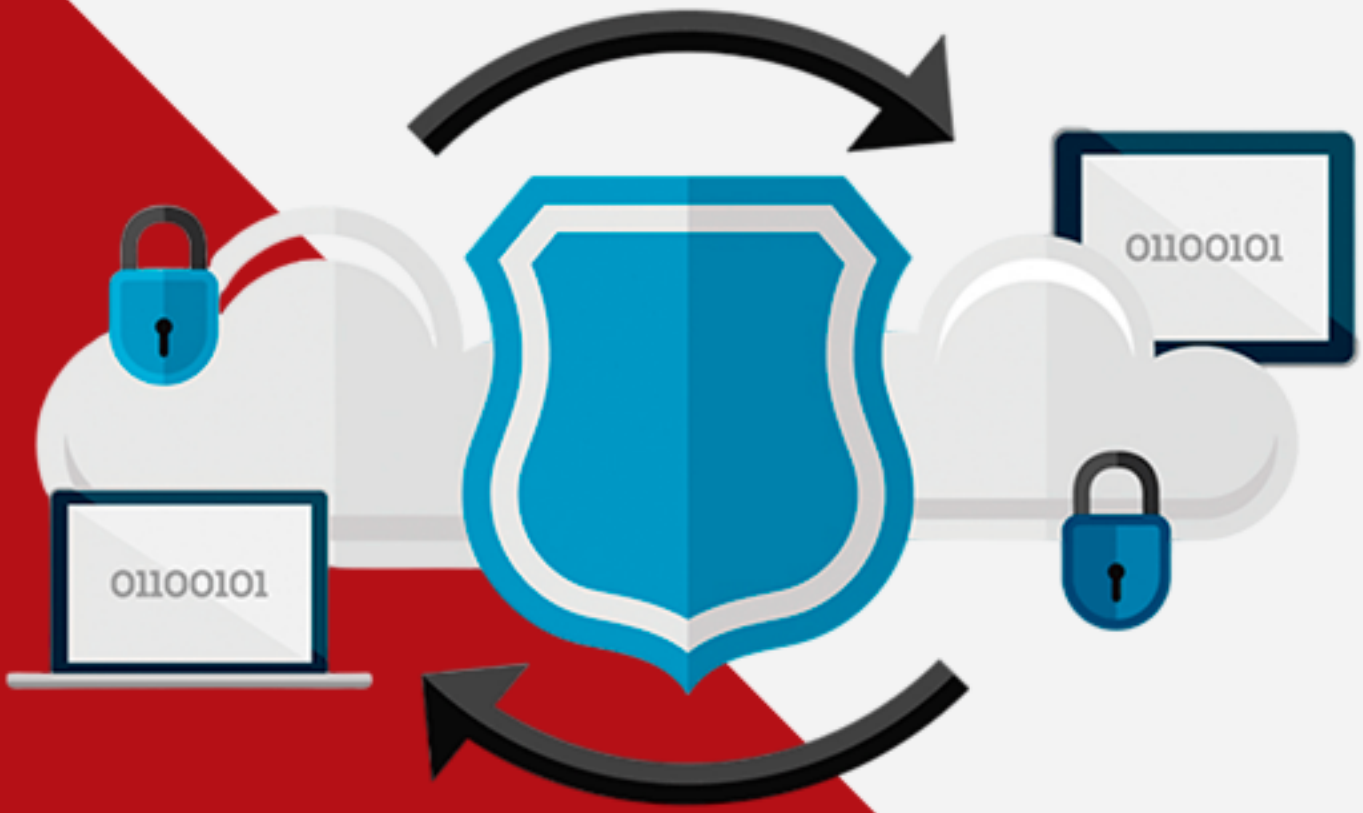

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

RECIFE-2024

FADE
UFPE

FOLHA DE CONTROLE

Informações Gerais

Título	Política de Segurança da Informação
Número de referência/Código	POL_SI_001
Status	Revisão
Autoria	Aurora Barros – Consultoria
Validação e Aprovação	Diretoria Executiva e Conselho de Curadores
Data da validação ou aprovação	Mai/2024
Validade	Indeterminada
Área Controladora da Política	Compliance

Histórico de Versões

Versão	**Motivo**	**Data**
1	Versão inicial	Mai/2024

FICHA TÉCNICA

Conselho de Curadores

Presidente do Conselho

Profª. Magdala de Araújo Novaes (Centro de Ciências Médicas – CCM)

Membros Titulares

Profª. Nadi Helena Presser (Centro de Artes e Comunicação – CAC)
Prof. Pablo Martin Rodriguez (Centro de Ciências Exatas e da Natureza – CCEN)
Profª. Sérgio Castelo Branco Soares (Centro de Informática – CIn)
Prof. Ricardo Pinto de Medeiros (Centro de Filosofia e Ciências Humanas – CFCH)
Profª. Darci Barbosa Lira de Melo (Centro de Educação – CE)
Prof. José Gilson de Almeida Teixeira Filho (Centro de Ciências Sociais e Aplicadas – CCSA)
Profª. Gabriela Cunha Schechtman Sette (Centro de Ciências da Saúde – CCS)
Prof. José Araújo dos Santos Júnior (Centro de Tecnologia e Geociências – CTG)
Prof. André Morgado Esteves (Centro de Biociências – CB)
Prof. Osmar Veras de Araújo (Centro Acadêmico do Agreste – CAA)
Profª. Lara Colognese Helegda (Centro Acadêmico de Vitória – CAV)
Prof. Humberto João Carneiro Filho (Centro de Ciências Jurídicas – CCJ)
Fernanda de Oliveira Muniz (Representante da Comunidade Estadual)

