**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - FACULDADE 2023**

**Histórico de Versões**

|  |  |  |
| --- | --- | --- |
| Versão | Data | Alteração – Controle das Modificações |
|  | | |
| 1.1 | 30/11/23 | Lançamento da Segunda versão |
|  |  |  |
|  |  |  |
|  |  |  |

**Introdução**

A Diretriz da Política de Segurança da Informação, conhecida como PSI, é o documento que fornece orientações e estabelece as políticas corporativas para proteger os ativos de informação e prevenir responsabilidades legais para todos os usuários. Portanto, deve ser observada e implementada em todas as áreas dessa instituição. Esta PSI é fundamentada nas diretrizes propostas pela norma ABNT NBR/ISO 27001-2013, internacionalmente reconhecida como um código de prática para a administração da segurança da informação, e está alinhada com as leis em vigor em nosso país.

“Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. (ABNT NBR ISO/IEC 17799:2005).

A informação representa um componente fundamental em todos os procedimentos operacionais de qualquer empresa. Portanto, a informação é considerada o recurso mais precioso da organização e requer proteção diligente. Essa proteção é realizada por meio da implementação de regras, normas, procedimentos e políticas. Essas informações podem ser alvo de diversas ameaças que visam explorar vulnerabilidades, resultando em possíveis danos significativos.

A criação de um processo de gestão da segurança da informação é indispensável para possibilitar a implementação efetiva de controles de segurança. Nesse sentido, esse processo deve incluir o estímulo à elaboração de políticas de segurança da informação e comunicações. É necessário adotar padrões de comportamento alinhados com as exigências de segurança da informação pertinentes às necessidades comerciais e à proteção legal da organização, das informações e dos indivíduos.

A segurança da informação engloba três fundamentos essenciais, que são:

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

● Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, com as devidas autorizações.

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

**Objetivos**

Definir diretrizes e normas que possibilitem que alunos, professores e outros prestadores de serviços sigam padrões de comportamento desejáveis e aceitáveis, em conformidade com a legalidade e boas práticas, com o objetivo de reduzir riscos técnicos e jurídicos;

Garantir a confidencialidade, integridade e disponibilidade das informações da Faculdade;

Assegurar a regularidade e a continuidade das operações da Faculdade, protegendo os processos críticos contra falhas ou desastres significativos;

Prevenir potenciais incidentes e mitigar a responsabilidade legal da instituição, seus funcionários, prestadores de serviços, alunos e demais envolvidos.

**Responsabilidades**

Usuários em Geral

Aderir integralmente às políticas, normas e procedimentos de Segurança da Informação, incluindo as regras estabelecidas neste documento.

Assegurar a proteção das informações contra acesso, alteração, divulgação ou destruição não autorizados.

Garantir que os recursos tecnológicos sejam empregados exclusivamente para propósitos profissionais e/ou acadêmicos aprovados e que estejam alinhados aos interesses da instituição. Ou seja, empregar os recursos computacionais e informacionais de maneira ética, legal e consciente.

Informar imediatamente à administração sobre qualquer violação desta Política de Segurança da Informação.

Gestores e Administradores

Demonstrar postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os alunos, colaboradores e prestadores de serviços sob sua responsabilidade.

Ajustar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para estar em conformidade com esta Política de Segurança da Informação (PSI), assim como outras políticas correlatas.

Solicitar aos usuários a assinatura, seja de forma manual ou digital, do Termo de Responsabilidade, assumindo o compromisso de aderir às normas estabelecidas nesse documento e de manter sigilo e confidencialidade.

Assegurar que todos tenham acesso e compreensão desta política, assim como das normas e procedimentos aqui delineados. Sempre que necessário, comunicar atualizações relacionadas a processos ou cadastros, a fim de que as permissões de acesso adequadas sejam concedidas ou revogadas conforme a necessidade.

Realizar decisões administrativas em relação ao descumprimento da Política de Segurança da Informação (PSI).

Setor de TI (Área da Informática)

Avaliar a eficácia dos controles empregados e comunicar aos gestores os riscos remanescentes.

Estabelecer diretrizes para a instalação de software nos dispositivos e supervisionar o acesso dos usuários à internet.

Supervisionar o ambiente de Tecnologia da Informação, criando indicadores e registros, como o uso da capacidade instalada da rede e dos equipamentos, incidentes de segurança e acessos não autorizados.

Ajustar os dispositivos, ferramentas e sistemas fornecidos aos colaboradores, implementando todos os controles necessários para atender aos requisitos de segurança estabelecidos por esta Política de Segurança da Informação (PSI).

