POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

Aprovado pelo Parecer do CONSEPE, n. 070/2021 de 22 de novembro de 2021

BAURU

2021

SUMÁRIO

1. CONTEXTUALIZAÇÃO

O UNISAGRADO possui compromisso de resguardar e proteger os dados – sejam eles pessoais ou não, que estão sob sua guarda.

Nesse sentido, a presente **Política de Segurança de Informação (PSI)** apresenta diretrizes gerais de conduta, bem como obrigações a serem seguidas no UNISAGRADO a fim de mitigar eventuais riscos e danos relacionados a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das informações de qualquer natureza, objetivando garantir sua preservação.

Amparada nos preceitos da Norma ISO 27001, padrão internacional para processos de gestão da segurança da informação, a PSI UNISAGRADO define também papéis e responsabilidades para a implantação dos seguintes controles da informação.

2. DEFINIÇÕES

AMEAÇA: evento que tem potencial em si próprio para comprometer os objetivos da Instituição, seja trazendo danos diretos aos ativos ou prejuízos indiretos decorrentes de situações inesperadas.

TIPOS DE INFORMAÇÃO: são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso às informações, assim como as próprias informações coletadas, produzidas, processadas, armazenadas, custodiadas, descartadas e transmitidas pelo UNISAGRADO.

AUTENTICIDADE: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

CLASSIFICAÇÃO DA INFORMAÇÃO: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada e credenciada.

CONFORMIDADE: processo que visa verificar o cumprimento das normas estabelecidas.

CONTROLE DE ACESSO: conjunto de procedimentos, recursos, meios utilizados com a finalidade de conceder ou bloquear o acesso.

CRIPTOGRAFIA: método de codificação da informação que visa evitar que ela seja comprometida ou alterada por pessoas não autorizadas;

CUSTODIANTE DO ATIVO DE INFORMAÇÃO: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

DADOS PESSOAIS: todo e qualquer dado relacionado à pessoa natural identificada ou identificável (conforme definição trazida no art. 5º, I, da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais), inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estiverem relacionados a uma pessoa. Também são considerados dados pessoais para fins da lei aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12, §2, LGPD).

DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido.

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações relacionadas a incidentes com ativos de informação do UNISAGRADO.

FORNECEDORES: no contexto da Instituição são considerados fornecedores os outros terceiros contratados e subcontratados, pessoa física ou jurídica, não enquadrados como parceiros comerciais.

GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO: conjunto de processos que permite identificar e implementar as medidas de proteção necessários para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação.

INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, softwares, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica.

INTEGRIDADE: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): Lei 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei (arts. 1º e 17 da LGPD).

PARCEIROS COMERCIAIS: no contexto do UNISAGRADO, são considerados parceiros comerciais os terceiros contratados, pessoa física ou jurídica, que atuam em seu nome: Consultores, Conveniadas e Agentes Comerciais (aqueles que indicam atividades onde a Instituição pode atuar como contratada).

QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

SEGURANÇA DE COMUNICAÇÕES: processo de proteção de dados em trânsito.

SISTEMA ESTRUTURANTE: conjunto de sistemas de informática fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente.

TERCEIROS: São os parceiros comerciais e os fornecedores do UNISAGRADO.

TRATAMENTO DA INFORMAÇÃO: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.

VULNERABILIDADE: fragilidade de um ativo ou grupo que pode ser explorada por uma ou mais ameaças.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Estabelece o compromisso do UNISAGRADO em resguardar e proteger as informações, sejam elas pessoais ou não que estão sob sua guarda, além de definir a governança de segurança da informação da IES.

Esta Política de Segurança da Informação exige o cumprimento do **Manual de Integração, Normas e Procedimentos internos** e de todas as leis e regulamentações aplicáveis e em vigor relacionadas à proteção de dados incluindo, sem limitação, a Lei Geral de Proteção de Dados (LGPD) e a General Data Protection Regulation (GDPR).

Esta política se insere nas diretrizes e regimentos internos do UNISAGRADO como sendo o documento que estabelece as diretrizes do Programa de Conformidade com a Lei Geral de Proteção de Dados Pessoais.

4. DESTINATÁRIOS

A presente Política se aplica a todos os membros da Reitoria, Vice-Reitoria, CONSEPE, Assessoria Jurídica, aos corpos técnico-administrativo, docente e discente, estagiários, aprendizes, professores convidados, parceiros comerciais (consultores, agentes comerciais e conveniadas) que atuam em nome do UNISAGRADO e fornecedores (outros contratados e subcontratados pela Instituição) e que, no âmbito dessa relação, possam acessar as áreas, equipamentos, informações, arquivos, redes e dados de titularidade ou propriedade da IES.

