POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

(VER. 02 – JULHO DE 2024)

1. OBJETIVO

Estabelecer diretrizes para a Fundação Faculdades Integradas de Ensino Superior do Município de Linhares e sua mantida Faculdade de Ensino Superior de Linhares – Faceli, que permitam a proteção de seus ativos de informação com eficiência, eficácia, de modo seguro e transparente, garantindo a disponibilidade, integridade, autenticidade, legalidade e sigilo, de forma alinhada aos requisitos legais e exigências dos órgãos regulatórios.

2. ABRANGÊNCIA

Esta política se aplica a toda Fundação Faculdades Integradas de Ensino Superior do Município de Linhares e sua mantida Faculdade de Ensino Superior de Linhares – Faceli.

3. DOCUMENTOS COMPLEMENTARES

- Lei nº 13.709/2018 – LGPD - Lei Geral de Proteção de Dados;
- Decreto Municipal n° 1693/2022 - Regulamenta a Aplicação da LGPD no Âmbito da Administração Direta e Indireta no município de Linhares;
- Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet;
- REG-TIC-Fundação Faceli/v001 - Uso dos Recursos de Tecnologia da Informação e Comunicação;
- Resolução CD/ANPD Nº 18, de 16 de julho de 2024.

4. DEFINIÇÕES

Para a compreensão deste documento adotam-se os seguintes termos e definições:

- **Ativos**: todas as formas de criação, processamento, armazenamento, transmissão e exclusão de informações. Os ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis, etc.

- **Incidente de segurança da informação**: É um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade e confidencialidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação e Comunicações. Um incidente é qualquer evento que não faz parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção do serviço ou uma redução da sua qualidade.
- **Incidente com dados pessoais "vazamento de dados"**: Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.
- **Informação**: Conjunto de dados, imagens, textos e quaisquer outras formas de representação, dotadas de significado dentro de um contexto.
- **Informação sensível ou crítica**: Toda e qualquer informação cujo comprometimento possa causar perda de vantagem competitiva, dano ou prejuízo ao negócio ou à imagem da instituição.
- **Segurança da Informação (SI)**: A informação é um ativo das organizações, ou seja, é um bem que possui valor e, portanto, deve ser protegida, independentemente de ser escrita ou impressa em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. A segurança da informação é alcançada através da preservação de três princípios: **Confidencialidade, Integridade e Disponibilidade da informação (CID).**
- **Vulnerabilidade**: Fragilidade de um ativo que pode ser explorada e gerar danos à instituição.

5. DIRETRIZES GERAIS

As diretrizes apresentadas para a preservação e proteção das informações de propriedade e/ou responsabilidade da Fundação Faceli são essenciais para manter a

segurança da informação. Elas promovem a integridade, confidencialidade e disponibilidade dos dados da instituição, bem como a conformidade com requisitos legais.

1. **Não divulgar informações privilegiadas e/ou sigilosas sem autorização prévia**: Isso se refere à importância de não compartilhar informações confidenciais ou privilegiadas com pessoas não autorizadas. Garante que dados sensíveis sejam protegidos contra divulgação não autorizada.
2. **Evitar modificação, despersonalização ou perda da informação**: Isso destaca a necessidade de manter a integridade dos dados. A informação deve ser mantida precisa e completa, evitando alterações não autorizadas, despersonalização (perda da identificação do autor ou fonte) ou perda acidental.
3. **Fazer o descarte seguro das informações**: A correta eliminação de informações sensíveis é fundamental para evitar vazamentos de dados. Isso pode incluir a destruição segura de documentos físicos e a exclusão segura de dados digitais quando não forem mais necessários.
4. **Não armazenar, transmitir ou compartilhar conteúdo indevido ou ilegal nos ativos de propriedade e/ou responsabilidade da Fundação**: Garante que os ativos da instituição não sejam usados para armazenar, transmitir ou compartilhar conteúdo inapropriado ou ilegal, o que poderia causar problemas legais ou de reputação.
5. **Não acessar, sem a devida autorização, a estrutura lógica, física e demais ativos compartilhados da Fundação**: Isso ressalta a importância de respeitar as políticas de acesso. O acesso não autorizado a sistemas ou ativos compartilhados pode representar um risco de segurança significativo.
6. **Não utilizar de forma indevida os ativos de propriedade e/ou responsabilidade da Fundação**: As ferramentas e recursos da instituição devem ser usados apenas para fins autorizados e legítimos. O uso indevido pode prejudicar a produtividade e a segurança da informação.

6. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

6.1 Política de Backup e Armazenamento dos Dados Institucionais

O procedimento detalhado para a realização de backups dos sistemas e arquivos eletrônicos na rede institucional da Fundação Faceli está documentado no **"REG-TIC-Fundação Faceli/2023"**. Este documento contém informações importantes sobre a execução e gestão dos backups, abrangendo os seguintes aspectos:

Agendamentos: Especifica os horários e a frequência com que os backups são programados para serem realizados (diários, semanais, mensais, etc.).

Tipos de Backup: Descreve os diferentes tipos de backup utilizados, como backup completo, incremental e diferencial, cada um com sua finalidade específica e impacto na quantidade de dados armazenados.

Retenção de Dados: Define o período de tempo pelo qual os backups são mantidos, garantindo a disponibilidade de versões anteriores dos dados e cumprindo requisitos legais de retenção de informações.

Locais de Armazenamento dos Backups: Especifica os locais onde os backups são armazenados, incluindo locais físicos, servidores de backup, dispositivos de armazenamento em nuvem ou outras infraestruturas.

Processos de Restauração: Detalha os procedimentos para a restauração de backups em caso de falha ou perda de dados, incluindo a equipe responsável e a velocidade esperada de recuperação.

6.1.1 Armazenamento de Documentos

Os documentos são armazenados predominantemente em drives de rede, uma prática que otimiza a gestão de dados, oferecendo segurança e acessibilidade às informações necessárias para as operações da instituição. A seguir, destacamos as principais vantagens dessa prática:

Centralização e Eficiência: O armazenamento de documentos em drives de rede centraliza as informações em um único local, acessível de qualquer dispositivo conectado à rede. Isso facilita o compartilhamento e a colaboração entre os membros da equipe, aumentando a eficiência do trabalho.

Medidas de Segurança: Os drives de rede possuem medidas robustas de segurança, como autenticação de usuários, configuração de permissões de acesso e protocolos

de criptografia, garantindo a proteção dos documentos contra acessos não autorizados.

Acessibilidade: A disponibilização de documentos nos drives de rede permite um acesso fácil e rápido, independentemente da localização geográfica dos servidores. Isso é particularmente útil para ambientes de trabalho remoto e equipes distribuídas, como professores e outros colaboradores.

Backup: A Fundação Faceli mantém cópias de segurança dos documentos armazenados nos drives de rede por um período de 30 dias. Isso assegura que, em caso de perda de dados, os documentos possam ser recuperados em qualquer estado dos últimos 30 dias, reduzindo significativamente o risco de perdas irreparáveis.

Riscos do Armazenamento Local: O armazenamento local em dispositivos individuais, como o disco rígido C: dos computadores, apresenta riscos significativos. Esses arquivos não possuem o mesmo nível de proteção das cópias de segurança e estão suscetíveis a perdas de dados devido a falhas técnicas, erros humanos e outras eventualidades.

6.2. Incidente de Segurança da Informação

Todos os incidentes de segurança relacionados à tecnologia da informação (fragilidades e ameaças, ocorridas ou suspeitas) devem ser notificados a encarregado dos dados através de e-mail ou canal institucional disponível no site da Fundação Faceli. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

1. **Detecção de Incidentes**: Esta é a primeira etapa, se identifica possíveis incidentes de segurança. Isso pode ser feito por meio de ferramentas de segurança, monitoramento de logs, relatórios de servidores ou qualquer outra fonte de informação.
2. **Notificação**: Assim que um incidente for detectado ou suspeito, a notificação deve ser enviada ao encarregado dos dados por e-mail para o endereço lgpd@faceli.edu.br ou pelo site: https://lgpd.fundacaofaceli.edu.br/contatos/ . A notificação deve conter detalhes sobre o incidente, incluindo data, hora, localização, natureza e impacto estimado.