Membros Suplentes

Profª. Márcia Ivo Braz (Centro de Artes e Comunicação – CAC)
Prof. Eduardo Padrón Hernandéz (Centro de Ciências Exatas e da Natureza – CCEN)
Prof. André Luís de Medeiros Santos (Centro de Informática – CIn)
Prof. Reginaldo Gonçalves de Lima Neto (Centro de Ciências Médicas – CCM)
Prof. Francisco Jatobá de Andrade (Centro de Filosofia e Ciências Humanas – CFCH)
Prof. Ramon de Oliveira (Centro de Educação – CE)
Prof. Luiz Carlos Marques dos Anjos (Centro de Ciências Sociais e Aplicadas – CCSA)
Prof. Tony Meireles dos Santos (Centro de Ciências da Saúde – CCS)
Profª. Yêda Medeiros Bastos de Almeida (Centro de Tecnologia e Geociências – CTG)
Profª. Maria Teresa Jansem de Almeida Catanho (Centro de Biociências – CB)
Prof. Mário Rodrigues dos Anjos Neto (Centro Acadêmico do Agreste – CAA)
Prof. Emerson Peter da Silva Falcão (Centro Acadêmico de Vitória – CAV)

Equipe Fade-UFPE

Diretoria Executiva

Profª. Maira Galdino da Rocha Pitta, Diretora Presidente

Assessorias

Rosali Maria Oliveira de Albuquerque (Assessoria de Planejamento)
Ladice Albuquerque Marinho (Assessoria de Compliance e Controle Interno)
Anderson de Oliveira Vasconcelos (Assessoria de Inovação e Captação de Projetos)
Eduardo Pontes Barbosa (Assessoria de Tecnologia da Informação)
Raquel Souza Guimarães (Assessoria Jurídica)

Gerências

Iraci Pereira do Nascimento (Gerência de Recursos Humanos)
David Soares Pessoa (Gerência de Projetos 1)
Samia Amancio Sindeaux (Gerência de Projetos 2)
Danielle Anizia da Silva (Gerência de Projetos 3)
Suzan Kelly de Vasconcelos Siqueira (Gerência Administrativa e Financeira)

SUMÁRIO

COM A PALAVRA A ALTA DIREÇÃO

É com satisfação que apresentamos a Política de Segurança da Informação (PSI) da Fade-UFPE, pilar fundamental na proteção dos nossos ativos mais valiosos: os dados e informações que nos permitem atender às necessidades dos nossos parceiros e alcançar nossos objetivos estratégicos.

No mundo cada dia mais veloz e informatizado, todas as medidas para a segurança para nossos dados e informações é de grande relevância para a nossa gestão.

Com vistas a isso, estamos empenhando esforços para assegurar que nossas atividades estejam adequadas e em conformidade com os mais altos padrões de segurança da informação.

Nesse sentido, A PSI estabelece diretrizes claras e responsabilidades para todos os colaboradores, visando garantir a proteção de dados confidenciais, preservação da privacidade dos indivíduos e manutenção da integridade dos dados, todos essenciais para o funcionamento e continuidade dos negócios.

Além disso, a PSI é um alicerce para a conformidade com leis e regulamentações, fortalece a confiança e a reputação da Fundação junto às apoiadas e parceiros, e protege contra ameaças cibernéticas e vazamentos de informações.

A PSI é um documento vivo, que será revisado periodicamente para garantir sua eficácia e adequação às necessidades da organização. Esperamos que todos se engajem nesse processo contínuo de melhoria e estejam sempre atentos às boas práticas de segurança da informação.

Uma estratégia de segurança da informação bem implementada é vital para a inovação segura, gestão de riscos, e estabelecimento uma cultura organizacional de responsabilidade e prestação de contas.

MAIRA GALDINO DA ROCHA PITTA:03997206422

Assinado de forma digital por MAIRA GALDINO DA ROCHA PITTA:03997206422
Dados: 2024.06.11 09:55:28 -03'00'

Profª. Maira Galdino da Rocha Pitta
Diretora Presidente da Fade-UFPE

1. OBJETIVO

Esta política tem como objetivo estabelecer um conjunto de controles e procedimentos de segurança da informação para proteger os ativos de informação, dados pessoais, dados pessoais sensíveis, informações confidenciais, informações sigilosas, sob o manto da propriedade intelectual, dentre outros, que estejam sob a responsabilidade da Fade-UFPE contra todas as ameaças internas, externas, deliberadas ou acidentais.

2. ESCOPO

Esta política aplica-se a todos os funcionários, contratados, fornecedores, aprendizes, estagiários, consultorias e outras partes interessadas que têm acesso aos sistemas de informação da Fundação ou que até mesmo não tenha acesso, mas que venha a ter eventualmente, de forma direta ou indireta, acidentalmente ou não, de forma autorizada ou não, mas que acesse de forma a tornar vulnerável as informações verificadas.

3. ANÁLISE CRÍTICA DOS SETORES E ALTA DIREÇÃO

A Diretoria Executiva, juntamente com as Gerências, Assessorias e eventuais consultorias especializadas, estabelecerá, regularmente, reuniões de monitoramento e de trabalho. A reunião de análise crítica deverá ser realizada semestralmente, onde serão apontadas soluções de melhoria, análises de riscos, discussões sobre os campos de atuações e demais assuntos relacionados à segurança da informação. A Assessoria de Compliance e Controle Interno será responsável pelo calendário destas reuniões, não podendo ultrapassar o ultimo dia útil de cada trimestre do ano-calendário vigente.

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é baseada em três princípios fundamentais: Confidencialidade; Integridade e Disponibilidade.

O princípio da confidencialidade na segurança da informação refere-se à restrição do acesso e divulgação de informações a pessoas, entidades ou processos autorizados. Trata-se de garantir que as informações não sejam disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados, assegurando que o acesso seja estritamente controlado e concedido exclusivamente àqueles que possuem a necessidade legítima de conhecer essas informações para desempenhar suas funções ou tarefas.

