ONCASE	Emitente	Vigência	Versão
Segurança da Informação	Operações	06/21 a 05/23	1.0

Política Pública de Segurança da Informação e Cibernética ONCASE

Aos Colaboradores, Parceiros, Terceiros e Clientes:

Como fator crítico de sucesso, a Oncase considera extremamente importante garantir a segurança das informações sob sua responsabilidade.

Desta forma, a Oncase torna pública a sua **POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA** adequada aos princípios e valores da Companhia.

Este documento consiste em um conjunto de orientações que valorizam e definem o uso adequado das informações, possibilitando ambientes de TI seguros, confiáveis e íntegros.

O comprometimento de todos em conhecer e vivenciar esta política é de extrema importância para alcançarmos um padrão de excelência na gestão de segurança, proporcionando a evolução dos nossos negócios de forma cada vez mais transparente e segura.

1. Introdução

A adoção de políticas, normas e procedimentos que visem garantir a segurança da informação deve ser uma das prioridades do Compliance, reduzindo-se os riscos de falhas, danos e/ou prejuízos que possam comprometer a imagem e os objetivos da organização.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

- **Confidencialidade**: somente pessoas devidamente autorizadas pela organização devem ter acesso à informação e as pessoas que tiverem acesso à informação devem tratá-la com dever de sigilo, cuidado e nos limites e para os fins a que teve acesso à informação;

- **Integridade**: somente alterações, supressões e adições autorizadas pela organização devem ser realizadas nas informações;

- **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em geral, o sucesso da Política de Segurança da Informação adotada pela Oncase depende da combinação de diversos elementos, dentre eles, a estrutura organizacional da empresa, as normas e os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de colaboradores, parceiros e sócios.

1.1 Classificação da Informação

Todos os colaboradores devem seguir as diretrizes e procedimentos de classificação e proteção das informações de propriedade da Oncase, manipuladas e armazenadas no ambiente físico e lógico existente, a fim de preservar a integridade, confidencialidade e disponibilidade das informações.

1.2 Eventos de Segurança

Todos os colaboradores, terceiros e demais partes interessadas podem registrar a suspeita de um evento de fragilidade de segurança cibernética através do e-mail "**suporte@oncase.com.br**".

2. Diretrizes

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação da ONCASE. Tais diretrizes constituem os principais pilares da Gestão de Segurança da Informação da ONCASE, norteando a elaboração das normas e dos procedimentos.

2.1 Leis e Regulamentações

Cabe à área de Gestão de Engenharia e desenvolvimento:

- Manter as demais áreas da ONCASE informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;

- Incluir, na análise e na elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação e proteção de dados, com o objetivo de proteger os interesses da ONCASE;

- Avaliar, quando solicitado, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da ONCASE.

2.2 Identificação e Autenticação

Todas as plataformas de Tecnologia & Operações da ONCASE devem autenticar a identidade de usuários (incluindo outros sistemas que acessam estas plataformas) antes de iniciar uma sessão ou transação, a menos que o usuário tenha direitos de acesso limitados à leitura de dados.

Todo usuário deve possuir uma identidade e ser identificado para cada plataforma de Tecnologia & Operações por:

- Um ID (login) de usuário não compartilhado;
- Um método de autenticação que possibilite a identificação do usuário, por exemplo: senha única (estática) ou dinâmica, chave privada, dados biométricos ou outro mecanismo de autenticação homologado e que atenda as melhores práticas de segurança;
- Cada usuário é responsável por toda atividade associada com o login de usuário associado à sua identidade ou sob sua custódia.

Os usuários devem seguir as seguintes práticas para proteção de senhas estáticas:

- As senhas devem ser geradas e guardadas em ferramenta de gerenciamento de senhas;
- Nunca podem ser compartilhadas ou apresentadas a terceiros;
- Nunca podem ser apresentadas/escritas em claro (com exceção de senha pré-expirada, utilizada no processo de senha inicial).

3. Confidencialidade e Integridade

Os gestores devem informar a todos os colaboradores da ONCASE, bem como a clientes, fornecedores e usuários em geral que todas as informações armazenadas, transmitidas ou manuseadas nos sistemas e processos são de propriedade da ONCASE, de seus clientes ou licenciados por terceiros. Sempre que permitido pela legislação, a ONCASE reserva-se o direito de revisar e monitorar estas informações para fins administrativos, de segurança ou legais.

Informações confidenciais da ONCASE, independentemente da mídia ou ambiente onde estejam sendo mantidas, devem ser protegidas contra acessos não autorizados e com as devidas aprovações.

Para a proteção adequada das informações custodiadas pela ONCASE, que estão sendo manuseadas nas estações de trabalho, sempre que o colaborador se ausentar do ambiente, em particular fora do horário de trabalho, é sua responsabilidade bloquear a estação de trabalho, solicitar e utilizar os recursos disponibilizados pela ONCASE para proteger as informações de acessos não autorizados. Para a proteção adequada das informações custodiadas pela ONCASE, que estão sendo manuseadas em equipamentos portáteis (notebook), todos os usuários devem cumprir os requerimentos definidos por esta política de segurança da informação.

