Fundação Salmina

Pelas Pessoas. Para a Vida.

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E COMUNICAÇÃO

Código:	FUSA.POL.006
Versão / Revisão:	000 – Emissão Inicial
Data de Emissão:	Abril 2026
Próxima Revisão:	Abril 2027 (ou após evento significativo)
Norma de Referência:	ISO 27001
Base Legal:	
Elaborado por:	Vanda Parruque
Revisto por:	
Aprovado por:	Patrício Chemane
Distribuição:	

Visão Geral

A reputação, a estabilidade dos negócios e o desenvolvimento da Fundação Salmina (FUSA), são dependentes de como gerenciamos e protegemos as informações e os sistemas de informação, como armazenamos e acessamos a nossa propriedade intelectual, informações de funcionários, informações de clientes e informações telemáticas que coletamos de nossos clientes.

Nossa rede corporativa pode se tornar um alvo para hackers e outros criminosos cibernéticos, ou nossas informações podem ser potencialmente vulneráveis a outras ameaças à confidencialidade, integridade ou acessibilidade. Portanto, implementamos esta Política de Segurança de Informação para garantir que todos os funcionários ajudem a proteger estas informações por meio da adoção, implementação e manutenção de proteções e controles adequados e apropriados.

Os usuários também podem receber revisões periódicas desta política. A FUSA reserva-se o direito de alterar esta política ou permitir exceções aprovadas a qualquer momento.

ÍNDICE

Objectivo

Esta política define os controles físicos, técnicos e administrativos necessários para proteger a Informação e os Sistemas de Informação e Comunicação.

Todos os usuários de Informações e Sistemas de Informação e Comunicação devem se familiarizar com os requisitos deste documento, política central e de quaisquer documentos de política suplementares adicionais. Os usuários devem relatar imediatamente qualquer conflito entre esta política e as leis existentes.

Âmbito

Esta política aplica-se a todos os usuários de informações da FUSA armazenadas eletronicamente, em papel ou de outra forma, e aos sistemas usados para armazenar as informações. Os usuários de Informação e Sistemas de Informação e Comunicação podem incluir funcionários, consultores, contratados e pessoal temporário contratado para trabalhar em nome da FUSA.

Definições

4.1. CISO - Chief Information Security Officer - Diretor de Segurança da Informação.

4.2. FUSA – Fundação Salmina.

4.3. Contratado - Qualquer não funcionário da FUSA que esteja contratualmente obrigado a fornecer alguma forma de serviço à FUSA.

4.4. Mídia eletrônica - Qualquer componente de qualquer sistema de informação usado para armazenar informações, incluindo, mas não se limitando a, discos rígidos magnéticos, discos rígidos de estado sólido (SSDs), discos compactos (CDs), DVDs, unidades flash compactas, unidades flash USB, mídia de backup de fita e dispositivos móveis.

4.5. Indivíduos - Pessoas vivas que podem ser identificadas, direta ou indiretamente, a partir das informações de que a FUSA dispõe. Por exemplo, um indivíduo pode ser identificado diretamente pelo nome ou indiretamente por gênero, cargo e localização do escritório, se você puder usar essas informações para descobrir quem ele é. Indivíduos incluem funcionários,

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

indivíduos dentro dos clientes e fornecedores da FUSA. Os indivíduos também incluem parceiros em parcerias e empresários em nome individual.

4.6. IT - Tecnologia de Informação – o Departamento dentro da FUSA é responsável por fornecer sistemas e serviços de informação.

4.7. Informação - Dados tangíveis e intangíveis ou dados em todas as formas, incluindo dados que são observados ou transmitidos oralmente, em forma eletrônica, escrita ou outra forma tangível.

4.8. Sistema de informação - Qualquer equipamento ou sala da FUSA usado para gerenciar, processar, acessar ou armazenar informações e que seja usado no curso da execução de negócios, incluindo, mas não se limitando a, desktops, computadores, laptops, smartphones, tablets, impressoras, redes de dados e voz, dispositivos em rede, softwares, dados armazenados eletronicamente, dispositivos portáteis de armazenamento de dados, serviços de rede de terceiros, aparelhos de telefone, sistemas de videoconferência e todos os outros itens semelhantes comumente entendidos como abrangidos por este termo.

4.9. Senha - Uma sequência arbitrária de caracteres escolhida por um usuário que é usada para autenticar o usuário no processo de login, a fim de impedir o acesso não autorizado à sua conta.

