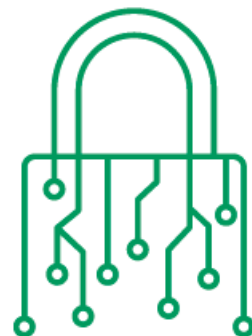


**SEGURANÇA DA  
INFORMAÇÃO**

Uma responsabilidade de todos!

**Unimed** 



# Programa Nacional de Segurança e Privacidade

Requisitos Técnicos

## 1. Tráfego Seguro de Arquivos

### a. Conectividade

REQUISITO	CONFORMIDADE	USO	DATA	OBS
Certificado Digital Auto Assinado	Utilizar certificado digital que utilize criptografia de, no mínimo, 256 bits. <u>Adotado novo padrão de Certificado Digital SHA2 com 512 bits / Uso do JWT</u>	OBRIGATÓRIO		Nessa primeira fase, substituir os certificados por esse padrão
Tipo de Certificado Digital Válido	Adquirir Certificado Válido através de certificadora reconhecida.	OBRIGATÓRIO		Essa fase será discutida posteriormente, na próxima Reunião (Março)
Uso do Certificado ICP-Brasil	Uso de Certificado ICP-Brasil através de certificadora reconhecida	RECOMENDADO		<b>Avaliação em conjunto posteriormente</b>

### b. Identificação e autenticação de usuário

REQUISITO	CONFORMIDADE	USO	DATA	OBS
Identificação e autenticação do usuário	Todo usuário deve ser identificado e autenticado antes de qualquer acesso a dados.	OBRIGATÓRIO		
Método de autenticação	Utilizar, no mínimo, um dos seguintes métodos de autenticação: <ul style="list-style-type: none"><li>• Usuário e senha;</li><li>• Certificado (para assinatura digital)</li></ul>	OBRIGATÓRIO		
Proteção dos parâmetros de autenticação	Se a aplicação gerir um repositório de credenciais, esta deverá garantir que as senhas são armazenadas usando funções fortes de salt e hash e que a tabela/arquivo que armazena as senhas e as próprias chaves sejam manipuladas apenas pela aplicação. Deve ser utilizado algoritmo reconhecidamente seguro como, por exemplo: SHA-2.	OBRIGATÓRIO		

Segurança de senhas	<p><b>Condição:</b> <u>Utilização de autenticação baseada em usuário/senha.</u></p> <p><b>Tamanho:</b> Mínimo de 10 caracteres ou mais</p> <p><b>Complexidade:</b> Utilizar combinação de pelo menos um (01) caractere de cada um dos quatro (4) tipos de caracteres listados abaixo:</p> <ul style="list-style-type: none"> <li>• Letras Maiúsculas e Minúsculas (AZ – az), <ul style="list-style-type: none"> <li>• Números (0-9)</li> </ul> </li> <li>• Símbolos ASCII (~! @ # \$% ^ &amp; * () _ + - = {}   \.:"; '&lt;&gt;?,. / e espaço) e caracteres Unicode.</li> </ul> <p><b>Idade (aging):</b> Trocar após um período de 60 dias</p> <p><b>Reutilização:</b> Após 5 trocas com aging</p> <p>Armazenar a senha de forma codificada (Apenas o código Hash).</p>	OBRIGATÓRIO		
Controle de tentativas de “Login Inválido”	<p>Bloquear o usuário após um número máximo de tentativas de <i>login</i> inválido.</p> <p>Sugere-se o bloqueio após 6 tentativas erradas ou após 45 dias de inatividade</p>	OBRIGATÓRIO		
Controle de Usuário de Serviços	<p>Definir políticas distintas de usuários de serviços e integração entre as aplicações</p>	OBRIGATÓRIO		

## 2. Desenvolvimento

### a. Controle de versão do software

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Controle de Versão de software	Os sistemas devem possuir uma versão associada contendo nome aplicação/componente, fornecedor e número de versão. Os sistemas devem permitir a visualização da versão da aplicação e/ou seus componentes de software por parte do usuário.	OBRIGATÓRIO		Voltado aos Sistemas que tratam dados pessoais ou segundo Critério de Risco
Código fonte	Deve ser possível, a partir do número de versão de cada componente da aplicação, resgatar seus códigos-fonte correspondentes, possibilitando a rastreabilidade dos arquivos fontes que o geraram.	OBRIGATÓRIO		Quando desenvolvido internamente  Voltado aos Sistemas que tratam dados pessoais ou Critério de Risco
Histórico de alteração	Manter histórico descritivo de todas as alterações realizadas em cada versão, contendo a data e o responsável pela alteração.	OBRIGATÓRIO		Voltado aos Sistemas que tratam dados pessoais ou Critério de Risco
Repositório de versões	Ter um repositório estruturado com todas as versões dos componentes (executáveis e códigos-fonte) que foram utilizadas em produção em algum momento, permitindo voltar versões anteriores em casos de atualizações mal sucedidas.	OBRIGATÓRIO		Voltado aos Sistemas que tratam dados pessoais ou Critério de Risco
Dependências dos componentes	Para cada versão de cada componente, criar e indicar no manual de instalação e requisitos de sistema, quais são suas dependências com outros componentes do sistema desenvolvido ou do ambiente, e os requisitos de operação.	OBRIGATÓRIO		Voltado aos Sistemas que tratam dados pessoais ou Critério de Risco