Desta forma:

Todos os destinatários deverão observar as presentes regras e recomendações em quaisquer operações que possam impactar na segurança das informações no UNISAGRADO. O não cumprimento das disposições ora previstos, sujeitará o infrator às sanções previstas fixadas pelo Comitê Central de Governança de Dados previsto nesta Política, sem prejuízo das medidas previstas em lei, caso aplique.

5. APLICABILIDADE

Esta Política estabelece as diretrizes para garantir que seus destinatários entendam e cumpram as leis de proteção de dados pessoais bem como os padrões e medidas técnicas visando à segurança da informação no UNISAGRADO.

6. OBJETIVOS

A PSI UNISAGRADO - Política de Segurança da Informação, tem como objetivos:

- Estabelecer as diretrizes que assegurem e reforcem o compromisso da Instituição com as práticas e medidas preventivas garantidoras de segurança da informação;
- Definir o referencial para a normatização das questões de segurança no UNISAGRADO;
- Criar condições para que a IES eleve continuamente a sua maturidade em segurança da informação por meio da adoção de diretrizes, normas e procedimentos, destinados a proteger os ativos de informação da Instituição visando à promoção da integridade, confidencialidade, autenticidade e disponibilidade dos ativos de informação do UNISAGRADO.
- Prover a Instituição de mecanismos de atendimento e conformidade às leis de segurança da informação, nacionais e internacionais.

- Descrever as regras comportamentais e diretrizes a serem seguidas na condução das atividades desenvolvidas pela IES que garantam a prevenção de incidentes de segurança da informação e a proteção de dados pessoais.

Os demais documentos do UNISAGRADO que se relacionam com esta Política são:

- Manual de Integração, Normas e Procedimentos.
- Normas e procedimentos – Tecnologia da Informação P01-004
- Todas as outras disposições internas

Cada um desses documentos tem seu objetivo específico, mas em todos está evidenciado o compromisso do UNISAGRADO com a segurança da informação.

7. PRINCÍPIOS

Os compromissos do UNISAGRADO com o tratamento adequado das informações se baseia nos seguintes princípios:

- Autenticidade – todos os esforços serão feitos para que as informações sejam confiáveis e corretas, ou seja, as informações não serão alteradas de forma não autorizada ou indevida;
- Confidencialidade – o acesso à informação é permitido somente para pessoas autorizadas e quando for de fato necessário;
- Disponibilidade – somente as pessoas autorizadas tem acesso à informação sempre que necessário;
- Integridade – todos os esforços serão feitos para que as informações sejam exatas e completas, bem como seu processamento.

8. DIRETRIZES

8.1 DIRETRIZES GERAIS

- A gestão de segurança da informação no UNISAGRADO é de responsabilidade do Comitê Central de Governança de Dados cujos membros são indicados pela Reitoria.

- O cumprimento desta Política e de suas normas de procedimentos complementares deve ser avaliado periodicamente por meio de verificações de conformidade, realizadas pelos CONTROLADORES.
- O UNISAGRADO, além das diretrizes estabelecidas nesta PSI, deve também se orientar pelas melhores práticas e procedimentos de segurança da informação recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões relacionados à segurança da informação.

8.2 DIRETRIZES E NORMAS COMPLEMENTARES ESPECÍFICAS

Para cada um dos controles complementares propostos pela ISO 27001 o Comitê Central de Governança de Dados deve elaborar estratégias, diretrizes e normas de procedimentos complementares, assim como manuais, procedimentos de conduta e avaliações periódicas de conformidade.

A PSI UNISAGRADO preconiza a implantação priorizada das seguintes normas de procedimentos com as seguintes diretrizes:

8.2.1 GESTÃO DE ATIVOS DE INFORMAÇÃO (Controle ISO 27001):

Os ativos de informação devem:

a) Ser inventariados e protegidos;
b) Ter identificados os seus proprietários custodiantes;
c) Ter mapeadas as suas ameaças, vulnerabilidade e interdependências;
d) Ter a sua entrada e saída nas dependências do UNISAGRADO autorizadas e registradas por autoridade competente;
e) Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;
f) Ser regulamentados por norma de procedimentos específica quanto a sua utilização; e
g) Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

E, além disso:

- O UNISAGRADO deve criar e gerir uma política de classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor;
- Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas;
- Os sistemas de informação e as aplicações da IES devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas;
- Dependendo do grau de sigilo da informação, o acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite do termo de sigilo e responsabilidade;
- Os ativos de informação devem possuir mecanismos que permitam à auditoria dos eventos de acesso a alteração dos registros. Esta auditoria deve estar sempre ativa (salvo quando explicitamente dispensado este requisito) e os registros devem ser armazenados pelo período mínimo de um ano.

