POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Hospital São Paulo
Rua Nívio Castelano, 1271 – Centro
Lagoa Vermelha/RS
CEP: 95300-000
(54) 3358 8700

Hospital São José
Av. Marechal Floriano, 801 – Centro
São José do Ouro/RS
CEP: 99870-000
(54) 3352 4750

Fundação Araucária
Av. Marechal Floriano, 811 – Centro
São José do Ouro/RS
CEP: 99870-000
(54) 3352 4700

SUMÁRIO

1. INTRODUÇÃO

A Política de Segurança da Informação ("PSI") tem por objetivo estabelecer regras sobre como todos os ativos de informação, em meio físico e digital, devem ser tratados, atendendo às boas práticas de segurança e à Lei Geral de Proteção de Dados (LGPD).

A Política de Segurança da Informação visa preservar a confiabilidade, integridade e disponibilidade das informações para a resolução de problemas e tomada de decisão.

2. ALCANCE

Esta Política é aplicável a todos os funcionários, titulares e usuários que se relacionem com a Fundação Araucária e suas filiais, abrangendo todas as suas unidades de atendimento, em todos os processos que envolvam o tratamento de dados pessoais.

3. DIRETRIZES GERAIS

No tratamento de todas as informações da Fundação Araucária e suas filiais, todos funcionários, além da legislaçãoe demais políticas e normas adotadas, deverão ter em vista, sobretudo, preservar a:

- Confidencialidade: Garantir que a informação, sempre que necessário, esteja disponível apenas aos funcionários vinculados a Fundação Araucária e suas filiais e nos procedimentos operacionais que a informação esteja sempre protegida do conhecimento de funcionários não autorizados;

- Integridade: Garantir a exatidão, integridade, revisão e confidencialidade dos ativos de Informação;

- Disponibilidade: Garantir que os ativos de Informação e recursos de acesso estejam acessíveis sempre que necessário aos funcionários vinculados a Fundação Araucária e suas filiais.

4. ATIVOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Todos os ativos de tecnologia da informação e comunicação (ATIC's) da Fundação Araucária e suas filiais, como e-mail, telefone, internet, devem ser utilizados exclusivamente

para o desempenho de atividades relacionadas à operação da organização. Jamais poderão ser utilizados para fins indevidos, como:

- Enviar mensagens com ofensas ou que conflitem com os interesses da Fundação Araucária e suas filiais;
- Enviar mensagens com informações da Fundação Araucária e suas filiais a terceiros estranhos à organização, sem que haja justificativa e autorização para tanto;
- Enviar mensagens utilizando assinatura ou endereço falso, com fins de falsificar ou adulterar o conteúdo da mensagem, fazendo-se passar por outra pessoa;
- Enviar mensagens para múltiplos destinatários, salvo nos casos em que o conteúdo do e-mail seja relacionado aos legítimos interesses da Fundação Araucária e suas filiais e mediante prévia autorização do gestor do setor;
- Enviar ameaças eletrônicas como: spam, vírus e outros malwares ou com arquivos com códigos executáveis (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que apresente riscos à segurança;
- Acessar ou tentar acessar conta de outra pessoa sem autorização;
- Acessar ou tentar acessar informações confidenciais sem autorização ou monitorar de forma secreta outros funcionários;

O funcionário não deverá abrir links e documentos recebidos de fontes desconhecidas. Caso desconfie de qualquer material recebido, a mensagem não deverá ser aberta e a área de Tecnologia da Informação deverá ser informada imediatamente.

É vedada a utilização dos ativos de tecnologia da informação e comunicação para acessar, armazenar, divulgar ou propagar qualquer material ligado à pornografia, pedofilia, jogos, racismo, homofobia ou qualquer outro conteúdo ilícito.

Documentos desenvolvidos por funcionários são de propriedade da Fundação Araucária e filiais, ressalvados em casos expressamente regulados por instrumentos contratuais ou não- contratuais por escrito.

Apenas funcionários devidamente autorizados a falar em nome do Fundação Araucária e suas filiais poderão manifestar-se, seja por e-mail, entrevista on-line, documento físico, ligação telefônica.

5. LOGINS E SENHAS

As credenciais (crachás, logins, senhas e demais credenciais de acesso a ambientes físicos e digitais) são pessoais e intransferíveis e não devem ser compartilhadas com terceiros.