4.10. Dados pessoais - Qualquer informação sobre um indivíduo (ver definição acima) que o identifica ou permite que ele seja identificado em conjunto com outras informações que são mantidas. Inclui informações desse tipo usadas em um contexto business to business.

Os dados pessoais são definidos de forma muito ampla e abrangem coisas como nome, endereço, endereço de e-mail (incluindo em um contexto de negócios, endereços de email de indivíduos em empresas como nome. sobrenome@organisation.com), endereço IP e também tipos de dados mais confidenciais como filiação sindical, dados genéticos e crenças religiosas. Dados pessoais são um elemento de informações confidenciais (definido abaixo).

4.11. Informações de identificação pessoal ("PII") - Informações que podem ser usadas isoladamente ou com outras informações para identificar, contactar ou localizar um indivíduo (por exemplo, cliente, funcionário, consumidor ou outro indivíduo), ou para identificar o

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

indivíduo no contexto de outras informações, incluindo o contexto de uma relação comercial com a FUSA. PII inclui; REVER A LEI NOVA

i Nome

ii Endereço físico

iii Número de telefone

iv Endereço de e-mail

v Data de nascimento

vi Número da segurança social

vii Números de cartão de crédito *

viii Números de carta de condução*

ix Números de identidade emitidos pelo governo*

x Números de passaporte*

xi Conta poupança, conta corrente, números de contas financeiras, códigos de segurança, PINs e senhas*

xii Apólice de seguro saúde ou outra conta de saúde*

xiii Histórico médico, saúde mental e física, diagnóstico e tratamento médico e informações sobre deficiência*

xiv Verificações de antecedentes de funcionários, incluindo relatórios de crédito, relatórios de consumos de crédito*

xv Endereço de e-mail em combinação com a senha ou pergunta de segurança e resposta que permitiria o acesso a uma conta online *

xvi Orientação ou preferências sexuais *

PII também são categorizadas como Informações confidenciais.

PII é um elemento de Informação Sensível.

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

4.12 Direcção de Procurement e Logística - A organização dentro da FUSA responsável pela aquisição de equipamentos, materiais e suprimentos para a FUSA.

Sanitização - O processo de remoção de Informações da Mídia Eletrônica antes da reutilização ou descarte. As técnicas de higienização incluem o uso de comandos "apagar" ou "formatar", apagar seguro e destruição física. O tipo de Mídia Eletrônica e a sensibilidade das Informações contidas, podem ditar o tipo de sanitização apropriado.

4.13 Informação sensível - Meios: informações da FUSA que podem causar perdas ou danos significativos ou substanciais à fundação, incluindo perdas econômicas e danos à reputação, se as Informações forem divulgadas publicamente ou acessadas por pessoas não autorizadas. Exemplos deste tipo de informação sensível incluem informações financeiras confidenciais da fundação, propriedade intelectual, projetos de produtos, desenhos de engenharia, processos de fabricação, planos de negócios confidenciais, planos e estratégias de fusão e aquisição, etc. Consulte o Código de Ética para obter exemplos e descrições adicionais de o que pode ser considerado Informação Sensível.

4.13Técnico de informática - Pessoa responsável pela manutenção dos Sistemas de Informação.

4.14Utilizador - Qualquer funcionário da FUSA ou contratado que tenha sido autorizado a acessar qualquer Informação da fundação ou Sistema de Informação.

5. Papéis e Responsabilidades

5.1. Técnicos de informática – Responsáveis pela manutenção dos Sistemas de Informação.

5.2. Administradores de sistema - Responsáveis pela administração de todos os Sistemas de Informação.

5.3.CISO – Responsável pela gestão do IT, pelo desenvolvimento, manutenção e monitoramento do cumprimento desta política e pela definição de padrões e procedimentos com objectivo de manter a confidencialidade, integridade e disponibilidade dos Sistemas de Informação e Informação. O CISO pode autorizar exceções a esta política, conforme apropriado.

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

5.4. Departamento Jurídico - Responsável por garantir o cumprimento legal de todas as atividades desenvolvidas no âmbito desta política e pela proteção jurídica da FUSA e dos seus ativos tangíveis e intangíveis.

5.5. Todas as descrições de trabalho do usuário incorporam responsabilidades para manter a segurança da informação e os supervisores incorporarão a adesão a essas responsabilidades nas avaliações de desempenho.