**b. Segurança na Aplicação**

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Verificar se o software e/ou componentes utilizados ainda são suportados	Verificar se a versão de todos os softwares utilizados na sua organização ainda é suportada pelo desenvolvedor ou adequadamente protegida com base nas recomendações de segurança do desenvolvedor.	OBRIGATÓRIO		
Ambientes de Sistemas separados de “Produção” e “Não produção”	Manter ambientes separados em sistemas de produção e não produção. Os desenvolvedores não devem ter acesso não monitorado aos ambientes de produção.	OBRIGATÓRIO		
Anonimização de Dados	Em ambientes Não Produção os dados sensíveis e pessoais devem ser anonimizado.	OBRIGATÓRIO		

**c. Controle de sessão de usuário**

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Encerramento de sessão por inatividade	Bloquear/encerrar a sessão do usuário automaticamente após um período de inatividade. Este tempo não deve ser superior a 30 minutos. - Após o bloqueio ou encerramento todas as informações em tela não deverão mais estar visíveis, sendo necessária uma nova autenticação para a retomada da atividade. - Não permitir a qualquer usuário do sistema desativar ou desabilitar esses controles	OBRIGATÓRIO		Abrangendo aplicações WEB e avaliação de APP
Segurança contra roubo de sessão de usuário	A sessão de comunicação deve possuir controles de segurança a fim de não permitir o roubo da sessão do usuário.	OBRIGATÓRIO		Avaliar na próxima reunião os cenários dessas ameaças

d. Autorização e controle de acesso - Administradores

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Concessão de autorizações	Garantir que haja ao menos um usuário responsável pela concessão de autorização e pelo controle de acesso aos recursos de acordo com o escopo de atuação, a política organizacional e legislação. <b>Nota:</b> Preferencialmente um usuário e suplente dedicado a esta atividade.	OBRIGATÓRIO		

e. Auditoria

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Trilhas e logs de auditoria	<p>Ao sistemas e demais recursos devem registrar/permitir consulta aos seguintes logs/trilhas de auditoria:</p> <p><b><u>Acessos bem-sucedidos:</u></b></p> <ul style="list-style-type: none"> <li>Identificador do usuário (login, ID processo, endereço IP, etc.); <ul style="list-style-type: none"> <li>Data e hora dos eventos / Tipo dos eventos;</li> <li>Arquivos / parâmetros acessados/alterados; <ul style="list-style-type: none"> <li>Programa utilizado.</li> </ul> </li> </ul> </li> </ul> <p><b><u>Tentativas de acesso malsucedidas:</u></b></p> <ul style="list-style-type: none"> <li>Identificador do usuário (login, ID processo, endereço IP, etc.); <ul style="list-style-type: none"> <li>Data e hora dos eventos / Ações rejeitadas ou falhas;</li> <li>Violações de políticas de acesso e notificações.</li> </ul> </li> </ul> <p><b><u>Operações privilegiadas:</u></b></p> <ul style="list-style-type: none"> <li>Uso de contas privilegiadas;</li> <li>Inicialização e finalização do sistema;</li> <li>Instalação e desinstalação de dispositivos de I/O.</li> </ul> <p><b><u>Alertas e falhas de sistemas:</u></b></p> <ul style="list-style-type: none"> <li>Alertas ou mensagens de consoles;</li> <li>Alarmes de gerenciamento de rede;</li> <li>Alarmes de sistemas de controle de acesso.</li> </ul> <p><b><u>Desempenho:</u></b></p> <ul style="list-style-type: none"> <li>Utilização do processador / disco / utilização da memória / Utilização da rede.</li> </ul> <p><b>Tempo de retenção desses dados:</b> 30 dias no mínimo</p> <p><b>Garantir a sincronização de Hora (NTP)</b></p>	OBRIGATÓRIO		
Proteção e armazenamento dos registros	Os registros de monitoração devem estar armazenados em servidores dedicados e em rede segregada, além de serem protegidos de modificações não autorizadas por meio de mecanismos de controle de acesso.	OBRIGATÓRIO		

### 3. Infraestrutura

#### a. Disponibilidade (Backup e Restore)

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Cópia de Segurança (Backup)	Garantir que os sistemas da organização sejam submetidos ao processo de backup completo, por meio de imagens, como exemplo, para permitir a recuperação rápida de um ambiente.	OBRIGATÓRIO		
Verificação de integridade na recuperação de dados	Testar a integridade dos dados em mídia de backup regularmente executando um processo de restauração de dados para garantir que o backup esteja funcionando corretamente.	OBRIGATÓRIO		