**Rede interna**

O acesso à internet deve ser restrito ao âmbito profissional e educacional, com conteúdo relacionado às atividades desempenhadas para os objetivos propostos pela faculdade, sempre mantendo uma conduta compatível com a moralidade. Neste acesso, os colaboradores utilizarão suas credenciais de rede, que são empregadas para realizar o login nas estações de trabalho. Dessa forma, é fundamental seguir as regras implementadas que são mencionadas a seguir.

1. O uso de provedores de acesso externos ou qualquer outra forma de conexão não autorizada é estritamente proibido e inaceitável.
2. É proibido acesso às páginas de conteúdo considerado ofensivo, ilegal ou impróprio, como pornografia, Violência, Jogos, Apostas e Chats de bate-papos fora do contexto da Organização.
3. O uso de serviços de proxy anônimo não é permitido.
4. A conexão à internet via cabo nas mesas estará disponível exclusivamente para os dispositivos de propriedade da organização, destinando-se apenas à execução das atividades laborais.
5. A autenticação do WiFi é necessária através do uso de usuário e senha pelo colaborador, visando garantir o registro adequado dos acessos realizados por eles.
6. A rede WiFi é designada apenas para o acesso à internet por dispositivos corporativos, no entanto, pode ser utilizada para fins pessoais, contanto que não interfira no andamento do trabalho nos setores.
7. A utilização de programas para análise de tráfego, detecção de vulnerabilidades, captura de pacotes ou qualquer outro que possa causar sobrecarga ou comprometer o funcionamento adequado e a segurança da rede interna é expressamente proibida, salvo nos casos em que o objetivo seja conduzir auditorias de segurança.
8. Qualquer modificação nos níveis de acesso existentes será efetuada somente mediante solicitação formal, acompanhada da justificativa adequada. Essa solicitação será avaliada, e, se necessário, poderá ser recusada.
9. A divulgação de informações importantes para a Organização em redes sociais, fóruns, blogs ou qualquer outro meio de comunicação é proibida.
10. As requisições para liberar acesso a um site específico devem ser formalmente encaminhadas à equipe de TI por meio do procedimento oficial, acompanhada de uma justificativa detalhada. A organização reserva o direito de recusar a solicitação conforme seu critério.

**Política de Uso de Senhas**

A senha é o método mais comum utilizado pelo usuário para acessar o sistema ou sua máquina, representando um recurso pessoal e intransferível que resguarda a identidade do colaborador. Dispositivos de identificação e senhas desempenham uma função fundamental na salvaguarda da identidade do usuário, impedindo a usurpação por parte de terceiros. A utilização inadequada de dispositivos e/ou senhas alheias é configurada como crime de acordo com o Código Penal Brasileiro (art. 307 – falsidade ideológica).

Com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1. A responsabilidade pela senha é integralmente atribuída ao usuário, sendo estritamente vetada a sua divulgação ou empréstimo. Em caso de suspeita de divulgação da senha, é necessário comunicar o setor de Tecnologia da Informação para efetuar o reset.
2. A senha inicial atribuída ao colaborador é temporária e deve ser modificada no primeiro acesso, sendo essencial memorizá-la.
3. As senhas devem possuir entre 10 e 15 caracteres, incluindo obrigatoriamente pelo menos um número e uma letra maiúscula, além de ao menos um caractere especial do conjunto (!-@#\_/). Por questões de segurança, é recomendável evitar a inclusão de informações pessoais, como data de aniversário, nomes de filhos, nome do cônjuge, entre outros. Exemplo: Z#10wardog
4. Após 4 (quatro) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o setor de TI.
5. Os usuários têm permissão para modificar suas próprias senhas e devem ser orientados a fazê-lo se suspeitarem que terceiros obtiveram acesso não autorizado às suas credenciais de login.
6. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

**Política de uso do E-mail**

● O uso do correio eletrônico é para fins corporativos e/ou acadêmicos relacionados às atividades do usuário dentro da instituição. A utilização desse serviço para fins pessoais não é permitida.

● Os e-mails enviados ou recebidos de endereços externos podem ser monitorados para bloquear malwares, spams ou outros conteúdos que violem a Política de Segurança da Informação.

● É proibido enviar mensagens que tenha conteúdo considerado impróprio, obsceno ou ilegal.

● É proibido enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Faculdade vulneráveis a ações civis ou criminais;

● Recomenda-se que as mensagens de correio eletrônico sempre incluam uma assinatura com o formato especificado pela área de comunicação, juntamente com um rodapé que solicita ao destinatário a preservação do sigilo das informações encaminhadas.

● É proibido baixar arquivos desconhecidos anexados em e-mails de remetentes não reconhecidos.