8.2.2 GESTÃO DE RISCOS E INCIDENTES (CONTROLE ISO 27001 #12)

- O gestor dos ativos de informação deve estabelecer processos de Gestão de Riscos de Segurança da Informação – GRSI que possibilitem identificar ameaças e reduzir vulnerabilidades dos ativos de informação, assim como reduzir os impactos de eventuais incidentes com os mesmos;
- A GRSI é um processo contínuo e deve ser aplicada na implementação e operação da Gestão de Segurança da Informação, levando em consideração o planejamento, execução, análise crítica e melhoria da SI no UNISAGRADO.

8.2.3 SEGURANÇA EM RECURSOS HUMANOS (CONTROLE ISO 27001 #3)

a) Os destinatários devem ter ciência:
   - Das ameaças e preocupações relativas à segurança da informação e;
   - De suas responsabilidades e obrigações no âmbito desta PSI.

b) Todos os destinatários devem difundir e exigir o cumprimento da PSI, das normas de segurança e da legislação vigente acerca do tema;
c) Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os destinatários, de acordo com seu relacionamento e atribuições no UNISAGRADO.

8.2.4 SEGURANÇA DAS OPERAÇÕES DE TI DO UNISAGRADO (ISO 27001 #7)

a) O controle de usuários de sistemas:
- É de responsabilidade do titular da unidade da IES juntamente com o RH; e
- Deve ser implementado controles de perfis, permissões e procedimentos necessários para salvaguarda dos ativos de informação do UNISAGRADO.

8.2.5 SEGURANÇA DAS OPERAÇÕES DE TI DO UNISAGRADO (CONTROLE ISO 27001 #7)

O setor de Tecnologia da Informação, através do Comitê Central de Governança de Dados, deve estabelecer normas de procedimentos específicas contendo diretrizes de segurança da informação para a disponibilização e execução dos serviços, sistemas e infraestruturas de recursos tecnológicos do UNISAGRADO.

8.2.6 SEGURANÇA DAS COMUNICAÇÕES DO UNISAGRADO (CONTROLE ISO 27001 #9)

O Comitê Central de Governança de Dados deve estabelecer normas de procedimentos específicas contendo diretrizes de segurança da informação para a disponibilização de serviços de comunicação relacionados aos ativos de informação do UNISAGRADO.

8.2.7 ASSINATURA DIGITAL E CRIPTOGRAFIA (CONTROLE ISO 27001 #6)

O setor de Tecnologia da Informação, através do Comitê Central de Governança de Dados, deve estabelecer normas de procedimentos específicas contendo parâmetros para o uso de assinaturas digitais que reflitam as necessidades específicas de garantia e autenticidade dos dados do UNISAGRADO.

Também deve ser estabelecida norma específica ditando quando e onde recursos criptográficos devem ser utilizados dentro da Instituição para proteger suas informações, além de estabelecer quais padrões de criptografia são aceitáveis.

8.2.8 CONTROLES DE ACESSOS (CONTROLE ISO 27001 #5)

O setor de Tecnologia da Informação e o setor de Recursos Humanos, através do Comitê Central de Governança de Dados, devem estabelecer normas de procedimentos específicas contendo parâmetros para a gestão de acesso aos dados UNISAGRADO, atendendo os requisitos abaixo:

a) Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.
b) Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.
c) Os usuários do UNISAGRADO são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.
d) A identificação do usuário, qualquer que seja o meio e a forma, deverá ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.
e) A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso, além do necessário dependente de prévia autorização do gestor da área responsável pela informação.
f) Todos os sistemas de informação da Instituição, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.
g) Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do UNISAGRADO ou bloqueados em caso de afastamento.
h) Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:
    - Ao acesso às suas bases de dados;
    - A extração, carga e transformação de dados e;

- Aos serviços acessíveis via linguagem de programação;

i) Os sistemas estruturantes devem possuir mecanismos automáticos para:
   - Revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;
   - Bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor, e;
   - Tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema;

8.2.9 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS (CONTROLE ISO 27001 #10)

O setor de Tecnologia da Informação, através do Comitê Central de Governança de Dados, deve editar norma de procedimentos específica estabelecendo critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e sustentação de sistemas.