Na prática, a confidencialidade é implementada por meio de uma série de controles, políticas e procedimentos que incluem:

- **Autenticação de usuários**: Verificação da identidade de uma pessoa ou sistema antes de conceder acesso a informações confidenciais;
- **Controle de acesso**: Restrições que limitam o acesso a informações com base em permissões de usuário definidas, geralmente em um modelo de mínimos privilégios, onde os usuários têm apenas os acessos necessários para realizar suas tarefas;
- **Criptografia**: Uso de técnicas matemáticas para transformar informações em um formato ilegível para quem não possui a chave de descriptografia, protegendo dados em trânsito e em repouso;
- **Acordos de confidencialidade**: Contratos legais que obrigam as partes a manter a confidencialidade das informações compartilhadas;
- **Treinamento e conscientização**: Educar os funcionários e partes interessadas sobre a importância da confidencialidade e como manter as informações seguras.

A violação da confidencialidade pode levar a consequências graves, incluindo danos financeiros, perda de reputação e ações legais.

No tocante a Integridade, no contexto da segurança da informação, refere-se à precisão, consistência e confiabilidade das informações ao longo de todo o seu ciclo de vida. O princípio da integridade assegura que os dados sejam protegidos contra alterações não autorizadas ou não intencionais, e que sejam exatos e completos quando acessados ou recuperados.

Os aspectos fundamentais do princípio da integridade incluem:

- **Prevenção de alterações indevidas**: Garantir que apenas pessoas, processos ou sistemas autorizados possam alterar os dados;
- **Detecção de alterações**: Capacidade de identificar quando e como os dados foram alterados, incluindo a identificação do responsável pela modificação;
- **Controle de versões**: Manter um histórico de versões dos dados ou documentos para que alterações possam ser rastreadas e, se necessário, revertidas;
- **Validação de dados**: Processos para verificar a precisão e consistência dos dados, tanto na entrada quanto ao longo do armazenamento e transmissão;
- **Segurança contra falhas**: Proteções contra erros de sistema ou falhas de hardware que podem corromper os dados.

Para manter a integridade, são implementadas várias medidas de segurança, como:

- **Controle de acesso**: Restrição do acesso a sistemas e dados com base em funções e responsabilidades;
- **Checksums e hashes**: Utilização de algoritmos matemáticos para verificar a integridade dos dados após o armazenamento ou a transmissão;
- **Assinaturas digitais**: Uso de chaves criptográficas para validar a autenticidade e a integridade de documentos e mensagens;
- **Auditorias e logs**: Monitoramento e registro de atividades para detectar e investigar acessos e alterações indevidas;
- **Backup e recuperação**: Implementação de cópias de segurança regulares e planos de recuperação para restaurar dados em caso de corrupção ou perda.

Política de Segurança da Informação

A integridade é essencial para a confiança nos sistemas de informação, pois garante que as decisões sejam tomadas com base em informações corretas e válidas. Uma violação da integridade pode levar a decisões equivocadas, perda de confiança e danos potencialmente graves para a Fundação e seus parceiros.

Com relação à disponibilidade, no contexto da segurança da informação, é um princípio que assegura que informações e recursos de TI estejam acessíveis aos usuários autorizados sempre que necessários. Esse princípio é crucial para o funcionamento eficiente das atividades de uma Fundação, pois a inacessibilidade das informações pode levar a perdas de produtividade, interrupções nos serviços e impactos financeiros.

Para garantir a disponibilidade, é necessário considerar vários fatores e implementar diversas medidas, tais como:

- **Redundância de hardware**: Utilização de múltiplos componentes, como servidores, discos rígidos e fontes de energia, para garantir que a falha de um não cause a indisponibilidade do sistema;
- **Balanceamento de carga**: Distribuição das demandas de processamento e tráfego de rede entre vários servidores para evitar sobrecargas em um único ponto, o que poderia levar a interrupções do serviço;
- **Manutenção preventiva**: Realização de manutenções regulares para prevenir falhas antes que elas ocorram, incluindo atualizações de software e substituição de hardware obsoleto ou em risco de falhar;
- **Planos de recuperação de desastres (DRP) e continuidade de negócios (BCP)**: Estratégias detalhadas que permitem a recuperação rápida de sistemas de TI e a retomada das operações de negócios, após um incidente que cause interrupção dos serviços;
- **Backup de dados**: Criação de cópias de segurança dos dados em intervalos regulares e seu armazenamento em locais seguros, possibilitando a restauração das informações em caso de perda ou corrupção de dados;
- **Monitoramento de rede e sistemas**: Vigilância constante dos sistemas para detectar e resolver rapidamente problemas que possam afetar a disponibilidade;
- **Defesa contra ataques cibernéticos**: Proteção contra ameaças como ataques de negação de serviço (DoS ou DDoS), que têm como objetivo tornar os recursos de TI indisponíveis para os usuários.

A gestão desses pilares, atendendo aos detalhamentos acima postos, será feita pela gestão interna de tecnologia da informação, e, se for o caso, também por consultorias especializadas.

Cabe, igualmente, que a gestão interna de tecnologia da informação identifique melhorias para cobrir o atendimento aos princípios apontados.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Todos os usuários são responsáveis pelas informações da Fade-UFPE, que circulam em diferentes formatos e meios de comunicação, dentro e fora da Fundação. Toda informação deve ser protegida e mantida sob sigilo, conforme sua importância e criticidade. Assim, quanto mais crítica ou sigilosa a informação, maiores cuidados devem ser dedicados ao manuseio, arquivamento e eventual descarte.

É de responsabilidade do Gestor de cada Setor estabelecer critérios relativos ao nível de confidencialidade da informação (física ou digital), gerada por sua área.