Controle de Acesso e Gerenciamento de Contas

6.1. IDs de usuário e senhas exclusivas - Após a aprovação dos Recursos Humanos na contratação inicial, ou a qualquer momento pelo CISO, os Administradores de Sistema fornecerão a cada Usuário as ID´s exclusivas para acesso aos Sistemas de Informação.

6.2. Grupos/ ID´s compartilhadas - Os administradores do sistema não podem fornecer ID´s compartilhadas e ou em grupos sem a devida permissão por escrito do CISO.

6.3. Acesso a arquivo / utilitário padrão - Os Administradores do Sistema irão configurar o acesso padrão a qualquer novo arquivo adicionado ou utilitário instalado no Sistema de Informação de forma que o Sistema de Informação bloqueie o acesso de Usuários não autorizados.

6.4. Controle de acesso baseado em função - Os Administradores do Sistema configurarão os privilégios de acesso dos Usuários com base em suas funções na FUSA, conforme determinado pelos Recursos Humanos.

6.5. Acesso de terceiros - O CISO deve fornecer aprovação por escrito para qualquer acesso aos Sistemas de Informação para um terceiro não afiliado.

6.6. Revogação de acesso - A FUSA pode revogar o acesso de um Usuário às Informações ou aos Sistemas de Informação a qualquer momento.

6.7. ID´s de usuários inativos - Os administradores do sistema devem configurar o sistema para desabilitar as ID´s após quarenta e cinco (45) dias de inatividade. Os usuários podem solicitar a reativação após longos períodos de ausência.

6.8. Exclusão de ID´s de usuário inativos - Os Administradores do sistema devem configurar o sistema para excluir a ID do usuário após ele permanecer inativo por cento e vinte (120)

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

dias. Os usuários podem solicitar uma exceção de Recursos Humanos para longos períodos de ausência.

6.9. Remoção de direitos de acesso - Para rescisões voluntárias, os Administradores do Sistema removerão todo o acesso físico e eletrônico do Usuário rescindido às Informações, Sistemas de Informação e instalações da FUSA imediatamente após a rescisão. Para encerramentos involuntários, os Administradores do sistema devem desabilitar o acesso do Usuário encerrado antes do encerramento.

6.10. Privilégios de usuário do administrador do sistema - O CISO deve aprovar a criação ou concessão de qualquer ID de usuário com privilégios de administrador do sistema. Os Administradores do sistema devem ter pelo menos dois IDs de usuário - um que fornece acesso privilegiado e outro para uso diário que fornece apenas acesso normal do usuário.

6.11. Acesso privilegiado ao utilitário - Os administradores do sistema configurarão o sistema para restringir o acesso aos utilitários que podem exibir o status de segurança do sistema ou modificar as configurações de segurança do sistema apenas para administradores do sistema.

6.12. Revisão dos direitos de acesso - O CISO revisará semestralmente os privilégios concedidos a cada usuário para determinar se os direitos de acesso atuais do usuário ainda são apropriados para as funções de trabalho do usuário.

6.13. Manuseio, acesso e uso de informações - Os usuários devem apenas acessar, usar e processar as informações da FUSA de acordo com todas as políticas e padrões e para os fins comerciais expressamente autorizados pela administração.

6.14. Isenção de responsabilidade de dados e danos ao programa - A FUSA pode usar vários tipos de controles de acesso e outras medidas de segurança semelhantes destinadas a proteger a confidencialidade, integridade e disponibilidade dos Sistemas de Informação e Informação da FUSA. Sem aviso ou notificação, a FUSA pode;

1. Restringir ou revogar os privilégios de qualquer usuário;

2. Inspecionar, copiar, remover e alterar qualquer dado, programa ou outro recurso do sistema que possa representar uma ameaça às Informações da FUSA e / ou Sistemas de Informação;

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

3. Tomar quaisquer outras medidas necessárias para proteger as Informações da FUSA ou Sistemas de Informação. A FUSA não é responsável por qualquer perda ou dano aos dados pessoais ou software do Usuário que resulte de tais medidas de proteção.

Gerenciamento de Renha

7.1. Senhas iniciais - Os administradores do sistema deverão definir a expiração de uma nova senha inicial do usuário, o que forçará o usuário a criar uma nova senha antes de concluir o login. As informações de login e senha do novo usuário serão fornecidas ao Administrador do Sistema por e-mail.