8.2.10 RELAÇÃO COM FORNECEDORES (CONTROLE ISO 27001 #11)

O UNISAGRADO, através do Comitê Central de Governança de Dados, deve estabelecer norma de procedimentos específica que vise o atendimento de demandas em segurança da informação para contratos, convênios, acordos e afins, conforme os requisitos abaixo:

a) Os acordos com terceiros que possuam algum relacionamento com ativos de informação da Instituição devem observar as disposições da PSI UNISAGRADO.
b) Os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PSI e de suas normas complementares.
c) O contrato, convênio, acordo ou instrumento congênere devem prever a obrigação da outra parte de divulgar esta PSI e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no UNISAGRADO.
d) Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

8.2.11 GESTÃO DE INCIDENTES (CONTROLE ISO 27001 #12)

O Comitê Central de Governança de Dados ficará responsável pelo tratamento e resposta a incidentes de segurança, sendo informado imediatamente caso ocorra algum incidente na IES.

8.2.12 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO EM CONTINUIDADE DAS ATIVIDADES (CONTROLE ISO 27001 #13)

O setor de Tecnologia da Informação, através do Comitê Central de Governança de Dados, deve instituir metodologias e norma de procedimentos que enderecem tratativas de segurança da informação relacionadas à disponibilidade dos ativos de informação do UNISAGRADO.

8.2.13 GESTÃO DE CONFORMIDADE (CONTROLE ISO 27001 #1)

a) Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de segurança da informação do UNISAGRADO e de suas unidades administrativas com esta PSI e suas normas de procedimentos complementares, bem como com a legislação específica de segurança da informação.
b) A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o UNISAGRADO.
c) O calendário de ações de verificação de conformidade é elaborado com base na priorização dos riscos identificados ou percebidos.
d) Nenhum setor da Instituição deve permanecer sem verificação da conformidade de segurança da informação por período superior a 2 (dois) anos.
e) É vedado aos prestadores de serviços executar a verificação da conformidade de segurança da informação dos próprios serviços prestados;
f) A verificação de conformidade pode combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.
g) Os resultados de cada ação de verificação de conformidade são documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Comitê Central de Governança de Dados, da unidade verificada, para ciência e tomada das ações cabíveis.
h) Para que seja possível efetuar as verificações de conformidade, a equipe delegada pelo Comitê deve possuir acesso aos ambientes computacionais do UNISAGRADO.

8.2.14 PLANO DE INVESTIMENTOS EM SEGURANÇA DA INFORMAÇAO DO UNISAGRADO

a) Os investimentos em segurança de informação serão realizados de forma planejada e consolidados em um plano de investimentos plurianual.
b) O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, o produtório entre a probabilidade de ocorrência e o impacto do risco no negócio ou na imagem do UNISAGRADO.
c) Os planos de investimento e seus orçamentos são produzidos, apresentados e geridos pelo Comitê de Segurança da Informação.

9 PAPÉIS E RESPONSABILIDADE REFERENTES À SEGURANÇA DA INFORMAÇÃO

9.1 O COMITÊ CENTRAL DE GOVERNAÇA DE DADOS deve:

a) Supervisionar a segurança da informação no âmbito do UNISAGRADO;
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
c) Elaborar normas específicas que complementem esta Política em consonância com a Política da Estrutura Normativa da IES;
d) Conduzir apurações quando da suspeita de ocorrências e incidentes em segurança da informação na Instituição;
e) Avaliar e aprimorar continuamente a PSI UNISAGRADO e suas normas de procedimentos complementares, visando a sua aderência aos objetivos institucionais da IES e às legislações aplicáveis vigentes;
f) Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PSI UNISAGRADO;
g) Monitorar e avaliar periodicamente o plano estratégico de segurança da informação, assim como determinar os ajustes cabíveis;
h) Apoiar a Reitoria e Pró-Reitorias da Instituição no planejamento dos investimentos em segurança da informação com base nas exigências estratégicas e legais;
i) Coordenar as atividades de tratamento e reposta a incidentes de segurança;
j) Promover a recuperação de sistemas junto à área de TIC responsável;

k) Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança da informação, e avaliando condições de segurança de redes por meio de verificações de conformidade;
l) Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
m) Analisar ataques e intrusões na rede UNISAGRADO;
n) Executar ações necessárias para tratar quebras de segurança;
o) Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
p) Apurar ações que violem a PSI UNISAGRADO ou quaisquer de suas diretrizes e normas de procedimentos. Aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor; e
q) Participar de fóruns, redes nacionais e internacionais relativas à segurança da informação.

9.2 OPERADORES

Cabe aos operadores:

a) Seguir as diretrizes desta Política;
b) Garantir a segurança dos ativos de informação sob sua responsabilidade;
c) Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta Política;
d) Conceder e revogar acessos aos ativos de informação;
e) Comunicar ao Comitê Central de Governança de Dados a ocorrência de incidentes de segurança da informação;
f) Designar custodiante dos ativos de informação, quando aplicáveis.