O processo de classificação da informação consiste em identificar quais são os níveis de proteção requeridos, bem como estabelecer classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

O sistema de classificação da informação da Fade-UFPE obedece a estrutura de criticidade de acordo com a tabela abaixo:

- **Pública**: É toda informação que pode ser acessada por usuários da Fade-UFPE, parceiros, prestadores de serviços e público em geral;
- **Interna**: É toda informação acessada apenas pelos colaboradores da Fundação. São informações que possuem um grau de confidencialidade, que pode comprometer a imagem da Fade-UFPE;
- **Confidencial**: É toda informação que pode ser acessada pelos colaboradores e parceiros da Fade-UFPE, contudo, a divulgação não autorizada dessa informação pode causar impacto financeiro, de imagem, operacional, reputacional, entre outros ao negócio da Fundação. A divulgação não autorizada dessa informação pode causar sérios danos ou comprometer a estratégia da Fade-UFPE.

Todos os gestores e suas lideranças devem orientar seus setores a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

6. GESTÃO DE ATIVOS

A gestão de ativos na área de segurança da informação é um processo sistemático para desenvolver, operar, manter e descartar ativos de forma eficiente e segura, garantindo a proteção das informações associadas a esses ativos. Ativos de informação podem incluir hardware, software, dados, infraestrutura de rede e também informações e processos cruciais para os negócios da Fundação.

Será procedida na Fade-UFPE a gestão de ativos de acordo com o que se segue:

- **Identificação de Ativos**: Catalogar todos os ativos de TI, incluindo hardware, software e informações. Atribuir um responsável por cada ativo. Classificar os ativos com base em sua importância para a Fundação;
- **Inventário e Rastreamento**: Manter um inventário atualizado que registre detalhes como versão, localização, configuração e status do ciclo de vida dos ativos. Utilizar etiquetas de identificação e ferramentas de gerenciamento de ativos para rastreá-los ao longo de seu ciclo de vida;
- **Avaliação de Risco**: Realizar avaliações regulares de risco para identificar vulnerabilidades e ameaças aos ativos. Determinar o impacto potencial de incidentes de segurança nos ativos e nas operações da Fundação;
- **Políticas de Segurança e Controles**: Desenvolver políticas de segurança que definam os padrões para uso, operação e manutenção dos ativos. Implementar controles de segurança físicos e lógicos para proteger os ativos;
- **Manutenção e Atualização**: Realizar manutenções preventivas para assegurar o funcionamento contínuo dos ativos. Atualizar regularmente o software para corrigir vulnerabilidades e melhorar a segurança;
- **Treinamento e Conscientização**: Treinar os usuários e a equipe de TI sobre responsabilidades e boas práticas na gestão de ativos. Promover uma cultura de segurança da informação;
- **Monitoramento e Revisão**: Monitorar continuamente os ativos para detectar atividades suspeitas ou não autorizadas. Revisar e atualizar o processo de gestão de ativos regularmente para incorporar mudanças nas tecnologias e no ambiente de negócios;
- **Descarte Seguro**: Quando um ativo chegar ao fim de seu ciclo de vida útil, ele deverá ser descartado de forma segura. Assegurar que todas as informações confidenciais sejam permanentemente removidas ou destruídas.

Poderão ser utilizadas as seguintes ferramentas:

- **Software de Gestão de Ativos de TI (ITAM)**: Ferramentas especializadas que automatizam muitas das tarefas associadas à gestão de ativos;
- **Sistemas de Gerenciamento de Configuração (CMS)**: Databases que armazenam informações sobre ativos e suas configurações;
- **Gestão de Mudanças**: Processos para controlar mudanças em ativos de TI, minimizando riscos e interrupções.

A gestão de ativos eficaz é fundamental para garantir a confidencialidade, integridade e disponibilidade das informações, o que, por sua vez, ajuda a Fundação a cumprir seus objetivos estratégicos e operacionais, além de manter a conformidade com as regulamentações pertinentes.

7. CONTROLE DE ACESSO

O controle de acesso é um componente crítico da segurança da informação que determina quem ou o que pode visualizar ou usar recursos em um ambiente de computação. Existem duas facetas

principais: controle de acesso físico e controle de acesso lógico. Ambos poderão ser adotados, a critério e na melhor forma aplicável em cada setor pelos seus supervisores. São eles:

- **Controle de Acesso Físico**: garante a segurança física de instalações, restringindo quem pode entrar em áreas específicas. Isso é conseguido através de: fechaduras e chaves, cartões de acesso, sistemas biométricos, guardas de segurança, câmeras de vigilância, alarmes;
- **Controle de Acesso Lógico**: refere-se à proteção de sistemas digitais e dados. O controle de acesso lógico inclui a implementação de políticas e procedimentos que limitam o acesso a sistemas de informação e dados. Isso é feito por meio de autenticação (algo que o usuário sabe, tem ou é; por exemplo, senha, token ou biometria), autorização (definindo o que cada usuário pode fazer após a autenticação, geralmente baseado em papéis ou atribuições), conta e gerenciamento de sessões (monitorando e encerrando sessões após inatividade ou após o término de um período de acesso autorizado).

Tais controles deverão ser verificados quanto a sua pertinência, por cada setor.

É preciso que se verifique sempre se estes aspectos estão sendo aplicados quanto ao controle de acesso:

- Vigência de política clara e atualizada que defina quem pode acessar o que, em que circunstâncias e como os direitos de acesso devem ser gerenciados;
- Usuários apenas com os direitos de acesso necessários para desempenhar suas funções;
- Implementação MFA para adicionar uma camada extra de segurança, combinando algo que o usuário sabe (senha), algo que o usuário tem (token ou telefone celular) e algo que o usuário é (biometria);
- Sistemas para centralizar ou federar o gerenciamento de identidades e acessos dos usuários;
- Acesso por meio de grupos com atribuição de permissões a determinados acessos;
- Acesso com base em uma combinação de atributos do usuário, do recurso e do ambiente;
- Registros detalhados de atividades de acesso e monitoramento para detectar acessos não autorizados ou anormais;
- Auditorias regulares para garantir que os controles de acesso estejam funcionando como pretendido e estejam em conformidade com as regulamentações aplicáveis.