#### b. Inventário de ativos

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Inventário de Hardware	Manter um inventário atualizado de todos os ativos de tecnologia com o potencial de armazenar ou processar informações. Este inventário deve incluir todos os ativos de hardware, conectados ou não à rede da organização.	OBRIGATÓRIO		
Inventário de Software	Manter um inventário preciso e atualizado de todos os ativos de tecnologia com o potencial de armazenar ou processar informações. Este inventário deve incluir todos os ativos de hardware, conectados ou não à rede da organização.  Manter a lista atualizada de todos os softwares autorizados que são necessários na organização para qualquer propósito de negócio ou qualquer sistemas de negócio.	OBRIGATÓRIO		

**c. Gerenciamento contínuo de vulnerabilidades**

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Uso de Ferramentas de Verificação de Vulnerabilidade	<p>Implementar processo de verificação periódica de ativos para garantir o levantamento das vulnerabilidades de segurança disponibilizadas pelos fornecedores. O processo deve incluir as seguintes ações:</p> <ul style="list-style-type: none"> <li>• Identificação de criticidade</li> <li>• Plano de ação de execução</li> <li>• Caso não seja possível implementar remediação, plano de ação</li> </ul>	OBRIGATÓRIO		
Processo de Atualizações	Definir e executar processo de aplicações das correções identificadas no levantamento de vulnerabilidades.	OBRIGATÓRIO		

**d. Proteção de Dados**

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Proteção de e-mail	Bloquear todo conteúdo potencialmente perigoso de emails endereçados a organização, analisando o conteúdo das mensagens a fim de mitigar ameaças (AntiSpam).	OBRIGATÓRIO		
Proteção Web	Aplicar filtros de URL baseados em rede que limitem a capacidade do sistema de se conectar a sites não aprovados pela organização. Essa filtragem deve ser aplicada para cada um dos sistemas da organização, estejam eles fisicamente nas instalações de uma organização ou não Inclusive em redes WI-FI	OBRIGATÓRIO		
Defesas contra Malware	<p>Utilizar software anti-malware gerenciável para monitorar e defender continuamente cada uma das estações de trabalho e servidores da organização.</p> <p>Recomenda-se o uso de soluções que permitam a solução em casos Zero Day e permitido para uso corporativo.</p>	OBRIGATÓRIO		

**e. Defesa de Fronteira / Perímetro**

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Uso de tecnologia para proteção de tráfego de rede	Fazer uso de tecnologias para proteção de tráfego WAN. Por exemplo: IPS, DDOS.	OBRIGATÓRIO		
Controle de acesso físico a rede	Utilizar solução de controle de acesso físico em rede LAN. Por exemplo: NAC	RECOMENDADO		
Uso de Firewall	Negar comunicações com endereços IP da Internet mal-intencionados ou não usados. Limitar o acesso apenas aos intervalos de endereços IP confiáveis e necessários em cada um dos limites de rede da organização.  Negar a comunicação por portas TCP ou UDP não autorizadas ou tráfego de aplicativos para garantir que apenas protocolos autorizados tenham permissão para cruzar o limite da rede dentro ou fora de cada um dos limites da rede da organização.	OBRIGATÓRIO		
Implantar Firewalls de Aplicativos da Web (WAFs)	Proteger aplicativos da Web implantando firewalls de aplicativos da Web (WAFs) que inspecionam todo o tráfego que flui para o aplicativo da Web em busca de ataques comuns. Para aplicativos que não são baseados na Web, firewalls de aplicativos específicos devem ser implantados se tais ferramentas estiverem disponíveis para o tipo de aplicativo fornecido. Se o tráfego for criptografado, o dispositivo deverá ficar atrás da criptografia ou ser capaz de descriptografar o tráfego antes da análise. Se nenhuma opção for apropriada, um firewall de aplicativo da Web baseado em host deverá ser implantado.	RECOMENDADO		

**f. Implementar um programa de conscientização e treinamento em Segurança da Informação**

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Implementar um programa de conscientização e treinamento em Segurança da Informação e Proteção de Dados	Criar um programa de conscientização de segurança para todos afim de assegurar que compreendam e exibam os comportamentos e habilidades necessários para ajudar a garantir a segurança da organização. O programa de conscientização de segurança da organização deve ser comunicado de maneira contínua e envolvente. Inclusive terceiros.	OBRIGATÓRIO		
Treinamento na identificação de ataques de engenharia social	Treinar o colaboradores sobre como identificar diferentes formas de ataques de engenharia social, como phishing, golpes de telefone e chamadas de representação.	OBRIGATÓRIO		

**g. Realização de testes de invasão**

REQUISITO	CONFORMIDADE	USO	INÍCIO	OBS
Estabelecer um programa de teste de invasão	Realizar testes de invasão externos e internos regulares para identificar vulnerabilidades e vetores de ataque que podem ser usados para explorar sistemas corporativos com êxito.	OBRIGATÓRIO		No proximo forum, em marco, será definido um novo escopo e periodicidade