POLÍTICA

DE

SEGURANÇA DA

INFORMAÇÃO

SUMÁRIO

1. INTRODUÇÃO

A Política Corporativa de Segurança da Informação (PCSI) da Organização de Saúde com Excelência e Cidadania (OSEC) é o documento corporativo que norteia o conjunto de princípios para a gestão da segurança da informação institucional, cujo compromisso é assegurar a proteção dos ativos de informações digitais e/ou físicas da Instituição para adotar medidas com o intuito de preservar a confiabilidade, a integralidade, a autenticidade, a legalidade e a disponibilidade da informação, atendendo aos requisitos legais em conformidade com a legislação vigente.

2. ABRANGÊNCIA E APLICAÇÃO

Esta política aplica-se a todos os usuários que venham a ter acesso a dados e informações da OSEC. Ou seja, colaboradores, estagiários, aprendizes, prestadores de serviço em geral, independente da denominação ou relação contratual.

3. DIRETÓRIO

A Política Corporativa de Segurança da Informação encontra-se armazenada no OneDrive, na pasta LGPD aprovada pela Mantenedora e Comitê Gestor de Privacidade e Proteção de Dados da Instituição.

4. TERMOS E DEFINIÇÕES

Para efeito da presente Política Corporativa de Segurança da Informação, aplicam-se as seguintes definições:

Ameaça: Risco ou possível perigo latente de uma situação, voluntária ou fenômeno natural, a qual é possível realizar a prevenção.

Ativo: Tudo que, de alguma forma, pode ser convertido em dinheiro.

Ativo Intangível: Ativo não monetário identificável sem substância física. Ou seja, tem valor econômico, mas não existe de fato.

Ativo Tangível: Ativo monetário e material, ou seja, tem valor econômico e existe de fato.

Antivírus: São aplicativos que detectam programas maliciosos e ameaças antes que elas sejam instaladas no dispositivo do usuário. Também são capazes de removê-los ou colocá-los em quarentena.

Autenticidade: Garantia da veracidade da autoria da informação.

Backup: Trata-se da cópia de segurança dos dados de um dispositivo de armazenamento ou sistema. Pode ser feito de forma física ou em nuvem.

Confidencialidade: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Comitê Gestor de Privacidade e Proteção de Dados (CGPPD): É composto pelas áreas das Uni dades das Mantidas OSEC as quais são responsáveis pela elaboração e atualização das diretrizese normas que abrangem os mecanismos de tratamento e proteção de dados na Instituição, bemcomo a supervisão, implementação e desempenho.

Criptografia: Mecanismo de segurança da informação em que os dados são codificados e decodificados mediante códigos de tradução designados somente para pessoas autorizadas.

Dados: Valor atribuído a uma informação.

Dados pessoais: Informação relacionada a pessoa natural identificada ou identificável. Ou seja, dados que comumente fornecemos em um cadastro, como nome, RG, CPF, gênero, data e local de nascimento, filiação, telefone, endereço residencial, cartão de crédito/débito ou dados bancários.

Dados sensíveis: Dados pessoais relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, dado genético ou biométrico.

Dispositivos móveis: Dispositivos de computação portáteis, pequenos e geralmente com acesso a aplicativos que permitem diversas funcionalidades.

E-mail: Correio eletrônico para troca de mensagens.

E-mail Corporativo: Correio eletrônico integrado à rede corporativa para troca de mensagens relacionadas às atividades profissionais.

Eliminação dos Dados: Exclusão de um dado ou de um conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Firewall: Dispositivo de segurança que monitora o tráfego de rede de entrada e saída, o qual decide permitir ou bloquear o tráfego específico de acordo com um conjunto definido de regra de segurança.

Incidente de Segurança: Qualquer evento adverso — confirmado ou sob suspeita — relacionadoà violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícitoque resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamentode dados inadequada, os quais possam ocasionar risco para os direitos e liberdades do titular dosdados pessoais.

Informação: É o resultado do processamento, manipulação e organização de dados. Trata-se deum ativo essencial para os negócios que precisa ser adequadamente protegido para que não sejaexposto a variedade de ameaças e vulnerabilidades.

Integridade: Garantia que a informação é mantida em seu estado original, visando protegê-la na guarda ou transmissão contra alterações indevidas, intencionais ou acidentais.

Internet: Conjunto de rede de computadores que fazem o compartilhamento de dados, informações e mensagens com um protocolo comum para todos os seus equipamentos.