É obrigação dos funcionários manter o sigilo de logins e senhas de acesso aos sistemas da Fundação Araucária e suas filiais, sob pena de incorrer em sanções disciplinares solidariamente com oterceiro com o qual tenha compartilhado suas credenciais; o uso de dispositivos e/ou senhasde identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

As senhas utilizadas em sistemas computacionais da Fundação Araucária e suas filiais, deverão ser diversas de senhas particulares.

Logins e senhas não deverão ser transmitidos por e-mail, chamados ou aplicativos de mensagens (ex. SMS, WhatsApp, Skype, Telegram etc.) e jamais devem ser deixados expostos em qualquer forma de anotação, como agenda, blocos de notas, papéis adesivos, entre outros do tipo.

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

As senhas deverão seguir os seguintes pré-requisitos: tamanho mínimo de 6 caracteres; existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais; não devem ser baseadas em informações pessoais de fácil dedução.

6. ACESSOS

A extensão dos acessos concedidos aos funcionários será definida de acordo com perfis de acesso, correspondentes à função desempenhada pelo funcionário interno ou externo, os quais serão detalhados na matriz de acessos a ser gerida pela área de Tecnologia da Informação.

Acessos que extrapolam as permissões definidas para o perfil previsto na matriz de acessos serão considerados privilegiados e somente poderão ser concedidos mediante avaliação de necessidade concreta e mediante solicitação do gestor da área.

A Gerência de Recursos Humanos ou os respectivos gerentes das áreas deverão comunicar, no menor tempo possível, à Gerência de Informática sobre a necessidade de

concessão, alteração ou cancelamento de acessos de funcionários aos sistemas de informação, de modo que ninguém possua acessos incompatíveis com sua função.

O funcionário não deverá acessar pastas, arquivos, sistemas e qualquer conteúdo que não seja necessário ao desenvolvimento de suas atividades ou após o término de seu relacionamento com a Fundação Araucária e suas filiais. Caso identifique que possui acesso a conteúdo desnecessário, comunique imediatamente à sua gerência ou a Gerência de Informática para que seja realizado o ajuste de seu acesso.

Após o encerramento de seu relacionamento, nenhum funcionário, titular ou usuário, deverá manter qualquer tipo de acesso aos ativos de informação Fundação Araucária e suas filiais, devendo cessar imediatamente o uso das credenciais às quais tinha acesso durante o relacionamento contratual.

Dados pessoais referentes à saúde de funcionários serão acessados exclusivamente pela Gerência de Recursos Humanos. Quando necessário, a Gerência de Recursos Humanos informará os reflexos de tais informações aos gestores competentes, sem, contudo, revelar os detalhes dos dados em si.

6 SEGURANÇA NAS ESTAÇÕES DE TRABALHO

Ao se ausentar de sua mesa o funcionário deverá bloquear a tela ou guardar os dispositivos, bem como guardar todos os documentos que não for levar consigo, preferencialmente em sua gaveta ou armário, trancando e levando a chave, de modo que não seja possível a outras pessoas visualizarem informações expostas na estação de trabalhoe/ou em seu monitor.

Documentos físicos devem ser armazenados de forma segura, em arquivo próprio com acesso restrito, não devendo ser deixados em exposição na estação de trabalho ou outros ambientes na ausência do funcionário.

O funcionário deve evitar a impressão de documentos ou informações, dando preferência para a leitura diretamente nas telas dos dispositivos. Caso seja necessária a impressão, o documento deverá ser coletado imediatamente na impressora.

Os armários, gavetas ou arquivos, devem sempre permanecer fechados e as chaves nunca deverão ser deixadas na fechadura, caso possua.

Ao término do expediente os ambientes devem ser trancados com chave, a qual ficará sob responsabilidade do gestor da área ou de quem ele determinar.

Informações confidenciais da Fundação Araucária e suas filiais não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel etc.) sem as devidas autorizações e proteções.

Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais).

Somente softwares homologados pela Fundação Araucária e suas filiais podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia da Informação.

Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio.

É vedada a abertura de computadores para qualquer tipo de reparo pelos funcionários. Caso seja necessário, o reparo deverá ser feito pela equipe da Gerência de Informática.

Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede interna da Fundação Araucária e suas filiais, mediante autorização do chefe imediato via memorando e prévio cadastro e liberação do setor de Tecnologia da Informação.