**Política de uso de Ativos**

Os dispositivos fornecidos aos colaboradores, assim como os que estão disponíveis nos laboratórios devem permanecer acessíveis pelo maior período possível, a fim de evitar prejuízos em suas atividades laborais. Cada usuário é responsável por utilizar e manusear os equipamentos adequadamente para as atividades institucionais, além de seguir as orientações presentes nos procedimentos operacionais fornecidos.

Algumas diretrizes e medidas de segurança devem ser adotadas, são elas:

1. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do setor de TI.
2. Cabe aos usuários (colaboradores e acadêmicos) zelarem pelo equipamento de informática utilizado, garantindo que estes estejam sempre em condições ideais de uso e limpeza. É terminantemente proibido aplicar adesivos e fotos para personalizar o equipamento, assim como danificar a etiqueta de patrimônio associada a ele.
3. O uso de software sem a devida licença é proibido.
4. Ao se ausentar da estação de trabalho, é necessário que o usuário bloqueie seu computador para evitar o acesso de terceiros à sua estação.
5. Todos os terminais de computador e impressoras devem ser protegidos por senha (bloqueados) quando não estiverem em uso.
6. O consumo de alimentos, bebidas e tabaco é rigorosamente proibido, nos laboratórios, mesas de trabalho, salas de aula e nas proximidades dos equipamentos.
7. Os sistemas e computadores devem contar permanentemente com versões do software antivírus instaladas, ativadas e atualizadas.
8. A instalação de software só pode ser realizada pela equipe do setor de Tecnologia da Informação.
9. O usuário é responsável por manter a configuração do equipamento fornecido, aderindo aos controles de segurança estabelecidos pela Política de Segurança da Informação e pelas normas específicas da instituição. Ele assume a responsabilidade como custodiante das informações.
10. Os documentos e arquivos referentes às atividades organizacionais devem ser armazenados exclusivamente no servidor de rede para funcionários ou drive na nuvem para os acadêmicos, nunca no disco local da máquina.

**Uso do Backup**

A implementação de uma Política de Backup (cópia de segurança) é um dos procedimentos fundamentais da Segurança da Informação. A organização deve estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra no caso de um incidente de perda de dados. É essencial realizar backups periodicamente, preferencialmente fora do horário comercial, durante as chamadas "janelas de backup" – períodos nos quais há pouco ou nenhum acesso de usuários ou processos automatizados aos sistemas de informática.

Seguem as regras:

1. Os responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida, sugestões de melhorias, entre outros.
2. As mídias de backup devem ser conservadas em um ambiente seco, limpo e com controle climático, afastadas da exposição direta à luz solar, e devem ser devidamente identificadas com a data e hora em que o backup foi realizado.
3. Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial
4. O tempo de vida e uso das mídias de backup deve ser monitorado e controlado, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.
5. Em caso de falha no backup e/ou restauração, é crucial que o procedimento seja realizado prontamente, no primeiro horário disponível, assim que o responsável tenha identificado e resolvido o problema.
6. Deve-se realizar testes de restauração (restore) de backup aproximadamente entre 30 e 50 dias, ajustando a frequência de acordo com a criticidade do backup.

**Penalidades para violação da Política de Segurança**

O descumprimento ou inobservância de quaisquer regras desta Política de Segurança definidas nesse documento constituem falta grave, às quais o colaborador ou acadêmico responderão com a aplicação de medidas administrativas, caso necessário, cíveis e judiciais cabíveis.

Em caso de descumprimento das normas estabelecidas, o usuário poderá enfrentar as seguintes sanções:

Advertência verbal:

O infrator receberá uma advertência verbal e as Normas e diretrizes da organização, com orientação para revisar a Política de Segurança da Informação.

Advertência formal:

O infrator será formalmente advertido, com identificação da norma infringida, e será instruído a assinar o termo de não conformidade.

Segunda Advertência formal:

O infrator será formalmente advertido, com identificação da norma infringida, e será orientado a assinar o termo de não conformidade. Nesse caso,ele não poderá desempenhar suas atividades diárias até passar por uma reciclagem no setor de informática.

**Considerações Finais**

Da mesma maneira que a ética, a segurança deve ser considerada uma parte fundamental da cultura desta organização. Em outras palavras, qualquer incidente de segurança implica que alguém está agindo contrariamente aos princípios éticos e aos bons costumes que devem ser seguidos por esta instituição.

Qualquer dúvida relacionada a este documento deve ser abordada com o setor de TI. Situações ou cenários não descritos nesta Política de Segurança da Informação devem ser encaminhados ao mesmo.

Este documento pode ser atualizado posteriormente, com alterações em suas novas versões, em resposta a eventos significativos que possam surgir e que não tenham sido abordados nesta Política de Segurança da Informação (PSI).

Belo Horizonte, dezembro de 2023.