Login: Forma de autenticação do registro de acesso à determinada base de dados contidos em e-mail, computador, celular, etc.

Logout: Ação de encerrar o acesso a determinada base de dados.

Recursos de Tecnologia da Informação: Conjunto de todas as atividades e soluções providas por recursos de computação dedicados ao armazenamento, processamento e comunicação da infor mação, bem como o modo como esses recursos são organizados sistemicamente.

Rede: Conjunto de computadores e equipamentos tecnológicos que compartilham informações.

Rede Corporativa: Sistema de transmissão de dados entre os equipamentos tecnológicos de uma mesma corporação.

Redes Sociais: Estruturas compostas por pessoas ou organizações conectadas por um, ou vários tipos de relações, que compartilham valores e objetivos em comum. Já as mídias sociais são os sistemas (sites e aplicativos) projetados para a conexão e interação entre os usuários das redes sociais.

Riscos: Efeito das incertezas nos objetivos.

Riscos Cibernéticos: Riscos de ataques aos recursos tecnológicos oriundos de fraudes externas, engenharia reversa, malware, invasão, entre outros, que possam causar danos financeiros e/ou de reputação e afetar a continuidade dos negócios.

Segurança da Informação: Proteção criada para as informações existentes na Instituição. São ati vidades de segurança da informação todos os controles de acesso, físicos ou lógico, cujo objetivo é proteger softwares, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

Violação de Dados: Qualquer falha de segurança que pode levar à perda, destruição, alteração, acesso ou divulgação não autorizada dos dados pessoais.

Wi-Fi: Tecnologia de rede sem fio que permite aos computadores, dispositivos móveis e periféricos se conectarem à internet.

5. OBJETIVOS

Esta Política de Segurança da Informação (PSI) estabelece as diretrizes, responsabilidades e conceitos da OSEC para proteção de dados físicos e digitais, e estabelece diretrizes procedimentais das áreas e comportamentais dos usuários sobre a segurança das informações; a estrutura organizacional; bem como a comunicação e a proteção de dados.

6. RESPONSABILIDADES

A PSI é aplicável a todos os usuários que coletam, tratam, armazenam e eliminam informações em nome da OSEC. Cada usuário deve utilizar a informação de acordo com a sua alçada de competência e grau de acesso. Alguns papéis são pré-definidos, outros são designados pelo gestor da área de acordo com a necessidade de acesso à informação.

1. **Controlador de dados:** empresa que gerencia os dados do conjunto de titulares. A OSEC é a controladora dos dados.
2. **Operador de dados:** realiza o tratamento dos dados pessoais em nome do controlador, ou seja, opera os dados com uma finalidade específica conforme estabelecido pelo controlador.
3. **Custodiante da informação:** responsável imediato pela informação. Cabe a ele garantir a proteção dos dados sob sua posse e comunicar ao Comitê de Privacidade e ao Encarregado de Dados qualquer situação que comprometa a integridade e confidencialidade da informação, pois atua como representante direto do controlador de dados.
4. **Departamento de Tecnologia da Informação:** equipe técnica responsável pela administração das informações em meio eletrônico. A equipe é subdividida e tem informações de acordo com atividades designadas.
5. **Gestor da informação:** colaborador com nível gerencial responsável por classificar as informações e definir procedimentos e critérios de acesso.
6. **Titular de dados:** indivíduo dono da informação.
7. **Usuário:** pessoa habilitada a acessar a informação no nível de consulta.
8. **Comitê Gestor de Privacidade e Proteção de Dados:** órgão colegiado de caráter permanente responsável pela deliberação de assuntos relacionados à privacidade de dados, ações, programas,

políticas e projetos que envolvam Segurança da Informação.

9. **Encarregado de Dados (DPO):** pessoa responsável para atuar como canal de comunicação entre con trolador, operador, usuário e ANPD oferece também suporte ao controlador na capacitação, adequação e governança de dados.

7. PROPRIEDADE DA INFORMAÇÃO

É de propriedade e de direito de uso da OSEC todas as informações criadas, coletadas, tratadas, armazenadas ou eliminadas bem como a marca e demais ativos tangíveis e intangíveis da Instituição.

A OSEC considera ativos de informações todos os dados coletados, gerados, tratados ou desen volvidos para a execução do negócio, incluindo arquivos digitais, documentos impressos, sistemas, dispositivos móveis, bancos de dados. As informações são classificadas de acordo com o grau de sigilo e anecessidade de acesso e cabe ao gestor estabelecer o critério de classificação dos dados da sua área.