É proibida a impressão de documentos de cunho pessoal e/ou ilegal.

A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica da Gerência de Informática.

O gestor de cada gerência ou de cada setor será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões excessivas;

As impressoras devem estar ligadas na energia através dos seus transformadores e serão proibidas intervenções desta natureza por parte de qualquer funcionário que não seja do setor de Gerência de Informática.

8 BACKUP

Os arquivos inerentes à Fundação Araucária e suas filiais, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor (sendo ela pública ou privada), localizada no servidor de arquivos, para a garantia de backup destes documentos. É

terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais.

Todo sistema ou informação relevante para a operação dos negócios da Fundação Araucária e suas filiais, deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da entidade.

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de funcionários vinculados à Fundação Araucária e suas filiais ou processos aos sistemas de informática.

Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento.

Na situação de erro de backup e/ou restauração é necessário que seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse *backup*, eles deverão ser executados apenas mediante justificativa de necessidade.

9 MONITORAMENTO E SEGURANÇA

Todos funcionários devem ter ciência de que o uso dos ativos de tecnologia da informação e comunicação, especialmente a internet, podem ser monitorados e os registros obtidos podem servir de evidência para fins jurídicos e aplicação de medidas disciplinares.

Neste sentido, com o único fim de assegurar o cumprimento das diretrizes presentes nesta PSI, a Fundação Araucária e suas filiais poderão:

- Monitorar os ativos de informação e analisar o uso deles. A informação gerada por esses sistemas poderá ser usada para identificar funcionários e respectivos acessos efetuados, bem como material manipulado;
- Realizar, sem aviso prévio, a qualquer tempo a inspeção física ou auditoria nos ativos de seu uso;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

10 INCIDENTES DE SEGURANÇA

Um incidente é qualquer evento que resulte ou que tenha possibilidade de resultar em perdas ou danos às informações e dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento de ativos.

Caso identifique algum incidente, o funcionário deverá no prazo máximo de 24 horas, comunicar a Gerência de Informática.

A comunicação deverá conter data, hora, local, possíveis causas, ativos comprometidos, dentre outros que o funcionário julgar necessário;

No tratamento de incidentes a área de Tecnologia da Informação ou o Encarregado pelo Tratamento de Dados tratará a ameaça, risco ou incidente por meio dos seguintes passos:

- Elaborar relatório contendo o máximo de informações possível, como descrição do ocorrido, áreas afetadas, possíveis causas, natureza, categoria e quantidade de dados pessoais ou sistemas afetados, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis para os titulares e para a Fundação Araucária e suas filiais;

- Proceder com adoção de medidas, isolamento de danos, caso seja necessário paralisar áreas e sistemas comprometidos;

- Em se tratando de efetivo incidente e verificados riscos ou danos relevantes aos Titulares de dados, a comunicação aos Titulares deverá ser realizada, necessariamente, com apoio da Direção da Fundação Araucária e suas filiais, que avaliará a forma mais adequada de abordagem das pessoas afetadas, podendo contar com agentes internos ou externos de marketing;

- Evidenciar e comprovar as possíveis causas da ameaça, risco ou incidente;

- Realizar o tratamento em si da ameaça, risco ou incidente, analisando todas aspossíveis soluções para resolução;

- Garantir que não haja outras ameaças, riscos ou incidente relacionados ao casodescrito na comunicação;

- Realizado o tratamento com a adoção de todas as medidas técnicas e administrativas remeter à Direção para a validação.

11 COMUNICAÇÃO

Sempre que se deparar com um risco ou efetiva violação de segurança aos ambientes de informação físicos e digitais da Fundação Araucária e suas filiais, o funcionário, deverá comunicar pelo e-mail thiago@araucaria.org.br ou diretamente ao seu gestor imediato, reportando o maior número possível de informações sobre o fato.

12 SANÇÕES

As violações ou infrações, ainda que por omissão ou mera tentativa não consumada, desta Política e toda e qualquer diretriz ou norma publicada e veiculada pela Fundação Araucária e suas filiais, poderão ensejar a aplicação de penalidades previstas.

As violações que impliquem em atividades ilegais, ou que possam incorrer em riscos aos titulares de Dados Pessoais, ou dano à Fundação Araucária e suas filiais, ensejarão a responsabilidade aos envolvidos pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

13 DISPOSIÇÕES FINAIS

Essa política entra em vigor a partir da sua publicação.