3. **Avaliação**: O encarregado dos dados irá junto com a Comissão Interna de Privacidade de Dados avaliar a notificação do incidente para determinar a sua gravidade e impacto potencial. Isso pode envolver a análise de evidências e a realização de investigações adicionais.
4. **Classificação do Incidente**: Com base na avaliação, o incidente pode ser classificado de acordo com sua gravidade. Isso ajuda a priorizar a resposta e as ações subsequentes.
5. **Resposta**: Uma vez que o incidente tenha sido classificado, uma equipe de resposta a incidentes de segurança deve ser acionada. Essa equipe tomará medidas para conter o incidente, minimizar danos e restaurar a normalidade.
6. **Notificação às Autoridades**: Em alguns casos, incidentes de segurança, especialmente aqueles que envolvem dados pessoais ou confidenciais, podem exigir notificação às autoridades reguladoras de privacidade de dados, de acordo com as leis aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.
7. **Investigação**: Uma investigação detalhada é conduzida para determinar a causa raiz do incidente, identificar os responsáveis e coletar evidências para futuras ações legais, se necessário.
8. **Remediação**: Com base nas descobertas da investigação, medidas corretivas são implementadas para evitar que incidentes semelhantes ocorram no futuro. Isso pode incluir aprimoramentos na segurança de TI, atualizações de políticas e procedimentos, treinamento de pessoal, entre outras ações.
9. **Comunicação**: Os usuários ou servidores devem ser informados sobre os incidentes sempre que necessário. Manter uma comunicação transparente é fundamental para preservar a reputação.
10. **Documentação**: Todas as etapas do processo, desde a detecção até a resolução, devem ser devidamente documentadas. Isso é essencial para fins de relatórios internos e conformidade regulatória.
11. **Revisão e Melhoria Contínua**: Após a resolução do incidente, é importante realizar uma revisão pós-incidente para aprender com a experiência e fazer melhorias contínuas na segurança da informação.

Registrar incidentes de segurança é uma prática de fundamental importância, desempenhando um papel vital na manutenção de um histórico detalhado e na geração de indicadores críticos. Este procedimento constitui uma estratégia indispensável para garantir a integridade e a eficácia das operações de segurança cibernética da instituição.

6.3. Incidente com Dados Pessoais

Todos os incidentes com dados pessoais devem ser notificados através do e-mail lgpd@faceli.edu.br e ou pelo site: https://lgpd.fundacaofaceli.edu.br/contatos/

O processo é composto pelas seguintes etapas:

1. **Detecção e registro**: compreende a detecção, recebimento, registro e autorizações necessárias para o encaminhamento da investigação;
2. **Investigação e contenção**: compreende a investigação e o tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias;
3. **Comunicação**: Comunicar à ANPD e ao titular de dados em caso de risco ou dano relevante aos titulares (Art.48 da LGPD);
4. **Avaliação de incidentes**: compreende a avaliação do histórico de incidentes, com consolidação de informações e indicadores, bem como a verificação das oportunidades de melhoria e lições aprendidas.
5. **Documentação**: Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

6.4 Gestão de acessos

1. **Solicitações de Acesso**: O acesso aos sistemas da Fundação não é concedido automaticamente, mas sim por meio de solicitações do gestor responsável. Os usuários que necessitam de acesso a sistemas específicos devem fazer essa solicitação. Essa abordagem controlada evita que pessoas não autorizadas acessem informações sensíveis.

