por exemplo, será escolhida uma sequência de 100 nomes masculinos, 100 nomes femininos e 100 sobrenomes que serão randomicamente combinados conforme um parâmetro informado e o retorno dessa função será usada para fazer uma atualização do dado real.
- Exemplo: CREATE FUNCTION `nome`(p_sexo INT) RETURNS varchar(255) CHARSET latin1 BEGIN

```
-- 1 M E 2 F
IF (p_sexo = 1) THEN
SET @nome := CONCAT(ELT(FLOOR(1 + (RAND() * (100-1))),
"Julio","Gabriel","João","PatricK","Roberto","Mario","Michel","Bernardo","William" ,"El
iziel","David","Jerry","Ricardo","Kelvin","Charles","Sergio","Jose","Marcos",
"Luciano","Marcelo","Antônio","Jorge","Daniel","Rafael","Paulo","Adriano","Marcos" ,"Th
iago","Aldair","Heitor","Raine","Sandro","Ygor","Anderson","André",
"Carlos Alberto","Edson","Alessandro","Arthur","Bruno","Ronaldo","Michael",
"Anthony","Lauro","Kevin","Andre","Jacson","Carlos Antônio",
"Matheus","Jonathan","Cleber","Giron","Timoteo","Elielton","Everton","Roney",
"Larry","Angelo","Diego","Douglas","Darley","Brendo","Nelson","Ney","Erico",
"Vanderley","Jose Carlos","Robson","Andrey","Vitor","Ramon","Cássio",
"Crisjes", "Reinaldo","Rogério","Marco Antônio","Jerry","Delcides",
"Denilson","Armando","Walter","Arlindo","Patrick","Julio Cesar","Peterson",
"Christiano","Aroldo","Julio Henrique","Wellington","Anecy","Henrique",
"Feno","Sarmento","Menezes","Maturana","Diaz","Miranda"));
END IF;
RETURN @nome;
END
```

- Além disso, também deverá ser feita uma anonimização do documento CPF original através de uma outra função conforme apresentada abaixo:

```
CREATE FUNCTION `cpf`() RETURNS varchar(255) CHARSET latin1
BEGIN
SET @n = 9;
SET @n1 = ROUND(RAND()*9);
SET @n2 = ROUND(RAND()*9);
SET @n3 = ROUND(RAND()*9);
SET @n4 = ROUND(RAND()*9);
SET @d1 = @n9 * 2 + @n8 * 3 + @n7 * 4 + @n6 * 5 + @n5 * 6 + @n4 * 7 + @n3 * 8 + @n2 * 9 + @n1 * 10;
SET @d1 = 11 - ( @d1 % 11 );
SET @d2 = 11 - ( @d2 % 11 );
SET @d2 = IF(@d2>=10,0,@d2);
RETURN concat(CAST(@n1 AS NCHAR) , CAST(@n2 AS NCHAR) , CAST(@n3 AS NCHAR) , '.' , CAST(@n4 AS
```

```
NCHAR) , CAST(@n5 AS NCHAR) , CAST(@n6 AS NCHAR) , '.' , CAST(@n7 AS NCHAR) , CAST(@n8 AS NCHAR) ,
CAST(@n9 AS NCHAR) , '-' , CAST(@d1 AS NCHAR) , CAST(@d2 AS NCHAR));
```

- Essa função deverá gerar CPF's numericamente válidos, porém, legalmente inválidos.
- Os profissionais DBA ao pegarem uma base real de produção para usá-la para a realização de testes nos ambientes de DESENVOLVIMENTO e/ou HOMOLOGAÇÃO devem utilizar essas duas funções para realizar atualizações nos dados reais em todos os locais que permitam a identificação do paciente real. Além disso, também deverão ser realizadas atualizações dos dados de endereço e contato para usar algum endereço e telefone fictício, removendo os dados reais.

Através desse procedimento, a A4PM não terá como objetivo utilizar dados reais para execução de teste em softwares.

3.3 Auditorias Internas

3.3.1 Para verificação do cumprimento das normas definidas nessa e nas demais políticas internas, será responsável o setor de Auditoria Interna, que poderá implementar rotinas, eventuais ou programadas, de auditoria.

3.3.2 Será de responsabilidade dos gestores de setor contribuir para a realização das auditorias citadas no item anterior fornecendo todos os dados necessários aos responsáveis pela sua realização.

3.4 Casos Omissos

3.4.1 Os casos omissos serão avaliados pelo Comitê Gestor de Proteção de Dados Pessoais para posterior deliberação;

3.4.2 As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da empresa adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da empresa.

3.5 Revisões

Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Proteção de Dados Pessoais.

3.6 Gestão da Política

3.6.1 A Política de Segurança no Desenvolvimento de Software é aprovada pela Diretoria da empresa, em conjunto com o Comitê Gestor de Proteção de Dados Pessoais.

3.6.2 Essa Política precisa estar atualizada em sua última versão na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas, conforme acesso anteriormente citado.

4. DIRETRIZES

4.1 Objetivo

Essa Política descreve controles, baseados em normas internacionalmente reconhecidas, que servirão como diretriz para garantir um padrão de segurança mínimo para que os clientes possam ter maior confiança nos produtos oferecidos pela empresa.

4.2 Atribuições e Responsabilidades

A Diretoria Executiva e os gestores de setor devem estar comprometidos com uma gestão efetiva de segurança da informação dentro da empresa. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da empresa.