7.2. Complexidade da senha - O usuário não deve usar nenhuma senha previsível ou qualquer parte de uma senha que possa ser facilmente adivinhada, incluindo palavras de dicionário, palavras estrangeiras, gírias, dialetos ou abreviações, derivados do ID do usuário, sequências de caracteres comuns incluindo quaisquer caracteres repetidos ou qualquer outro detalhe pessoal, como apelidos, nomes de crianças, nomes de animais de estimação, datas de nascimento ou aniversário de casamento. As senhas devem consistir no seguinte:

7.2.1. Pelo menos 8 caracteres.

7.2.2. Não deve conter espaços.

7.2.3. Não deve conter mais de 3 caracteres idênticos em uma linha.

7.2.4. As senhas devem conter três das quatro regras de complexidade de senha.

7.2.4.1. Pelo menos um caractere alfabético minúsculo.

7.2.4.2. Pelo menos um caractere alfabético maiúsculo.

7.2.4.3. Pelo menos um caractere numérico.

7.2.4.4. Pelo menos um símbolo do conjunto de @ # $% ^ & * () _ + | - = \ '} {[]: "' ~ <>?,. /.

O uso de uma frase secreta pode ser útil ao escolher uma senha segura que ainda seja fácil para o usuário lembrar. Por exemplo, um usuário pode usar uma frase secreta "Isto pode ser uma maneira de lembrar" que resulta em uma senha "TmB1w2R" ou "Tmb1W> r".

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

7.3. Senhas semelhantes - Quando um usuário altera sua senha, a nova senha não deve ser substancialmente semelhante à senha antiga, incluindo, por exemplo, o uso de uma senha de base significativamente semelhante com a alteração de "1," "2," "3" ...

7.4. Expiração de senha - Os usuários devem alterar suas senhas pelo menos a cada noventa (60) dias. Os Administradores de sistema implementarão políticas de sistema apropriadas para solicitar que um usuário altere sua senha após noventa (60) dias ou sempre que se justificar e antes que o login possa ser concluído.

7.5. Senhas reutilizadas - O usuário não pode reutilizar nenhuma das últimas vinte e quatro (24) senhas utilizadas anteriormente.

7.6. Senhas após uma intrusão - Os administradores do sistema marcarão todas as senhas do usuário para expirar após qualquer violação real ou suspeita da segurança do sistema que possa afetar ou envolver as senhas do usuário.

7.7. Ferramentas de quebra de senha e verificação - O CISO pode aprovar o uso de ferramentas de quebra e / ou cracking de senha de forma periódica ou aleatória, sem aviso prévio. Se a senha de um usuário for descoberta ou quebrada com sucesso durante este processo, o usuário será notificado por e-mail e precisará alterar sua senha no próximo login para estar em conformidade com as regras de complexidade da senha (Seção 7.2) desta política.

7.8. Solicitações de alteração de senha - O usuário pode solicitar uma redefinição de sua própria senha entrando em contato com o Serviço de Apoio após a verificação da identidade do usuário ou usando o utilitário de redefinição de senha automático. Os usuários não têm permissão para solicitar redefinições de senha para outros usuários sem o consentimento expresso do Administrador de Sistema. Os usuários serão notificados por e-mail quando abrirem um tíquete no Serviço de Apoio após qualquer solicitação para alterar suas senhas. Se um usuário alterar sua senha, ele não poderá alterá-la novamente por 72 horas, a menos que entre em contato com o serviço de apoio e um administrador do sistema permita a alteração da senha.

7.9. Bloqueios de conta - A conta do usuário será bloqueada após 3 tentativas incorretas de senha. Um usuário pode solicitar que sua conta seja desbloqueada ou sua senha redefinida entrando em contato com o Serviço de Apoio após a verificação da identidade do usuário.

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

7.10. Senhas comprometidas - Se um usuário acredita que sua senha foi comprometida de alguma forma, o usuário deve alterar imediatamente sua senha no sistema afetado e notificar o Serviço de Apoio da extensão e escopo da divulgação suspeita.

7.11. Armazenamento de senhas - Exceto para a divulgação inicial de uma nova senha por um Administrador do Sistema a um usuário, os usuários nunca devem anotar as senhas ou armazenar sua senha eletronicamente de forma (incluindo, mas não se limitando a, arquivos em lote, scripts de login automático, macros de software, arquivos de configuração ou cofres de chaves) que não requerem criptografia protegida por outra senha.

