POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

BARBALHA-CE
2025

1. OBJETIVO

Estabelecer diretrizes e atribuir responsabilidades para o tratamento, a proteção e a manutenção da confidencialidade, a integridade e a disponibilidade das informações de propriedade da Fundação Otília Correia, e determinar sanções pelo uso indevido delas, visando prevenir danos aos negócios da Fundação.

2. ASPECTOS GERAIS

2.1. Toda informação gerada, armazenada, processada e administrada pela Fundação Otília Correia Saraiva é de sua propriedade, estando regulamentada por esta Política de Segurança da Informação e sujeita a auditoria e a monitoramento de uso.

2.2. Os processos de negócio deverão implementar registros que possibilitem a análise e a rastreabilidade das informações. Através destes registros será possível identificar incidentes e violações, os quais possibilitam trilhas para auditoria e análise forense.

2.3. Toda informação que deva ser descartada, o será de modo seguro, de forma que não seja possível sua recuperação ou reutilização.

2.4. O acesso às dependências da Fundação Otília Correia Saraiva será controlado, registrado e segmentado por perímetros. Todo profissional prestador de serviço ou visitante será identificado e seu acesso será restrito ao ambiente determinado. Cada visitante receberá um crachá identificado com “Visitante”.

2.5. Empregados e contratados, quando deixarem a Fundação Otília Correia Saraiva ou mudarem suas responsabilidades, perderão seus atuais privilégios e acessos concedidos, devolvendo os equipamentos sob sua tutela.

2.6. Todo novo processo deverá ser homologado pelo gestor responsável e pelo responsável pela segurança da informação.

2.7. A divulgação ou o uso indevido das informações da Fundação Otília Correia Saraiva, bem como o descumprimento/violação da presente política de segurança da informação poderá implicar em sanções de caráter disciplinar previstos no item “15. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO” deste instrumento, sem prejuízo de eventual apuração de responsabilidade cível/criminal do ato cometido.

3. RESPONSABILIDADES

3.1. Diretoria da Fundação Otília Correia

- Aprovar o Plano de Segurança da Informação da Fundação Otília Correia Saraiva.

3.2. Equipe de Tecnologia da Informação e Comitê de Privacidade

- Determinar as ações pertinentes a Segurança da Informação.
- Apoiar a deliberação sobre os normativos de segurança da informação desenvolvidos.
- Avaliar a gestão da segurança da informação na Fundação Otília Correia Saraiva.
- Requisitar auditoria nos processos envolvidos com a Política de Segurança da Informação, no intuito de aferir o nível de segurança dos processos de gestão da Segurança da Informação, investigar situações de crise, violações de segurança ou não conformidades.
- Definir programas destinados à conscientização e a capacitação dos recursos humanos que serão utilizados na consecução dos objetivos da Política de Segurança da Informação.
- Deliberar sobre sistemas de informação e operação de T.I. no âmbito da Segurança da Informação.
- Conhecer e disseminar conceitos e ações realizados por empresas consideradas referenciais de mercado.

3.3. Recursos Humanos

- Apoiar os projetos de disseminação da Cultura de Segurança da Informação junto aos colaboradores.

3.4. Usuário da informação

- Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Sugerir, ao responsável pela segurança da informação, melhorias e mudanças necessárias, visando manter a Política de Segurança da Informação atualizada e aderente às necessidades da Fundação Otília Correia Saraiva.
- Não fazer uso indevido das informações pertencentes à Fundação Otília Correia Saraiva a que possui e manter a confidencialidade delas.
- Comunicar imediatamente ao comitê de segurança da informação quaisquer descumprimentos e/ou violação das diretrizes descritas nesta política, através dos e-mails: ti@focs.org.br / privacidade@focs.org.br
- Proteger as informações pertencentes à Fundação Otília Correia Saraiva contra divulgações, modificações, destruições e acessos não autorizados.

4. SOLUÇÕES DE CONFLITOS

4.1. Quaisquer situações decorrentes das informações contidas nessa Política ou em outra derivada desta, que possam gerar conflitos internos ou externos à Fundação Otília Correia Saraiva, deverão ser imediatamente notificadas ao responsável pela Segurança da Informação para que as ações corretivas necessárias sejam tomadas.

5. CONTAS DE ACESSO

5.1 É de responsabilidade de cada colaborador a memorização e a proteção de seu login e senha, devendo-se evitar anotações em papéis ou outros meios inseguros.

5.2 A senha deverá conter no mínimo 8 caracteres, letras maiúsculas e minúsculas, números e caracteres especiais. A cada 6 (seis) meses colaborador receberá uma solicitação em sua estação de trabalho para a alteração de sua senha.

5.3 Nas situações em que o colaborador for desligado da empresa, o gestor imediato deverá solicitar o bloqueio definitivo de todos os seus acessos através do Neovero Sistemas ao setor de T.I.

6. USO DA INTERNET

6.1 O colaborador tem a obrigação de utilizar a internet de maneira profissional, ética e responsável e voltado às atividades de trabalho.

6.2 O acesso à internet poderá ser monitorado através de recursos tecnológicos sempre que a Fundação Otília Correia Saraiva julgar necessário, bem como todos os registros de acessos poderão ser armazenados.