9.3 CUSTODIANTE DO ATIVO DE INFORMAÇÃO

O Custodiante do Ativo de Informação:

a) Deve proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PSI.

b) Deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

9.4 CONTROLADOR UNISAGRADO

Cabe ao Controlador do UNISAGRADO:

a) Conscientizar os usuários sob sua supervisão em relação às políticas e normas de segurança da informação UNISAGRADO;
b) Incorporar aos processos de trabalho de sua unidade, ou de sua área, boas práticas em segurança da informação;
c) Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão;
d) Garantir a realização do tratamento e a classificação da informação definidos nas Políticas e normas de procedimentos;
e) Autorizar, de acordo com a legislação vigente e as diretrizes do Comitê Central de Governança de Dados, a divulgação das informações produzidas na sua unidade administrativa;
f) Comunicar ao Comitê Central de Governança de Dados os casos de quebra de segurança;
g) Solicitar suporte ao Comitê Central de Governança de Dados quando perceber riscos ou suspeitas de incidentes em segurança da informação;
h) Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores;
i) Informar o setor de Recursos Humanos sobre a movimentação de pessoal de sua unidade.

10 TERCEIROS E PARCEIROS COMERCIAIS DO UNISAGRADO

Cabe aos terceiros e Parceiros Comerciais:

a) Tomar conhecimento e seguir as diretrizes estabelecidas pelo UNISAGRADO em relação à segurança da informação;

b) Disponibilizar listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação, objetos dos contratos;
c) Fornecer toda documentação dos sistemas, produtos, serviços relacionados às suas atividades;

APÊNDICES

APÊNDICE A - USO E ACESSO DE INTERNET NO UNISAGRADO

A. POLÍTICAS E PROCEDIMENTOS

Do presente procedimento constam normas de natureza técnica, inerentes à organização produtiva e execução do trabalho. O Centro Universitário Sagrado Coração - UNISAGRADO, com vistas à melhor organização e funcionamento, resguarda o seu direito de promover, unilateralmente, alterações que respondam às suas necessidades, interesses e/ou conveniência, sem qualquer reflexo jurídico nos contratos de trabalho.

B. OBJETIVO

Definir o uso aceitável da Internet dentro do sistema de comunicação do UNISAGRADO de modo a torná-la útil à instituição e seus funcionários. O uso inaceitável da Internet pode comprometer o bom nome da IES.

C. MONITORAMENTO

O UNISAGRADO afirma nesta política, como também no contrato de trabalho de cada colaborador, que o uso da internet, e-mail, telefonia e todos os demais recursos de informática, são ferramentas valiosas para seus negócios; entretanto, o mau uso destas pode ter impacto negativo na produtividade dos funcionários, e a própria reputação da Instituição. Todos os recursos tecnológicos da empresa existem para o propósito exclusivo de seu negócio, portanto a IES se dá o direito de monitorar toda sua utilização, a fim de identificar qualquer desacordo com as normas da instituição e legislação vigente.

D. POLÍTICA

É proibido (sob pena de punição):

- Acessar a Internet usando nomes ou senhas (passwords) de outras pessoas;
- Tentar experiências novas de acesso, para as quais não está autorizado;
- Navegar em páginas não éticas, ou explorar páginas sem objetivos definidos;

- Publicar qualquer documento, de natureza contratual ou não contratual, que conste do Manual de Procedimento do UNISAGRADO "Revisão, Aprovação e Publicidade de Documentos Contratuais ou não contratuais";
- Publicar informação de propriedade do UNISAGRADO através de meios eletrônicos;
- Enviar informações confidenciais ou de propriedade do UNISAGRADO, através de e-mail, a não ser que estas estejam protegidas pela codificação e aprovada pela Tecnologia da Informação, área do UNISAGRADO que cuida da tecnologia da informação;
- Fazer o download de qualquer programa executável DOS /não DOS, se não tiver o programa de antivírus aprovado pela Tecnologia da Informação, instalado no seu PC;
- Usar o e-mail para SPAMs, correntes (correspondência externa coletiva não solicitada).

b) Censura Automática

O sistema será monitorado através de logs de acesso dos usuários, e censurará qualquer material que contrarie leis vigentes e a doutrina da instituição. Assim, qualquer conotação com os assuntos abaixo relacionados sofrerá bloqueio:

- Comentários raciais depreciativos;
- Material de Conteúdo Sexual, não educativo;
- Comentários depreciativos às pessoas físicas ou jurídicas e/ou instituições;
- Linguagem ofensiva sob qualquer alegação;
- Qualquer material que possa refletir negativamente sobre o UNISAGRADO;
- Conteúdo proibido por leis locais ou regulamentos;
- Difamação ou ataques abusivo-depreciativos de um indivíduo ou de um grupo;
- Anexação de declarações políticas;
- Uso da Internet para ganho pessoal.
- Uso pessoal da Internet, exceto nos casos relativos aos negócios do UNISAGRADO.