7.12. Compartilhamento de senhas - Exceto para a divulgação inicial de uma nova senha por um administrador do sistema para um usuário, os usuários nunca devem compartilhar senhas ou de outra forma revelar qualquer senha emitida pelo usuário a outro indivíduo, incluindo um assistente administrativo do usuário ou supervisor de assinatura, ou compartilhada com o pessoal de TI. Os usuários não devem discutir sobre qualquer senha com outras pessoas ou documentar a senha em nenhum questionário. Os usuários não devem fornecer dicas de senha para outras pessoas. Os usuários devem relatar quaisquer solicitações de divulgação de sua senha ao CISO.

7.13. Senhas em sistemas diferentes - Os usuários devem usar uma senha diferente em cada sistema da FUSA e não devem reutilizar nenhuma senha de um sistema externo (incluindo sistemas como Facebook, Google, Yahoo, Twitter, Amazon e também incluindo o computador pessoal doméstico do próprio usuário, roteador, tablet) em qualquer sistema da FUSA.

7.14. Dicas de senha - Se um sistema exigir o uso de "dicas" de senha para recuperar uma senha esquecida, os usuários não devem usar informações precisas. Por exemplo, se uma dica de senha solicitar o nome da cidade onde um usuário nasceu e o usuário nasceu em Maputo, o usuário deve inserir "Pemba" ou uma resposta não respondida como "Mambas" em vez de "Maputo."

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

Área de Trabalho Limpa

8.1. Computadores autônomos - Os usuários devem fazer logo off e / ou bloquear a tela com um protetor de tela protegido por senha que oculta o conteúdo da tela enquanto está longe do computador. As telas dos usuários serão bloqueadas / desconectadas automaticamente após 30 minutos de inatividade.

8.2. Área de Trabalho Limpa - Os usuários devem limpar todas as informações confidenciais da aérea de trabalho no final das horas de trabalho e garantir que todas as informações confidenciais foram devidamente protegidas em pastas definidas no Nextcloud.

Gestão de ativos

9.1. Etiquetas de ativos - Quando apropriado, o TI anexará um número de etiqueta de patrimônio exclusivo a cada peça de computador e equipamento de comunicação. Os usuários estão proibidos de remover ou alterar essas etiquetas de ativos.

9.2. Compras - O TI adquirirá todos os componentes de hardware e software para garantir a compatibilidade com os padrões de segurança de hardware e software aplicáveis.

9.3. Localização de ativos - O CISO realizará periodicamente e sem aviso prévio uma pesquisa da localização de todos os ativos de informações da FUSA, incluindo a localização de todas as informações armazenadas física e eletronicamente.

9.4. Desativação Remota para Sistema de Informação Perdido / Roubado - A FUSA pode instalar software em cada Sistema de Informação usado para acessar a rede da FUSA que desativa e / ou apaga automaticamente todas as Informações do dispositivo. A FUSA também pode usar software de rastreamento em sistemas de informação emitidos pela FUSA que podem ser usados para localizar ou apagar remotamente dispositivos perdidos.

Licenciamento de Software

10.1. Licenças de software - A FUSA usa softwares licenciados, não vendido. A FUSA e seus usuários devem cumprir os direitos limitados de uso do software de acordo com o contrato de

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

licença e conforme permitido por lei. O uso de software não licenciado pode expor a FUSA e os Usuários à responsabilidade por violações de direitos autorais, marcas registradas e / ou patentes. Os usuários não devem exceder os direitos limitados concedidos por qualquer contrato de licença. Os usuários que fazem uso de software não licenciado ou excedem os direitos concedidos no contrato de licença o fazem em seu próprio nome e sem a aprovação da FUSA.

10.2. Instalação de software pelo usuário - Os usuários não devem instalar software de propriedade da FUSA em seus computadores pessoais, servidores de rede ou outros sistemas de informação sem autorização prévia do TI. Apenas Administradores de Sistema têm permissão para instalar e / ou atualizar software nos Sistemas de Informação.

10.3. Compartilhamento de software - Os usuários não devem copiar nenhum software para qualquer meio eletrônico de armazenamento, transferir software instalado em um Sistema de Informação para outro Sistema de Informação ou compartilhar ou divulgar qualquer software externamente ou com outro Usuário.

10.4. Cópia de software - Os usuários não devem copiar nenhum software ou sua documentação, a menos que tal cópia seja permitida pelos contratos de licença aplicáveis e seja previamente aprovada pelo TI.

10.5. Aquisições de software - O TI deve comprar e registrar todos os softwares usados nos Sistemas de Informação da FUSA ou usados para fins comerciais.