Os recursos tecnológicos disponíveis na OSEC como *desktops*, *notebooks*, *smartphones*, impressoras e periféricos utilizados para o desenvolvimento de atividades presenciais e/ou remotas (*home office*),acadêmicas e profissionais são de propriedade e/ou responsabilidade da Mantenedora.

8. CLASSIFICAÇÃO, IDENTIFICAÇÃO E AUTENTICAÇÃO DA INFORMAÇÃO

A classificação da informação deve ser respeitada por todos, independentemente da denominação ou relação contratual. Em caso de dúvida, todos devem tratar a informação como de uso interno, não passível de divulgação — incluindo a internet e mídias sociais.

As informações são devidamente identificadas de acordo com o grau de confidencialidade a que estiverem condicionadas para que sejam devidamente protegidas. Dessa forma, as informações internassão identificadas e autenticadas com *login* e senha.

Todas as informações envolvendo dados sensíveis são tratadas como confidenciais pelo usuário.

O Departamento de Tecnologia da Informação dispõe de mecanismos tecnológicos para assegurar o armazenamento e o compartilhamento de conteúdo confidenciais somente à pessoas autorizadas.

9. GESTÃO DE ACESSO

Todo usuário de informação que faça uso dos recursos de tecnologia da informação e comunicaçãoda OSEC possuem uma conta de acesso com credencial única, pessoal e intransferível

que permita seureconhecimento de maneira individual e inequívoca. Os critérios de perfil de acesso são concedidos deacordo com a natureza das responsabilidades dos usuários.

10. DISPOSITIVOS MÓVEIS INSTITUCIONAIS

Os dispositivos móveis institucionais possuem as funções necessárias para seu funcionamento e suas informações corporativas são armazenadas em servidores específicos, os quais são acessados apenas por pessoas autorizadas.

É vedado aos usuários que possuem dispositivos móveis: emprestar, ceder ou transferir os dispositivos pertencentes à Instituição para qualquer pessoa que não seja o usuário responsável pelo equipamento.

Em caso de perda, roubo ou furto de dispositivos institucionais, o usuário deve imediatamente registrar um Boletim de Ocorrência, notificar o gestor imediato e o Departamento de Tecnologia da Informação para que haja a análise da extensão do dano em relação à segurança da informação.

11. AUDITORIA DE REDES

A OSEC pode acessar, revisar e monitorar todos os aspectos de comunicação interna ou externa,incluindo e-mails, internet, sistemas de telefonia, tráfego de rede e quaisquer sistemas sob sua gestão. O consentimento para tais registros e monitoramento é feito pelo usuário no ato da assinatura do contrato entre as partes.

12. INTERNET

O acesso à internet é concedido por meio de autenticação pessoal e intransferível, além de ser condicionado às necessidades do usuário. O titular é o único responsável pelas atividades realizadas em sua conta, responsabilizando-se civil e criminalmente por atos identificados por meio de *software* de monitoramento do uso da internet pelo usuário.

As solicitações de liberação de sites úteis para as atividades diárias do departamento são feitas pelo gestor imediato por meio de solicitação formal ao Departamento de Tecnologia da Informação.

13. E-MAIL CORPORATIVO

O e-mail corporativo é uma forma oficial de comunicação dos colaboradores da OSEC, o qual deve ser utilizado somente para fins relacionados à realização das atividades profissionais de suas funções, além de obedecer às seguintes regras:

O e-mail é para a formalização da comunicação com o público interno (colaboradores, estagiários, aprendizes) e externo (fornecedores, prestadores de serviços etc.);

É dever do usuário proteger seu endereço de e-mail com senha de acesso segura, devendo ser pessoal e intransferível, assim como atualizada periodicamente para reforçar a segurança das informações;

O usuário tem a responsabilidade de proteger os dados pessoais (próprios e de terceiros) que manuseia, cumprindo o necessário para a execução da atividade, conforme estipulado pelo controlador.

14. MÍDIAS SOCIAIS

A utilização das redes sociais pelos colaboradores, terceirizados, estagiários e aprendizes da OSEC deve respeitar as seguintes orientações:

- Utilizar as redes com cautela, sempre evitando a exposição negativa da Instituição.
- Atrelar, vincular, publicar e compartilhar a imagem da Instituição à mídias sociais do ambiente institucional com conteúdos ilícitos, ou que não faça parte do nicho da saúde sem autorização da OSEC.