Aos coordenadores dos departamentos caberá a responsabilidade de assegurar que o uso da Internet por seus funcionários esteja de acordo com estes procedimentos, e que seu uso pessoal não interfira nos negócios do UNISAGRADO.

Seguir a política de acesso à Internet permitida pelo UNISAGRADO e não tentar o acesso não autorizado. Fornecer sempre a fonte correta e legítima e a informação de endereço (nome do usuário, endereço do e-mail, servidor, etc.) para logons, anexos de e-mail, etc.

E. EXCEÇÕES

Exceções deste procedimento deverão ser documentadas e aprovadas pelo Comitê Central de Governança de Dados e Diretoria do UNISAGRADO.

APÊNDICE B - ALTERAÇÃO DE SENHAS DE ACESSO AOS SERVIDORES

A. POLÍTICAS E PROCEDIMENTOS

Do presente procedimento constam normas de natureza técnica, inerentes à organização produtiva e execução do trabalho. O UNISAGRADO, com vistas à melhor organização e funcionamento, resguarda o seu direito de promover, unilateralmente, alterações que respondam às suas necessidades, interesses e/ou conveniência, sem qualquer reflexo jurídico nos contratos de trabalho.

B. OBJETIVO

Estabelecer critérios de acesso e utilização aos computadores (servidores) em ambiente de rede. Este procedimento estabelece quem terá acesso aos servidores do UNISAGRADO, mostra como selecionar as pessoas que devem ter a senha de acesso, e como informá-las da responsabilidade desse conhecimento.

C. POLÍTICA

É dever dos coordenadores, responsáveis pelos departamentos envolvidos:

1 - Enviar, a Tecnologia da Informação, um documento (e-mail ou SCI – Sistema de Chamados Internos), contendo o nome completo da pessoa autorizada, data de nascimento e CPF, bem como as áreas disponíveis do usuário, sempre que qualquer acesso seja criado;

2 - Informar, a Tecnologia da Informação, para a liberação de uma senha de acesso, o nome do usuário responsável e autorizado a utilizar tal servidor;

3 – A Tecnologia da Informação ao criar usuário criará também uma senha temporária que deve ser alterada nos primeiros acessos;

4 - A senha de acesso deverá ter o tamanho mínimo de oito caracteres, composta de alfanuméricos e caracteres especiais e a mesma será renovada automaticamente a cada 60 dias.

D. EXCEÇÕES

Todas as exceções deste procedimento deverão ser documentadas e aprovadas pelo Comitê Central de Governança de Dados e Diretoria do UNISAGRADO.

APÊNDICE C - CADASTRO E MANUTENÇÃO DE SENHAS DE SISTEMAS CORPORATIVOS

A. POLÍTICAS E PROCEDIMENTOS

Do presente procedimento constam normas de natureza técnica, inerentes à organização produtiva e execução do trabalho. O UNISAGRADO, com vistas à melhor organização e funcionamento, resguarda o seu direito de promover, unilateralmente, alterações que respondam às suas necessidades, interesses e/ou conveniência, sem qualquer reflexo jurídico nos contratos de trabalho.

B. OBJETIVO

Estabelecer critérios para mudança e/ou cadastramento de senhas para os sistemas corporativos da Instituição e telefonia. Entende-se por sistemas corporativos os seguintes sistemas aplicativos:

- Sistema Acadêmico
- Sistema Financeiro
- Sistema Atendimento Odontológico
- Sistema de Agendamento
- Sistema Administrativo
- Telefonia

Entende-se por sistema de telefonia, acesso com usuário (PIN) e senha pessoal, individual e intransferível para realização de chamadas telefônicas conforme nível de acesso determinado pelo coordenador do setor responsável e aprovado pela diretoria do UNISAGRADO. (Este procedimento contém instruções relativas à seleção das pessoas que devem conhecer a senha de acesso e informações sobre a responsabilidade desse conhecimento).

C. MONITORAMENTO

O UNISAGRADO afirma nesta política, como também no contrato de trabalho de cada colaborador, que o uso da internet, e-mail, telefonia e todos os demais recursos de informática, são ferramentas valiosas para seus negócios; entretanto, o mau uso destas pode ter impacto negativo, produtividade dos funcionários, e a própria reputação da IES. Todos os recursos tecnológicos da empresa existem para o propósito exclusivo de seu negócio, portanto

a Instituição se dá o direito de monitorar toda sua utilização, a fim de identificar qualquer desacordo com as normas da Instituição e legislação vigente.