É importante e necessário que a Gestão de Engenharia e Desenvolvimento da Oncase atue diretamente nos seguintes pontos:

- Monitorando os terceiros que armazenam, processam, gerenciam ou acessam as informações da ONCASE (PÚBLICA) ou têm conexão com os recursos de rede da ONCASE, para que cumpram os padrões aqui definidos;
- Realizando avaliações de segurança da informação nos Terceiros de acordo com os procedimentos aprovados pelo Comitê Corporativo;
- Formalizando acordos de confidencialidade NDA – “Non Disclosure Agreement” ou disposições equivalentes, aprovados pela área jurídica da ONCASE, com os Terceiros que armazenem, processem, gerenciem ou acessem informações custodiadas pela ONCASE (exceto informação classificada como PÚBLICA).

3.1 Adoção de Comportamento Seguro

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações da ONCASE, com destaque para os seguintes itens:

- Sócios, colaboradores e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da ONCASE;

- Todos na ONCASE devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação;
- Todo tipo de acesso à informação da ONCASE que não for explicitamente autorizado é proibido;
- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protegido;
- Somente softwares homologados pela equipe de TI da ONCASE podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia & Operações da ONCASE, respeitando as questões legais de licenciamento;
- A política para uso de internet e correio eletrônico deve ser rigorosamente seguida;
- Arquivos de origem desconhecida nunca devem ser abertos e/ou executados;
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos;
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecida com a Gestão de Engenharia e Desenvolvimento da Oncase;

3.2 Avaliação dos Riscos de Segurança da Informação

A Gestão de Engenharia e Desenvolvimento da Oncase deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação da ONCASE.

A análise dos riscos deve atuar como ferramenta de orientação sobre a segurança da Informação, principalmente, no que diz respeito a:

- Identificação dos principais riscos aos quais as informações da ONCASE estão expostas;
- Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas etc. O escopo da análise/avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.;
- O Planejamento trimestral de identificação e análise dos riscos, podendo ser alterado o ciclo de análise conforme definido pelo Comitê de Segurança da Informação;
- Implantação de ferramentas para identificação de riscos e compliance.

4. Monitoramento e Controle

Os equipamentos, os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da ONCASE, não podendo ser interpretados como de uso pessoal.

Todos os profissionais da ONCASE devem ter ciência de que o uso das informações e dos sistemas de informação da ONCASE pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política, as Normas e Procedimentos de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

4.1 Treinamento e Conscientização de Segurança da Informação

Cada gestor deve garantir que todos os colaboradores e fornecedores, ao iniciar a relação com a ONCASE ou quando tiverem alteração significativa na responsabilidade do trabalho, estejam cientes sobre aspectos de segurança da informação relacionados a sua função em até 5 (cinco) dias do início de seu relacionamento com a Oncase.

4.2 Procedimentos de Desenvolvimento Seguro

A Oncase utiliza um conjunto de princípios para projetar sistemas seguros, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas, levando a privacidade em consideração desde a sua concepção.

4.3 Descarte de Informações Sensíveis

Não atuamos com dados disponíveis em mídias físicas (ex.: pen drive, cds, dvds). Todos os dados de clientes são transferidos e trafegados entre servidores privados e serviços de nuvem, utilizando canais privados (ex.: VPN) para consulta e armazenamento.

4.4 Segurança em Recursos Humanos e Acessos

A Oncase mantém controles de Segurança nos processos de recursos humanos nos momentos de seleção, contratação, mudança de função e encerramento do contrato de trabalho. Todas as nossas senhas são centralizadas e gerenciadas através de uma ferramenta de geração e gerenciamento de logins e senhas. Apenas os usuários do domínio oncase.com.br podem ter acesso.
Os acessos ao ambiente de cloud também são controlados através de permissões temporárias e específicas aos serviços e conjuntos de dados necessários.

4.5 Controles de Auditoria e Acessos

Em adição às políticas de controle de acessos e de usuários, atualmente utilizamos também logs de monitoramento e acessos às ferramentas utilizadas em cloud, por todos os usuários Oncase e Terceiros. Esse tipo de solução permite a rastreabilidade das ações de usuários e geração de relatórios.

5. Revisão do documento

5.1 Este documento será revisto e atualizado a cada dois anos ou quando:

- Houver solicitação de atendimento, correção ou adição de informações;
- Existir a necessidade de atender requisitos legais, boas práticas ou recomendações de auditoria;
- Existir mudança na organização que tenha impacto relevante na atividade abordada neste documento.

Recife, 01 de junho de 2021

_____	_____
Bruno Ricardo Silva	Iandé Bailey Bezerra Coutinho
COO	CEO