Tais verificações ficarão a cargo da gestão interna de tecnologia da informação que poderá solicitar, eventualmente, consultoria especializada.

O controle de acesso eficaz é uma parte fundamental da estratégia de segurança de uma Fundação, ajudando a proteger informações confidenciais contra acessos indevidos, reduzindo o risco de violações de dados e mantendo a conformidade com as regulamentações.

8. GERENCIAMENTO DE RISCOS

O gerenciamento de riscos na segurança da informação é um processo contínuo e abrangente, crucial para proteger os ativos de informação de uma Fundação contra ameaças e vulnerabilidades que podem levar a perdas ou danos. Esse processo envolve identificar, avaliar e tratar riscos para garantir que permaneçam em um nível aceitável. A seguir estão os componentes-chave e etapas para um gerenciamento de riscos eficaz que deverá ser adotado pela Fade-UFPE:

- **Identificação de Riscos**: Detectar potenciais ameaças (intencionais ou acidentais) e vulnerabilidades dentro dos sistemas de informação que possam ser exploradas por essas ameaças;
- **Avaliação de Riscos**: Avaliar a probabilidade de ocorrência de um evento de segurança e o impacto potencial que esse evento poderia ter sobre a Fundação. Classificar os riscos identificados por níveis de gravidade;
- **Tratamento de Riscos**: Definir medidas apropriadas para tratar os riscos identificados, que podem incluir evitar, mitigar, transferir ou aceitar o risco. Implementar controles de segurança para reduzir a probabilidade e/ou impacto dos riscos;
- **Mitigação de Riscos**: Aplicar controles técnicos, como firewalls, criptografia, e sistemas de detecção de intrusão. Implementar controles administrativos, como políticas de segurança, treinamento de conscientização e procedimentos de resposta a incidentes;
- **Transferência de Riscos**: Em certos casos, é possível transferir o risco para terceiros, através de contratos ou seguros de responsabilidade civil;
- **Aceitação de Riscos**: Quando o custo da mitigação é maior do que o impacto potencial do risco, a Fundação pode optar por aceitar o risco em decisão fundamentada e com a transparência e anuência de todas as partes interessadas;
- **Monitoramento e Revisão**: Monitorar continuamente o ambiente de segurança para identificar mudanças nos riscos. Revisar periodicamente os controles de segurança e adaptá-los conforme necessário para garantir sua eficácia;
- **Comunicação e Consulta**: Manter a comunicação com as partes interessadas durante o processo de gerenciamento de riscos. Consultar especialistas externos quando necessário para uma avaliação mais aprofundada dos riscos;
- **Ferramentas e Estratégias**: Monitoramento de ativos, análises de vulnerabilidades, monitoramento de processamento do banco de dados;
- **Análise Qualitativa e Quantitativa**: Utilizar métodos qualitativos para avaliações subjetivas de riscos ou quantitativos para estimativas baseadas em dados e estatísticas;
- **Frameworks de Gerenciamento de Riscos**: Adotar frameworks padronizados como ISO 27005, NIST SP 800-30, ou OCTAVE para orientar o processo de gerenciamento de riscos;
- **Plano de Resposta a Incidentes**: Desenvolver e manter um plano eficaz para responder aos incidentes de segurança;
- **Auditorias de Segurança**: Realizar auditorias regulares para assegurar a conformidade com políticas de segurança e regulamentações.

O gerenciamento de riscos é essencial para manter a segurança da informação alinhada com as estratégias de negócios da Fundação. Ao identificar e tratar riscos proativamente, a Fade-UFPE

pode evitar ou minimizar impactos negativos, como perda de dados, interrupções de serviço, danos à reputação e penalidades legais.

9. SEGURANÇA EM RECURSOS HUMANOS

Na segurança da informação, os Recursos Humanos (RH) desempenham um papel vital, pois grande parte da segurança depende do comportamento e consciência dos funcionários. A seguir, são apresentadas algumas medidas de segurança em recursos humanos que devem ser adotadas para reforçar a proteção da informação:

- **Acordos de Confidencialidade**: Garantir que os novos contratados assinem acordos de não divulgação ou de confidencialidade;
- **Programas de Conscientização**: Fornecer treinamento regular e atualizações sobre práticas recomendadas de segurança da informação, phishing, engenharia social, e outros riscos relevantes;
- **Integração**: Todos que ingressam no corpo de funcionários deverão receber as políticas, procedimentos e treinamento para entender o ambiente digital ao qual integrarão. Ainda, registrarão em documento específico cientificando o recebimento de todos os normativos e treinamento, cujo alinhamento de aprendizado para verificação da apreensão do conteúdo deverá ser pontuado em, pelo menos, 70% (setenta por cento);
- **Simulações de Segurança**: Realizar exercícios e simulações, como testes de phishing, para educar os funcionários sobre ameaças;
- **Alterações de Acesso**: Atualizar prontamente as permissões de acesso quando um funcionário muda de função ou deixa a empresa para garantir que somente as pessoas autorizadas tenham acesso a informações sensíveis;
- **Avaliação de Risco para Mudanças de Função**: Avaliar quaisquer novos riscos de segurança que possam surgir devido a mudanças nas responsabilidades do funcionário;
- **Avaliações Regulares**: Conduzir avaliações periódicas de desempenho que incluam a aderência às políticas de segurança da informação;
- **Procedimentos de Desligamento**: Ter um processo formal de desligamento que inclua a revogação de todos os acessos a sistemas e informações da empresa;
- **Entrevistas de Saída**: Realizar entrevistas de saída para reforçar as obrigações de confidencialidade após o término do emprego.