D. POLÍTICA

Para a liberação de uma senha de acesso ao sistema, os coordenadores responsáveis dos departamentos, deverão informar a Tecnologia da Informação, o nome do usuário responsável e autorizado a utilizar o menu principal do aplicativo, bem como os grupos de programas existentes em cada submenu. Entende-se como grupos de programas aplicativos, toda e qualquer rotina de atualização, consulta relatórios e rotinas de encerramento que possa ter.
Toda e qualquer nova senha que necessite ser criada, deverá o coordenador responsável do departamento envolvido, enviar a Tecnologia da Informação um documento (e-mail ou SCI – Sistema de Chamados Internos) com o nome completo da pessoa autorizada, data de nascimento e CPF, bem como quais os níveis do menu principal que irá utilizar.
Em hipótese alguma a Tecnologia da Informação irá cadastrar qualquer senha para qualquer sistema aplicativo se não tiver em mãos o documento de autorização e acesso ao sistema aprovado previamente pelo coordenador responsável do departamento.
A Tecnologia da Informação deverá ser comunicada imediatamente quando houver qualquer desligamento do funcionário do UNISAGRADO até então autorizado a acessar quaisquer sistemas aplicativos descritos acima, para que se possa cancelar a senha de acesso.

E. EXCEÇÕES

Exceções deste procedimento deverão ser documentadas e aprovadas pelo Comitê Central de Governança de Dados e Diretoria do UNISAGRADO.

APÊNDICE – D CADASTRO E UTILIZAÇÃO DE E-MAILS CORPORATIVOS

A. POLÍTICAS E PROCEDIMENTOS

Do presente procedimento constam normas de natureza técnica, inerentes à organização produtiva e execução do trabalho. O UNISAGRADO, com vistas à melhor organização e funcionamento, resguarda o seu direito de promover, unilateralmente, alterações que respondam às suas necessidades, interesses e/ou conveniência, sem qualquer reflexo jurídico nos contratos de trabalho.

B. OBJETIVO

Estabelecer normas e informar aos colaboradores do UNISAGRADO quais atividades são permitidas e proibidas quanto ao uso de correio eletrônico.

C. MONITORAMENTO

O UNISAGRADO afirma nesta política, como também no contrato de trabalho de cada colaborador, que o uso da internet, e-mail, telefonia e todos os demais recursos de informática, são ferramentas valiosas para seus negócios; entretanto, o mau uso destas pode ter impacto negativo na produtividade dos funcionários, e a própria reputação da Instituição. Todos os recursos tecnológicos da empresa existem para o propósito exclusivo de seu negócio, portanto a IES se dá o direito de monitorar toda sua utilização, a fim de identificar qualquer desacordo com as normas da instituição e legislação vigente.

D. POLÍTICA

O uso do correio eletrônico do UNISAGRADO é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o UNISAGRADO e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do UNISAGRADO:

• enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

• enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o UNISAGRADO vulneráveis a ações civis ou criminais;

• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

• produzir, transmitir ou divulgar mensagem que:

- ✓ Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do UNISAGRADO;
- ✓ Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- ✓ Contenha arquivos com código executável (exe.,com.,bat.,pif.,js.,vbs.,hta.,src.,cpl. reg.,dll. e inf.) ou qualquer outra extensão que represente um risco à segurança;
- ✓ Vise obter acesso não autorizado a outro computador, servidor ou rede;
- ✓ Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- ✓ Vise burlar qualquer sistema de segurança;
- ✓ Vise vigiar secretamente ou assediar outro usuário;
- ✓ Vise acessar informações confidenciais sem explícita autorização do proprietário;
- ✓ Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- ✓ Inclua imagens criptografadas ou de qualquer forma mascaradas;
- ✓ Contenha anexo(s) superior (es) a 20 MB para envio (interno e internet) e 20 MB para recebimento (internet)
- ✓ Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- ✓ Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- ✓ Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- ✓ Tenha fins políticos locais ou do país (propaganda política);

- ✓ Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

• Nome do colaborador
• Setor
• Nome da empresa
• Telefone(s)
• Correio eletrônico

E. EXCEÇÕES

Exceções deste procedimento deverão ser documentadas e aprovadas pelo Comitê de Segurança e Diretoria do UNISAGRADO.