15. MESA LIMPA E TELA LIMPA

O princípio da confidencialidade da segurança da informação recomenda a política da mesa limpa e tela limpa, que consiste na mitigação de riscos de exposição desnecessária de quaisquer informações com o objetivo de evitar o acesso não autorizado, perdas ou danos às informações durante e fora doexpediente. Nenhuma informação confidencial ou interna deve ficar à vista, seja em papel, dispositivos eletrônicos, ou telas de computador em desuso.

16. ÁUDIO, VÍDEOS E FOTOS

É vedada a gravação, reprodução, compartilhamento e/ou publicação de vídeos, áudio e imagens de aulas, reuniões, eventos institucionais, bem como das instalações internas sem autorização prévia da Instituição.

A imagem dos colaboradores, estagiários, aprendizes, prestadores de serviços pode ser utilizadapara fins de identificação, autenticação, segurança, registro de atividades e acervo histórico da Instituição, além das previsões legais, o que inclui eventos institucionais.

17. SEGURANÇA FÍSICA E DO AMBIENTE

O ambiente interno da Instituição é monitorado por câmeras de segurança para a proteção das pessoas, do patrimônio e da reputação institucional, conforme Lei Municipal nº 13.541 de 24 de março de 2003, que dispõe a colocação de placa informativa sobre filmagem de ambientes e outras providências.

Qualquer mudança de ambiente é feito de forma estruturada, visando minimizar impactos e as- segurar a disponibilidade, integridade, confidencialidade, legalidade e autenticidade das informaçõese dos dados, bem como a proteção de dados pessoais e a privacidade. Toda e qualquer alteração nosambientes computacionais deve ser obrigatoriamente homologada pelo Departamento de Tecnologiada Informação.

18. SEGURANÇA DA INFORMAÇÃO

A prevenção de riscos deve ser feita com a implantação de controles internos de caráter geral. São atividades de controle:

1. **Classificação de informação:** separação das informações de acordo com o grau de sigilo.
2. **Segregação de função:** definição de alçadas de competência.
3. **Alçada de competência:** concessão de acesso a dados de acordo com a atividade executada.
4. **Camadas de proteção à informação:** criação de controles físicos e lógicos para acesso aosdados.
5. **Aplicação do princípio da necessidade:** coletar somente informações estritamente necessárias para a execução da atividade.
6. **Credencial de acesso:** responsabilização individualizada de acordo com atividades executadasno usuário de acesso.
7. **Uso seguro de ativos da informação:** criação de controle de acesso e monitoramento dos ativos sob a guarida institucional.

19. DESCARTE DE DADOS

O descarte de dados deve ser feito conforme estabelecido na Política de Descarte de Dados, definida e aprovada pela Instituição.

20. PENALIDADES

A violação as regras descritas nesta política e nas demais normas e procedimentos de segurança da informação da Instituição estão sujeitas às sanções previstas no Código Penal e na Consolidação das Leis do Trabalho (CLT).

21. DISPOSIÇÕES GERAIS

Todos os usuários são responsáveis por proteger os ativos tangíveis e intangíveis, incluindo informações contra qualquer tipo de ameaça ou danos. Os recursos institucionais, como a marca, a reputação, propriedade intelectual, informações e o conteúdo interno da OSEC devem ser preservados e usados com responsabilidade.

Em caso de dúvidas quanto à PSI, demais procedimentos, ou casos de incidente de segurança da informação, infração ou suspeita de violação de segurança de dados/informação, devem ser comunicados imediatamente ao Departamento de Tecnologia da Informação, ao Comitê de Privacidade e ao Encarregado de Dados (DPO) por meio do e-mail dpo@Osec.br.

É de responsabilidade de todos os gestores da OSEC promover o conhecimento e a disseminação desta Política e correlatas, bem como estabelecer procedimentos de segurança da informação nas áreas sob sua gestão. Esta política entra em vigor na data de sua publicação.

22. REFERÊNCIAS

Lei Federal n° 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

Lei nº 14.155, de 27 de maio de 2021 – Lei que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet.

Lei nº 14.289 de 3 de janeiro de 2022 - Torna obrigatória a preservação do sigilo sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos casos que estabelece; e altera a Lei nº 6.259, de 30 de outubro de 1975.

23. REGISTRO DE APROVAÇÃO/VERSÃO

Política de Segurança da Informação	Versão	**1**
	Área Gestora	**Jurídico**

		Classificação da Informação		**Público Interno**
Versão	Data	Nome	Aprovador	Status
1	**25/03/2024**	**Sebastião Lacarra Medina**	**Mantenedor**	**Aprovada**