Os setores envolvidos deverão estar em contato e em contínuo estabelecimento de melhorias quanto a estes pontos e com sugestão de aprimoramento.

10. SEGURANÇA FÍSICA E DO MEIO AMBIENTE

Medidas de segurança física devem ser implementadas para prevenir o acesso não autorizado, dano e interferência aos locais e informações da Fundação.

As medidas de segurança física e de meio ambiente são projetadas para proteger os recursos físicos da Fundação, incluindo dados, pessoal, equipamentos e instalações, contra danos

acidentais ou intencionais, desastres naturais e outras ameaças ambientais. Aqui estão algumas das medidas de segurança física e ambiental a serem implementadas e melhoradas:

- Instalação de fechaduras, portões e barreiras para restringir o acesso a áreas sensíveis;
- Sistemas de autenticação, como cartões de acesso, teclados de código PIN ou scanners biométricos;
- Utilização de câmeras de vigilância (CCTV) para monitorar e gravar atividades em áreas críticas;
- Sistemas de detecção de intrusão para alertar sobre acessos não autorizados.
- Iluminação adequada em torno das instalações para desencorajar atividades não autorizadas e facilitar a vigilância;
- Sensores de movimento e cercas eletrificadas para detectar e prevenir intrusões;
- Sistemas de detecção e supressão de incêndio, como detectores de fumaça e sprinklers;
- Extintores de incêndio e planos de evacuação claramente marcados e praticados regularmente;
- Sistemas de controle de temperatura e umidade para proteger equipamentos sensíveis, como servidores e hardware de rede;
- Detecção de vazamento de água e sistemas de drenagem para prevenir danos a equipamentos de TI;
- UPS para fornecer energia em caso de interrupção e geradores para manter operações críticas em longas falhas de energia;
- Dispositivos de supressão de surtos para proteger equipamentos sensíveis de danos causados por flutuações de energia;
- Inspeções regulares e manutenção de todos os sistemas de segurança e infraestrutura para assegurar a funcionalidade contínua;
- Cópias de segurança (backups) regulares e armazenamento off-site de dados críticos;

Implementar medidas de segurança física e ambiental é uma parte essencial da estratégia de segurança total de uma Fundação. Isso não apenas protege contra intrusões e danos mal-intencionados, mas também assegura que a Fade-UFPE possa resistir e se recuperar rapidamente de desastres naturais ou falhas de infraestrutura.

11. GESTÃO DE COMUNICAÇÕES E OPERAÇÕES

A gestão de comunicação e operações é um aspecto crítico da segurança da informação que abrange a administração e o controle dos dispositivos, processos e procedimentos que sustentam a infraestrutura de TI. Esta gestão tem como objetivo garantir que as informações e os serviços de TI sejam protegidos, confiáveis e disponíveis, minimizando os riscos de segurança e garantindo a continuidade das operações.

O que deve ser observado na Fade-UFPE quanto a este aspecto:

- Manter documentação abrangente sobre procedimentos de operações de TI, políticas de segurança, e diretrizes de configuração de sistemas;
- Gerenciar alterações em sistemas e aplicações, garantindo que todas as mudanças sejam analisadas, testadas, aprovadas e documentadas;

- Manter um inventário atualizado dos ativos de TI e garantir que as configurações de segurança estejam em conformidade com as políticas internas e padrões de mercado;
- Monitorar e analisar o desempenho e a capacidade dos sistemas para garantir que a infraestrutura de TI possa atender às demandas atuais e futuras;
- Implementar processos regulares para a aplicação de patches e atualizações de segurança, assim como para identificar e remediar vulnerabilidades;
- Proteger redes contra intrusões e ataques usando firewalls, sistemas de detecção/prevenção de intrusões e outras tecnologias de segurança;
- Estabelecer e manter um plano de resposta a incidentes de segurança da informação para lidar com eventos de segurança de forma rápida e eficaz;
- Assegurar a implementação de políticas e procedimentos de backup para recuperar dados em caso de perda ou dano, e testar regularmente os procedimentos de restauração;
- Aplicar princípios de desenvolvimento seguro, revisão de código e testes de penetração para garantir que as aplicações sejam resistentes a ataques;
- Gerenciar os direitos de acesso dos usuários, incluindo a criação, modificação e exclusão de contas de usuário e a atribuição de privilégios;
- Garantir a segurança física e ambiental dos *data centers*, bem como a manutenção e monitoramento dos sistemas críticos;
- Monitorar continuamente a infraestrutura de TI para identificar atividades suspeitas ou não autorizadas e revisar periodicamente os processos e procedimentos de operações;
- Manter todos os envolvidos informados sobre as políticas e procedimentos relevantes e fornecer treinamento necessário para garantir a compreensão e a conformidade.

12. CONTROLE DE ACESSO

A Fade-UFPE terá de forma pormenorizada a sua **POLÍTICA DE CONTROLE DE ACESSO**, de maneira que maiores informações também poderão ser obtidas neste documento. No entanto, para fins de elucidação quanto à segurança da informação, é preciso que se observem os seguintes aspectos:

- **Múltiplos Fatores**: Utilizar autenticação multifatorial (MFA) que combina algo que o usuário sabe (senha), algo que o usuário tem (token ou celular) e algo que o usuário é (biometria);
- **Senhas Fortes**: Política de senhas complexas e requisitos de mudança periódica;
- Atribuir aos usuários apenas as **permissões necessárias** para realizar suas tarefas, evitando excesso de privilégios;
- Manter um processo de **gerenciamento de identidade** para criar, manter e desativar contas de usuário, vinculando o acesso aos processos de RH para refletir mudanças de pessoal;
- **Logs de Acesso**: Registrar todas as tentativas de acesso, bem sucedidas e falhas, e manter os registros para auditoria futura;
- **Monitoramento em Tempo Real**: Utilizar ferramentas de SIEM (Security Information and Event Management) para monitoramento e alertas em tempo real de atividades suspeitas;