2. **Início do Processo**: As solicitações de acesso são iniciadas pelo gestor responsável e ou por alguém designado. Isso garante que apenas pessoas autorizadas tenham o poder de conceder acesso aos sistemas.
3. **Níveis de Acesso:** Quando o gestor inicia uma solicitação de acesso, ele deve especificar os níveis de acesso necessários para o usuário. Isso significa que o usuário só terá acesso às informações e recursos que são essenciais para suas responsabilidades, evitando acessos desnecessários que possam representar um risco de segurança.
4. **Desligamento de Servidores:** É responsabilidade do gestor informar quando um servidor é desligado ou retirado de serviço. Isso garante que as contas de usuário relacionadas a esse servidor sejam inativadas de forma oportuna. Caso contrário, as contas inativas podem ser alvo de ataques ou uso indevido.
5. **Proteção de Dados:** O processo de gestão de acessos visa, em última instância, proteger os dados da Fundação Faceli. Ao garantir que apenas as pessoas autorizadas tenham acesso aos sistemas e que os acessos sejam revogados quando necessário, a instituição pode reduzir significativamente o risco de violações de segurança e vazamento de dados.
6. **Conformidade com Políticas de Segurança:** O processo também ajuda a assegurar a conformidade com as políticas de segurança da Fundação Faceli. Atendendo as regulamentações e padrões de segurança, bem como para manter a integridade e a reputação da instituição.

7. PRINCÍPIOS DA PRIVACIDADE DE DADOS

7.1. Ciclo de vida da informação

O ciclo de vida da informação contém etapas e eventos como produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação. Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

1. **Coleta**: é a etapa onde a informação é criada e manipulada.
2. **Retenção**: consiste no armazenamento da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.
3. **Processamento**: essa fase é quando o documento é alterado, consultado, classificado, utilizado, entre outros.
4. **Compartilhamento**: ocorre quando a informação é compartilhada com outras unidades de dentro da Fundação ou com terceiros.
5. **Eliminação**: essa fase refere-se à eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives)

7.2. Privacidade de dados: Classificação da informação e critérios de utilização

Todas as informações da Fundação devem ter um responsável definido. É recomendado que as informações sejam classificadas de acordo com seu grau de sensibilidade e confidencialidade, assegurando seu acesso pelos profissionais devidamente autorizados.

A classificação da informação deve seguir os critérios da tabela a seguir:

Classificação	Critério
Confidencial	A informação confidencial deve ser mantida em sigilo e repassada somente às pessoas que irão utilizá-las em suas atribuições. Estas informações devem ser armazenadas em diretórios auditáveis para assegurar seu controle.
Interna	A informação interna é restrita às áreas internas da Fundação, podendo ser compartilhada entre todos os servidores, colaboradores e prestadores de serviço, porém não pode ser repassada a indivíduos que não pertençam às instituições, isto é, não deve ser divulgada publicamente.
Pública	A informação pública não possui restrições de divulgação, podendo ser repassada a qualquer indivíduo, dentro ou fora da Fundação, podendo ser publicada na internet.

Essas diretrizes compõem uma política de gerenciamento de informações e segurança da Fundação:

1. **Uso de Informação:** Toda informação deve ser utilizada exclusivamente para os interesses da Fundação Faceli, que é a mantenedora, e da Faculdade Faceli, que é a mantida.
2. **Proprietários e Classificação:** Cada informação deve ser associada a um servidor responsável por sua classificação. Essa classificação deve ser atribuída no momento de sua criação.
3. **Alterações de Classificação:** Alterações na classificação da informação devem, sempre que possível, ser realizadas pelo servidor que inicialmente a classificou. Em sua ausência, servidores que assumiram sua função ou possuam nível hierárquico superior ao exigido para a classificação podem providenciar essas alterações.

4. **Descarte Seguro:** Para informações classificadas como confidenciais, o descarte deve ser realizado de maneira que torne impossível a sua recuperação.
5. **Padrão de Classificação:** Qualquer informação institucional que não seja classificada será considerada, por padrão, como informação interna.

Essas diretrizes têm o propósito de proteger a integridade e confidencialidade das informações da Fundação Faceli, que é a mantenedora, e da Faculdade Faceli, que é a mantida, bem como promover o uso responsável desses ativos de informação em conformidade com os objetivos institucionais. Elas estabelecem a base para o gerenciamento seguro da informação ao longo de seu ciclo de vida, desde a criação até o descarte.

