Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

Política da Segurança da Informação

1. OBJETIVO

Este documento tem como objetivo definir uma Política de Segurança para a Ass Beneficente São João da Reserva – Hospital da Reserva "HdR", especialmente quanto à proteção de seus ativos, estabelecendo procedimentos e recomendações visando preservar o patrimônio e a informação no que se refere aos setores computacionais, comunicação e a reputação da Entidade.

Este documento tem como objetivo definir uma Política de Segurança para o HdR, especialmente quanto à proteção de seus ativos, estabelecendo procedimentos e recomendações visando preservar o patrimônio e a informação e em conformidade a lei 13.709 (Lei Geral de Proteção de Dados), no que se refere à Dados Pessoais, setores computacionais, comunicação e a reputação da Entidade.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

2. ABRANGÊNCIA DA SEGURANÇA

Esta política tem abrangência em todo o HdR a qual se caracterizará em manter a autenticidade, confidencialidade, disponibilidade e integridade.
A política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da Entidade poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

3. PRINCÍPIOS DA POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional é de propriedade do HdR.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços, conforme avaliação técnica da área de TI.

O HdR, por meio da Gestão de Sistemas, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações.

4. REQUISITOS DA SEGURANÇA DA INFORMAÇÃO

A política da segurança da informação deverá ser comunicada a todos os colaboradores do HdR tem com o objetivo de manter a uniformidade da informação e para que ela seja cumprida dentro e fora da Entidade.

As Políticas e Normas deverão ser revisadas periodicamente sempre que algum evento ou fato novo aconteça.

Deverá constar em todos os contratos do HdR o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição obrigatória para que possa ser concedido o acesso aos ativos de informação da instituição. As revisões contratuais tem previsão de iniciar em 01/08/2021 pelo Escritório Kinsel Adv.

Todo o incidente que afete a segurança da informação deverá ser reportado imediatamente à Gestão da Entidade, caso contrário poderá ser penalizado.

Um plano de contingência e continuidade de negócio dos principais sistemas e serviços deverá ser implantado e testado, pelo menos uma vez ao ano, reduzindo riscos de perdas de informação.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

Todos os requisitos de segurança da informação deverão ser identificados na fase de levantamento de escopo de um projeto ou sistema e, justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico e nos sistemas corporativos da Entidade. **Orientando a todos integrantes da equipe do HdR a usar apenas os meios de comunicações oficiais, telefones, e-mails assim evitando o uso dos pessoais.**

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes.

O HdR exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta política de segurança da informação será implementada em todo o HdR, utilizando meios específicos e obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na Entidade, bem como de vínculo empregatício ou de prestação de serviço.

O não cumprimento dos requisitos previstos nesta política e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

5. DAS RESPONSABILIDADES ESPECÍFICAS

a) Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da Entidade. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao HdR e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Desligamento: O colaborador que for desligado deverá devolver todos os equipamentos pertencentes a Entidade e, caso possua arquivos particulares, deverá fornecer uma mídia para cópia acompanhado de um colaborador do setor de TI.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

b) Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação. Exigir dos colaboradores a assinatura do **Termo de Compromisso e Ciência**, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Entidade. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

6. DA ÁREA DA SEGURANÇA DA INFORMAÇÃO

6.1. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, pelas Normas de Segurança da Informação complementares.

6.2. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido mediante a autorização do proprietário da informação para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

6.3. Segregar as funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

6.4. Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

6.5. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Entidade.

6.6. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

6.7. Implantar controles que gerem registros auditáveis para retirada, transporte de mídias das informações ou transferência de dados custodiadas pela TI, nos ambientes totalmente controlados por ela.

6.8. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário, conforme o processo de novos colaboradores.

6.9. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

6.10. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

6.11. Proteger continuamente todos os ativos de informação da Entidade contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

6.12. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Entidade em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

6.13. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Entidade.

6.14. Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

6.15. Realizar em tempo hábil, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Entidade, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Entidade.

6.16. Monitorar o ambiente de TI, gerando indicadores e históricos de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, entre outros);

- atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

6.17. Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

6.18. Propor e apoiar iniciativas que visem à segurança dos ativos de informação na Entidade.
Publicar e atualizar as versões da Política da Segurança da Informação.

6.19. Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio Do HdR, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

6.20. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

6.21. Analisar criticamente incidentes em conjunto com a Gestão da Entidade.

7. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política, o HdR poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial;
- realizar, a qualquer tempo, inspeção física nas máquinas de propriedade da Entidade.
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

8. CORREIO ELETRÔNICO

O uso do correio eletrônico do HdR é para fins corporativos e relacionados às atividades do colaborador / usuário dentro da Entidade. A utilização para fins pessoais é permitida desde que feita com bom senso, não prejudique a instituição e que não cause impacto no consumo de rede.
Somente é permitida aos colaboradores o uso do e-mail corporativo para tratamento de assuntos da Entidade, não permitindo o uso de e-mails pessoais ou outras plataformas não aprovadas

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

previamente e ou de nível e pertencimento pessoal, assim garantido a memória e registros da entidade.