6.3 É expressamente proibido o acesso à internet com o intuito de violar leis e regras brasileiras ou de outro país. A utilização deste recurso para atividades ilegais é motivo de sansões administrativas e/ou criminais se este for o caso.

7. USO DO E-MAIL

7.1 A Fundação Otília Correia Saraiva concede ao colaborador uma conta de e-mail corporativo. Este recurso deverá ser utilizado de modo responsável para fins estritamente profissionais.

É de responsabilidade do colaborador todo e qualquer conteúdo enviado e recebido através desta ferramenta.

7.2 É proibido o envio de mensagens contendo informações sigilosas ou de propriedade da Fundação Otília Correia Saraiva para destinatários não autorizados.

7.3 É proibido (a): a) o envio de e-mail com materiais que caracterize a divulgação, o incentivo ou a prática de atos ilícitos; b) o cadastro do e-mail corporativo em sites de compra coletiva, relacionamentos ou outros de mesma natureza; c) a utilização do e-mail corporativo para envio de mensagens do tipo corrente.

7.4 Caso ocorra o recebimento de links ou arquivos anexados oriundos de remetentes desconhecidos ou com características suspeitas, sua abertura ou acesso somente poderá ocorrer após prévia análise pela área de Tecnologia da Informação.

8. USO DO WHATSAPP

8.1 É proibido o uso do WhatsApp pessoal para fins de compartilhamento interno ou externo de dados pessoais e de informações confidenciais da empresa.

8.2 A Fundação Otília Correia Saraiva possui contas de WhatsApp corporativos em em setores específicos para realização de suas atividades.

8.2.1 Fica proibido o compartilhamento de dados pessoais ou confidenciais externamente ou fora do contexto da finalidade do uso da informação pré-determinada pela Fundação Otília Correia Saraiva.

8.2.3 As exceções ao uso de WhatsApp pessoal devem ser autorizadas pela Direção da Fundação Otília Correia Saraiva e comunicadas ao Encarregado de Proteção de Dados, sem prejuízo de apuração de responsabilidade prevista no tópico 15 em caso de uso indevido do aplicativo.

9. INSTALAÇÃO DE SOFTWARE

9.1 É proibido o uso e a instalação de softwares ilegais, não licenciados e não autorizados nos dispositivos da T.I. da Fundação Otília Correia Saraiva.

9.2 Somente a equipe da T.I. da Fundação Otília Correia Saraiva poderá instalar, remover, atualizar e substituir qualquer tipo de software nos dispositivos de T.I, tais como: computadores, notebooks, servidores, smartphones etc.

9.3 Para toda e qualquer solicitação desta natureza, o colaborador deverá abrir um chamado através do sistema Neovero com as devidas justificativas desta necessidade.

10. SISTEMAS CORPORATIVOS / ERPs

10.1 Sistemas adquiridos ou desenvolvidos internamente são de propriedade intelectual e de uso exclusivo da Fundação Otília Correia Saraiva. Atualmente, todos os sistemas são terceirizados.

10.2 É proibido o compartilhamento, a divulgação e a distribuição de informações contidas nos sistemas.

10.3 O colaborador deverá utilizar de suas credenciais para seu acesso. Para cada usuário será configurada as permissões específicas de acordo com suas atividades e perfil.

11. ACESSO REMOTO

Apenas os colaboradores da TI utilizam acesso remoto (quando solicitado).

12. MANUTENÇÃO

É proibido qualquer tipo de manutenção, troca de peças, instalações físicas, modificações, alteração de local de qualquer recurso físico de T.I. por parte do colaborador. Somente a equipe de T.I. Poderá realizar tais atividades.

13. CONTROLE DE ACESSO FÍSICO E REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

13.1 O acesso físico nas dependências dos ambientes Administrativo, TI, Recursos Humanos, Marketing e Departamento De Pessoal é realizado apenas por pessoas devidamente autorizadas, mediante crachá identificativo e/ou fardamento.

13.2 Eventual acesso de terceiros e/ou prestadores de serviços que necessitarem ter acesso físico ao local de armazenamento dos servidores será feito com o acompanhamento de pessoas da área de Tecnologia da Informação devidamente autorizadas.

14. POLÍTICA DA MESA LIMPA

14.1 Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

14.2 Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancados, quando não estiverem em uso, especialmente fora do horário do expediente.

14.3 Anotações, recados e lembretes não devem ser deixados amostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador.

14.4 Computadores pessoais e terminais de computador e impressoras não devem ser deixados “logados”, caso o usuário responsável não esteja presente. Deve ser realizado o bloqueio do computador sempre que se ausentar da sua mesa de trabalho.

14.5 Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar computador.

14.6 Informações importantes não devem ser escritas em rascunhos ou post its.

15. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

15.1 Nos casos de descumprimento/violação a essa política, em parte ou no todo, a Fundação Otília Correia Saraiva realizará uma sindicância interna para apurar os fatos e, identificada a conduta contrária, será aplicada penalidade de acordo com o grau da responsabilidade e o impacto da violação.

15.2 O descumprimento, pelo colaborador, das normas estabelecidas neste documento, seja isolado ou cumulativamente, poderá causar, de acordo com a infração cometida, as seguintes penalidades: advertência verbal, advertência escrita, suspensão ou demissão por justa causa, conforme previsão do artigo 482 da Consolidação das Leis do Trabalho.

Barbalha-CE, 01 de agosto de 2025.