APÊNDICE E - NORMA PARA ATUALIZAÇÃO E APLICAÇÃO DE PATCH DE SEGURANÇA

A. POLÍTICAS E PROCEDIMENTOS

Do presente procedimento constam normas de natureza técnica, inerentes à organização produtiva e execução do trabalho. O Centro Universitário Sagrado Coração, com vistas à melhor organização e funcionamento, resguarda o seu direito de promover, unilateralmente, alterações que respondam às suas necessidades, interesses e/ou conveniência, sem qualquer reflexo jurídico nos contratos de trabalho.

B. OBJETIVO

Estabelecer normas para aplicação de patchs de segurança nos serviços críticos de tecnologia da informação do UNISAGRADO de modo a torná-la útil à instituição e seus funcionários.

C. POLÍTICA

A aplicação de patches é uma tarefa a ser realizada pelos administradores dos serviços, para garantir que os serviços permaneçam em operação de forma segura e estável.

Havendo correções ou atualizações disponibilizadas pelo fabricante aos sistemas operacionais das estações e dos servidores, ou sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas em até 15 (quinze) dias, a fim de se evitar que estes sistemas fiquem vulneráveis.

É necessário diariamente monitorar a liberação de patches de segurança para os serviços críticos de tecnologia da informação

Para serviços Microsoft, deverá ser utilizada a ferramenta para gerenciamento da distribuição de patches chamada WSUS ou similar.

Os patches de segurança devem ser instalados sempre que disponíveis, porém antes da instalação eles deverão ser:

- ✓ Homologados em ambiente segregado;
- ✓ Analisados e documentados no plano de implantação, contendo plano de teste e de Disaster Recovery;
- ✓ Aprovados.

APÊNDICE F - UTILIZAÇÃO DE COMPARTILHAMENTO E ARMAZENAMENTO DE ARQUIVOS NOS SERVIDORES

A. POLÍTICAS E PROCEDIMENTOS

Do presente procedimento constam normas de natureza técnica, inerentes à organização produtiva e execução do trabalho. O Centro Universitário Sagrado Coração, com vistas à melhor organização e funcionamento, resguarda o seu direito de promover, unilateralmente, alterações que respondam às suas necessidades, interesses e/ou conveniência, sem qualquer reflexo jurídico nos contratos de trabalho.

B. OBJETIVO

Definir o uso aceitável do compartilhamento e armazenamento de arquivos dentro dos servidores de arquivos do UNISAGRADO conhecidos também com File Servers de modo a torná-la útil à utilização da instituição e seus funcionários. O uso inaceitável da área de armazenamento que possibilita o compartilhamento de pastas e arquivos com devido controle de acesso, garantindo toda segurança e auditoria dos arquivos.

C. MONITORAMENTO

O UNISAGRADO afirma nesta política, como também no contrato de trabalho de cada colaborador, que o uso da internet, e-mail, telefonia e todos os demais recursos de informática, são ferramentas valiosas para seus negócios; entretanto, o mau uso destas pode ter impacto negativo na produtividade dos funcionários, e a própria reputação da Instituição. Todos os recursos tecnológicos da empresa existem para o propósito exclusivo de seu negócio, portanto a IES se dá o direito de monitorar toda sua utilização, a fim de identificar qualquer desacordo com as normas da instituição e legislação vigente.

D. POLÍTICA

Recomendações

a. Arquivos de escritório (doc, xls, pdf, txt, entre outros): a cópia deste tipo de arquivo é permitida, recomendamos que todos os arquivos sensíveis e importantes sejam armazenados nesta área.

b. Arquivos de imagens (jpg, png, bmp, psd, entre outros): a cópia deste tipo de arquivo é monitorada, recomendamos o armazenamento de fotos digitais no servidor, caso esse tipo de arquivo seja institucional.

c. Todos os setores do Unisagrado têm direito a um espaço de armazenamento de arquivos para uso entre seus colaboradores. Caso não possua, basta abrir um Chamado de Solicitação de Atendimento Técnico. Essa área é de uso exclusivo do setor que solicita e não pode ser compartilhada com outros setores. Caso ocorra a necessidade de um espaço entre mais de um setor, o mesmo deve ser solicitado da mesma forma que explicado antes.

Restrições

a. Arquivos de áudio e vídeo (avi, mp3, wav, wmv): caso esse tipo de arquivo seja institucional recomendamos o armazenamento, não sendo institucional, não devem ser armazenados no servidor de arquivos.

b. Não é permitido compartilhamento de pastas e arquivos em computadores e/ou qualquer outro equipamento.

c. A fim de evitar problemas, não misturar arquivos pessoais com arquivos de trabalho.

E. EXCEÇÕES

Exceções deste procedimento deverão ser documentadas e aprovadas pelo **Comitê Central de Governança de Dados** e Diretoria do UNISAGRADO.

UNISAGRADO

Ensino Superior de Excelência