9. INTERNET

O uso da internet do HdR é para fins corporativos e pessoais, sempre visando o bom senso na sua utilização.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet da Entidade está sujeita a divulgação e auditoria.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Entidade, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Entidade cooperará ativamente com as autoridades competentes.

Os colaboradores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades da Entidade e deverão providenciar, o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Gestão da Segurança da Informação.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Sistemas.

Os colaboradores não poderão em hipótese alguma utilizar os recursos do HdR para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

essas categorias. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload de qualquer software licenciado do HdR ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos do HdR para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Utorrent, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) são liberados a todos os colaboradores.

Não é permitido acesso a sites de proxy, ou qualquer meio para contornar as medidas de segurança para acesso a sites.

O acesso remoto nas estações de trabalho oriundos do setor de TI deverão sempre ser autorizados pelo usuário, não permitindo acesso automatizado sem prévia autorização.

10. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante ao HdR e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro. (Art. 307 – falsa identidade).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o HdR e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

Os usuários deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

As senhas não devem ser anotadas, armazenadas ou compartilhadas em arquivos eletrônicos (Word, Excel etc.) ou outros meios de comunicação, compreensíveis por linguagem humana (não criptografados).(Política de Mesa limpa)

Após 5 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a TI da unidade e posteriormente caso necessário com a TI do HdR ou setor responsável.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 90 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá, imediatamente, comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

As senhas de prestadores de serviço devem ter uma data de expiração previamente acordada com o solicitante do acesso, essa deverá ser definida na criação do acesso.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer à área técnica responsável para cadastrar uma nova.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

11. COMPUTADORES E RECURSOS TECNOLOGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade do HdR, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Entidade, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do HdR.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação e depois de testes com resultados esperados e sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro no sistema de chamados.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Entidade (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem aviso prévio.

Documentos imprescindíveis para as atividades dos colaboradores da Entidade deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), **não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário**.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Todos os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela área de TI;
- **Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;**

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do HdR;
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pela Entidade devem ter imediatamente suas senhas padrões (default) alteradas;
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso;
- No descarte de qualquer equipamento deve ser realizada uma formatação utilizando ferramenta específica para limpeza garantindo a não recuperação da informação.

Situações em que é proibido o uso de computadores e recursos tecnológicos da Entidade:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança;
- Utilização dos recursos da Entidade para ganhos pessoais;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

12. DISPOSITIVOS MÓVEIS

A utilização de equipamentos móveis como notebooks, smartphones e pendrives é permitida na Entidade com algumas ressalvas:

- Somente notebooks da Entidade poderão ser conectados a cabos de rede ou rede sem fio corporativa.
- A utilização de notebooks e smartphones pessoais está condicionada a conexão somente na rede convidado.
- A utilização de pendrives deve ser somente para fins corporativos e com conhecimento do gestor da área.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

- **É orientado ao colaborador a usar apenas meios de comunicação oficiais corporativos para comunicação com publico em geral.**
- Não é permitido a utilização de equipamentos pessoais na rede da Entidade, salvo exceções onde há uma aprovação prévia da Gestão da Entidade com ciência dos riscos envolvidos.
- **A utilização de aplicativo de troca de mensagens como WhatsApp, Skype, Telegram entre outros deve ser utilizado com consciência, evitando ao máximo, o contato em horários fora do turno de trabalho. Evitando dar informações sensíveis de clientes/pacientes a não ser que pelos meios legais.**

13. DATACENTER

O acesso ao Datacenter “CPD” somente deverá ser feito por autorização da gestão.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas e, assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade.

O acesso por pessoas não autorizadas ao Datacenter, por meio de chave, apenas em emergências, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial .

Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse da direção.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.
Não é permitida a entrada de nenhum tipo de alimento, bebida ou inflamável.
A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

No caso de desligamento de colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

14. BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

Na ausência de backup em fita, os dados deverão ser direcionados para um diretório na nuvem utilizando uma conta corporativa, conforme documento de Plano de Backup.
Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Associação Beneficente São João da Reserva

São João da Reserva – 6° Distrito – 96170-000
SÃO LOURENÇO DO SUL – RS
Fone: 533251 7920– Email: centrosaudereserva@hotmail.com
CNPJ n° 90.938.713/0001-93

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 90 dias, de acordo com a criticidade do backup.

15. DA SOLICITAÇÃO DE INFORMAÇÕES

Será designado Encarregado na instituição para informações e ou retiradas de dados, sempre quando solicitado formalmente/oficialmente pelo próprio paciente e ou representante legal, de forma presencial e ou por meio dos endereços eletrônicos divulgados no site da instituição

> III - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
>
> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. **§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador**. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A Política de Segurança da Informação será divulgada no site da instituição, assim tornando publico as políticas de segurança.

Serão respeitados os chamados “Dados Sensíveis”

> v I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> Exceto” VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;”

16. DISPOSIÇÕES FINAIS

A segurança da informação é parte fundamental de uma instituição e deve fazer parte da cultura da Entidade, sendo revisitada diariamente nas suas ações.
Os avanços tecnológicos facilitam atividades diárias, mas também expõe a riscos virtuais, dessa forma manter sistemas, políticas e procedimentos atualizados é uma forma de manter o ambiente mais seguro.