- **Dividir responsabilidades** entre diferentes pessoas para reduzir o risco de fraude ou erros não detectados;
- Implementar **medidas de segurança física** para restringir o acesso a áreas sensíveis, como salas de servidores ou centros de dados;
- Gerenciar o **acesso de visitantes e terceiros** rigorosamente, com acompanhamento e períodos de acesso definidos;
- **Instruir os usuários** sobre a importância do controle de acesso e como manter suas credenciais seguras;
- Ter **procedimentos claros** para responder a violações de controle de acesso, incluindo como revogar o acesso e investigar o incidente;
- Realizar **auditorias regulares e revisões de acesso** para garantir que os direitos de acesso ainda são apropriados e que não existem contas órfãs ou privilégios excessivos;
- Assegurar que o controle de acesso esteja em **conformidade com os requisitos** legais, regulatórios e de conformidade aplicáveis;
- Manter todos os **sistemas de controle de acesso atualizados** com os patches de segurança mais recentes para proteger contra vulnerabilidades conhecidas.

Implementar e manter um controle de acesso eficaz é um processo contínuo que envolve tecnologia, pessoas e processos. O objetivo é proteger os ativos de informação contra acessos não autorizados, enquanto permite que os usuários autorizados realizem suas funções de maneira eficiente e eficaz.

13. CRIPTOGRAFIA

A criptografia é uma técnica de segurança que utiliza algoritmos matemáticos para transformar informações claras (texto claro) em uma forma não legível (texto cifrado), de modo que apenas pessoas autorizadas possam entender e processar essas informações. A criptografia é essencial para proteger a confidencialidade e a integridade dos dados, bem como para garantir a autenticidade das comunicações.

É recomendável que, para proteger arquivos e dados, sejam utilizados programas de criptografia para arquivos importantes em seu computador ou quando estiverem armazenados na nuvem.

Os sistemas operacionais modernos geralmente vêm com ferramentas integradas para criptografar discos inteiros, como o BitLocker no Windows ou o FileVault no macOS.

Para comunicações seguras, recomenda-se a utilização, se for permitido, de aplicativos de mensagens que ofereçam criptografia de ponta a ponta.

Em e-mails, use extensões ou programas que suportam PGP (Pretty Good Privacy) ou S/MIME (Secure/Multipurpose Internet Mail Extensions) para criptografar mensagens.

Para transações online seguras, recomenda-se a criptografia SSL/TLS que é usada para proteger as comunicações entre o navegador da web e os servidores da web, garantindo que todas as informações transmitidas (como detalhes de cartão de crédito) sejam seguras.

14. SEGURANÇA EM RELACIONAMENTO COM TERCEIROS

A segurança da informação no contexto de relações com terceiros começa com a devida diligência e avaliação de riscos. Antes de estabelecer qualquer parceria ou delegar funções que envolvam acesso a dados sensíveis, é imprescindível avaliar a postura de segurança do terceiro, devendo este ponto ser critério de avaliação pela área de Compliance quando da aplicação da diligência de terceiros (*due diligence*)

Isto inclui verificar certificações de segurança (como ISO 27001), analisar políticas e procedimentos de segurança da informação, e compreender as práticas de gestão de riscos e resposta a incidentes do terceiro. A avaliação deve resultar em um entendimento claro do nível de risco que a parceria pode representar e das medidas necessárias para mitigá-lo.

Após a avaliação inicial, é crucial formalizar as expectativas e responsabilidades através de contratos e acordos, inclusive com cláusula de sigilo e confidencialidade que devem incluir cláusulas específicas de segurança da informação.

Esses acordos devem estabelecer requisitos claros para a proteção de dados, como o uso de criptografia, controle de acesso, e gestão de vulnerabilidades, além de definir processos de auditoria e conformidade regulatória.

Importante também é o estabelecimento de processos claros de comunicação e escalonamento no caso de incidentes de segurança, garantindo que qualquer exposição seja tratada rapidamente e de acordo com as políticas predefinidas.

Por fim, manter um monitoramento contínuo e realizar auditorias periódicas são essenciais para assegurar que os terceiros estejam cumprindo com suas obrigações contratuais relacionadas à segurança da informação. Isto pode ser alcançado através de revisões regulares de segurança, testes de penetração e avaliações de conformidade.

Além disso, é importante promover a melhoria contínua através de feedbacks, treinamentos de segurança e atualizações de políticas conforme necessário para lidar com novas ameaças e vulnerabilidades, mantendo assim uma postura de segurança robusta em todas as interações com terceiros.

15. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A gestão de incidentes de segurança da informação é um processo estruturado para identificar, responder, mitigar e aprender com os incidentes de segurança que afetam as informações e sistemas de uma Fundação. Este processo é crucial para minimizar o impacto dos incidentes e restaurar os serviços normais o mais rápido possível, enquanto preserva as evidências para análises e melhorias futuras. São etapas da gestão de incidentes:

- **Identificação de Incidentes:** O processo começa com a capacidade de detectar rapidamente atividades anormais ou suspeitas que possam indicar uma violação de

segurança. Isso geralmente é feito através de sistemas de monitoramento, alertas de segurança, análise de logs e relatórios de usuários;

- **Resposta a Incidentes:** Uma vez identificado o incidente, a resposta deve ser imediata. Equipes de resposta a incidentes (usualmente chamadas de CIRT, Computer Incident Response Team) são mobilizadas para conter a ameaça, avaliar o impacto e começar os esforços de recuperação. Isso pode incluir desligar sistemas afetados, isolar segmentos da rede ou revogar acessos;
- **Comunicação:** Durante e após um incidente, a comunicação eficaz é vital. Isso inclui notificar as partes internas relevantes, como a liderança executiva e departamentos afetados, e, quando necessário, comunicar-se com clientes, parceiros e autoridades regulatórias;
- **Recuperação:** Restaurar os serviços e processos normais é uma prioridade. Isso envolve eliminar a causa raiz do incidente, restaurar dados a partir de backups e implementar medidas para evitar a recorrência do incidente;
- **Análise e Melhoria:** Após a resolução do incidente, é fundamental realizar uma análise pós-incidente para identificar as causas, aprender com os erros e melhorar as medidas de segurança. Isso pode resultar em atualizações de políticas, reforço de infraestruturas de segurança, e treinamento adicional para a equipe.