7.3. Descarte de informações físicas e digitais

Todas as informações em papel ou em qualquer outra mídia que não sejam mais utilizadas, devem ser destruídas antes de serem colocadas no lixo. Além disso, é preciso tomar alguns cuidados ao apagar arquivos no computador, porque existem técnicas de recuperação de dados previamente apagados. O descarte de informações deve seguir as seguintes regras:

- Documentos impressos que contenham informações pessoais, financeiras ou outros dados importantes para a Fundação devem ser destruídos e não podem ser reutilizados;
- Periodicamente os servidores devem realizar uma avaliação no conteúdo dos diretórios de rede sob sua responsabilidade com o objetivo de manter no ambiente corporativo apenas informações relevantes;
- Dispositivos de armazenamento (CDs, DVDs, discos rígidos, memórias "flash" e outros meios de armazenamento) devem seguir o procedimento de descarte adequado.

8. RESPONSABILIDADES

8.1. Cabe a Gestores

- Cabe aos gestores da Fundação Faceli estabelecer as diretrizes constantes nesta política, alocar os recursos necessários à sua execução e zelar pelo seu cumprimento.

8.2. Cabe a Todos os Servidores

- Zelar pelo cumprimento da políticas, normas e procedimentos do sistema de segurança da informação;
- Garantir a proteção das informações físicas e eletrônicas, evitando a exposição de dispositivos de armazenamento removíveis, documentos impressos sobre mesas e impressoras, etc;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Relatar todo e qualquer incidente percebido;
- Zelar pela proteção de sua senha corporativa, assegurando seu caráter pessoal e intransferível;
- Participar dos treinamentos desenvolvidos pela instituição.

8.3. Cabe à Comissão Especial de LGPD

- Ofertar parecer sobre privacidade e proteção de dados pessoais nos casos em que for consultado pelo Encarregado;
- Propor, revisar e supervisionar as políticas e normas corporativas, referente a Segurança e Privacidade de Dados;
- Propor ações de capacitação e conscientização em segurança da informação, definindo o conteúdo, periodicidade e público-alvo;
- Encaminhar à comissão Especial da LGPD os incidentes ocorridos afim de avaliar violações e resultados de auditorias do sistema de segurança da informação e propor ações para tratá-las;
- Monitoramento das ações dos incidentes de segurança da informação.

8.4. Cabe ao Encarregado pelo Tratamento de Dados Pessoais

- Manter registro de incidentes e fragilidades de segurança da informação para apresentação periódica à Comissão Especial;
- Reportar quando necessário à Comissão Especial da LGPD, para análise e tomada de decisão.

8.5. Cabe a Coordenação de Tecnologia da Informação

- Fornecer o embasamento técnico necessário ao encarregado pelo tratamento de dados pessoais e à Comissão Especial, para subsidiar a tomada de decisão;
- Coordenar a implantação dos controles e processos de segurança da informação aprovados pela alta administração;
- Identificar fragilidades e ameaças significativas às informações e propor as tratativas cabíveis;
- Realizar periodicamente análise crítica independente para verificação da eficácia do sistema de segurança da informação.

9. DISPOSIÇÕES FINAIS

Os casos omissos, bem como ajustes na presente Política Institucional devem ser submetidos à apreciação e aprovação da Gestores da Fundação Faceli.

O descumprimento desta Política de Segurança da Informação poderá implicar em penalidades, consequências e medidas disciplinares, se necessário a Comissão deverá ser envolvido no processo de análise.

Esta versão substitui e revoga as versões anteriores.

10. ELABORADORES/ REVISORES

Comissão Especial para Revisão da Política de Segurança da Informação da Fundação Faceli e Implantação da Lei Geral de Proteção de Dados Pessoais (LGPD) às Atividades da Fundação Faculdades Integradas de Ensino Superior do Município de Linhares –Fundação Faceli e da Sua Mantida, Faculdade de Ensino Superior de Linhares - Faceli.

Presidente da Comissão – Coordenador de Tecnologia da Informação	Welton Castoldi

Membro – Encarregada de Dados – Analista de Gestão Pública	Cristina Giovanelli Biancardi
Membro – Analista de Sistemas	Jardel Terci Flores

11 CONTROLE DE REVISÕES

Revisão	**Data**	**Descrição**
00	03/05/2018	Emissão da Política
01	10/2023	Revisão geral no texto para adequação a LGPD.
02	07/2024	Revisão geral do texto pela direção