As informações mais detalhadas, inclusive quanto ao Comitê de gestão de incidentes de segurança da informação e LGPD serão detalhadas em Política própria.

16. CONFORMIDADE

A Fade-UFPE engendrará todos os esforços para atuar em conformidade com o ambiente legal da segurança da informação, notadamente quanto a Constituição Federal, Marco Civil da Internet, Lei Geral de Proteção de Dados e ISO/IEC 27001, inclusive buscando as respectivas certificações de mercado.

Além do ambiente externo, a Fade-UFPE investirá em continuidade e treinamento das suas políticas de segurança da informação, privacidade de dados e compliance, visando a manutenção do mais alto padrão de suas atividades.

17. TREINAMENTO E COMUNICAÇÃO

Anualmente, ao fim de cada ano-calendário, a equipe de TI, Recursos Humanos, Comunicação, Compliance e Encarregado de Dados elaborará o cronograma de treinamentos anual com a temática de segurança da informação, privacidade de dados e cultura de dados na Fade-UFPE que será aprovado pela alta gestão até último dia útil de janeiro. Haverá previsão orçamentária anual para as despesas com treinamento e comunicação, de modo a que todos da Fade-UFPE sejam contemplados com treinamento e continuamente comunicados de todos os conceitos e melhores práticas organizacionais da segurança da informação.

18. AUDITORIA E MONITORAMENTO

A auditoria na segurança da informação é um processo crítico que visa avaliar e garantir que as políticas e controles de segurança de uma Fundação estão em conformidade com as normas regulamentares, padrões do mercado e objetivos internos. Ela funciona como uma checagem abrangente dos sistemas de informação para identificar vulnerabilidades e não conformidades, permitindo que a Fundação avalie a eficácia de suas práticas de segurança.

As auditorias podem ser internas, conduzidas por equipes da própria empresa, ou externas, realizadas por terceiros independentes. Tais cronogramas serão apresentados a cada fim de ano-calendário para ser implementada no ano subsequente.

A melhoria contínua é um componente essencial do ciclo de vida da segurança da informação, que segue o princípio do PDCA (Plan-Do-Check-Act).

A melhoria contínua garante que a segurança da informação se mantenha resiliente diante de um cenário de ameaças em constante evolução e de uma paisagem regulatória que pode mudar rapidamente e deve ser desenvolvida por todos que compõem a Fade-UFPE.

Reavaliações periódicas e a adaptação às novas circunstâncias são fundamentais para manter a integridade, a confidencialidade e a disponibilidade dos ativos de informação da Fundação ao longo do tempo.

19. PROCEDIMENTOS E NORMAS

Para dar maior abrangência em assuntos específicos, a Fade-UFPE descreverá procedimentos que, inicialmente, tratarão sobre:

- **Treinamento e Comunicação:** identificando o planejamento anual para a disseminação desta POLÍTICA, dos demais procedimentos inerentes e providências quanto ao comportamento digital na Fade-UFPE;
- **Contratação de Fornecedores:** visando estender as boas práticas em suas relações, a Fade-UFPE discorrerá sobre o que deve ser exigido a partir da análise de riscos dos fornecedores, dentro da diligência de terceiros, capitaneada pela Assessoria de Compliance e Controle Interno;
- **Acesso Remoto:** em face das novas dinâmicas sociais, o acesso remoto em teletrabalho será devidamente delineado para que os funcionários tenham a mesma conduta interna, ainda que o acesso seja remoto;
- **Uso da Internet:** o uso da internet é um aspecto importante da atuação de todos que fazem a Fade-UFPE. Dessa forma, o procedimento para orientação da conduta será detalhado para que os riscos na utilização sejam mitigados;
- **Uso de senhas:** a senha é sua identidade digital. Sendo assim, é preciso que se tenha consciência de sua utilização e o procedimento estará para orientar de forma ampla;
- **Encarregado de Dados:** um dos agentes da Lei Geral de Proteção de Dados é o Encarregado, figura que se conecta com o titular e a Autoridade Nacional de Proteção de Dados. O procedimento será para informar quem está na condição de Encarregado, suas

atribuições, medidas disciplinares e vinculações a esta POLÍTICA e as demais que lhes forem pertinentes;

- **Comitê de Proteção de Dados:** será formado por equipe, devidamente especializada no assunto, visando apoiar tomadas de decisões, gerenciamento de crises e formar opinião e direcionamento quanto a este assunto. Será formalizado através de Regimento Interno.

20. MEDIDAS DISCIPLINARES

Na eventualidade desta POLÍTICA ser negligenciada quanto a sua aplicação, ou mesmo, ser desabonada ou de forma direta ou indireta não colocada em prática, a Fade-UFPE poderá aplicar as medidas disciplinares cabíveis e previstas legalmente, não se resumindo a advertências, suspensões, afastamento ou mesmo o desligamento por justa causa, sem prejuízo de ações judiciais, inclusive de reparação de danos causados pela falta de atendimento das melhores práticas aqui dispostas.

21. REVISÃO DA POLÍTICA

Esta política deve ser revisada anualmente ou sempre que houver mudanças significativas nos sistemas de informação ou na Fundação, em mesma reunião que verificará o cronograma de treinamento e comunicação, realização de auditorias anuais e melhorias contínuas.