10.6. Software Pessoal - Os usuários não devem instalar o software que adquiriram para seu uso pessoal em qualquer Sistema de Informação sem autorização prévia do TI.

10.7. Registro de software - O TI deve registrar todos os novos softwares instalados nos Sistemas de Informação com o fornecedor de software apropriado imediatamente após a instalação (ou o mais rápido possível após ter sido determinado que o software não foi registrado corretamente).

10.8. Verificações de conformidade - Pelo menos uma vez por ano, o TI deve revisar todos os contratos de licença de software e uso para conformidade.

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

Segurança Física da Sala de Processamento de Informação

11.1. Localização dos Sistemas de Informação - Os Sistemas de Informação e centros de dados devem estar localizados, em uma sala interna sem paredes ou janelas externas e longe de fontes potenciais de água ou incêndio.

11.2. Controles ambientais da Sala de Processamento de Informação - Na medida do possível, os sistemas de informação e centros de dados devem ter sistemas de proteção ambiental adequados, incluindo, mas não se limitando a, sistemas para: detectar e suprimir o fogo, resfriar, ventilar, aquecer, umidade e manter níveis adequados de umidade do ar em torno da sala, e para fornecer o condicionamento adequado da energia fornecida a esses sistemas.

11.3. Portas da Sala de Processamento de Informação - As localizações físicas dos Sistemas de Informação, incluindo quaisquer salas de máquinas de computadores, armários de telefone/rede e outras áreas semelhantes que possam conter Sistemas de Informação e equipamentos de comunicação, devem ser protegidas com medidas de segurança física que impeçam o acesso de pessoas não autorizadas. As portas para estes locais devem ser trancadas e resistentes à entrada forçada. Sempre que possível, a sala deverá ter relatórios de acesso revisados periodicamente para garantir que os níveis de acesso do pessoal sejam respeitados. A sala deverá ser coberta pelo sistema de vídeo vigilância.

Restaurar e Recuperar

12.1 Os usuários não devem armazenar dados críticos de negócios em discos rígidos de PCs locais. Isso torna a recuperação quase impossível no caso de falha do disco rígido. Os dados críticos de negócios devem ser armazenados no gerenciador de ficheiros Nextcloud.

12.2O TI garantirá que os dados da FUSA armazenados no Nextcloud ou dispositivos de armazenamento de rede tenham backups e sejam totalmente recuperáveis. Isso pode ser obtido usando uma combinação de cópias de imagem, backups incrementais, backups diferenciais, logs de transações ou outras técnicas.

12.3Os administradores do sistema determinarão a frequência dos backups pela volatilidade dos dados; o período de retenção para cópias de backup é determinado pela criticidade dos dados.

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

12.4A documentação de backup e recuperação deve ser revisada e atualizada regularmente para levar em conta novas tecnologias, mudanças nos negócios e migração de aplicativos para plataformas alternativas.

12.5A FUSA priorizará os esforços de restauração sistema por sistema para apoiar as funções críticas da fundação no caso de um grande evento.

12.6Os procedimentos de recuperação devem ser testados anualmente.

Segurança de rede

13.1. Wifi - O acesso do usuário à rede sem fio pode ser interrompido a qualquer momento sem aviso prévio.

13.2. Segmentação de Rede - Os administradores do sistema podem configurar a rede interna em vários segmentos físicos ou lógicos para proteger diferentes tipos de informações. Os usuários não devem tentar contornar esta segmentação de rede sem o consentimento expresso do CISO.

13.3. Senhas de dispositivos de rede - Os administradores do sistema configurarão cada dispositivo de rede para exigir uma senha de rede do administrador do sistema e administrarão cada dispositivo de rede usando as ID´s privilegiadas do administrador do sistema.

13.4. Acesso à rede fornecido pelo usuário - Os usuários não podem configurar nenhuma conexão com qualquer rede externa, inclusive por meio do uso de dispositivos sem fio, celulares ou outros dispositivos de acesso de banda larga, sem o consentimento expresso por escrito do CISO.

13.5. Configurações seguras necessárias para segurança de rede - Todos os computadores devem ser configurados com software de gerenciamento de dispositivos antes de terem permissão para acessar a rede com ou sem fio.

13.6. Configurações de firewall - O CISO revisará e aprovará todas as políticas de firewall pelo menos uma vez por ano, após a revisão de qualquer incidente de segurança e em qualquer outro momento necessário. O CISO testará periodicamente a suficiência das regras de política de firewall pelo menos uma vez por ano ou mediante qualquer alteração nas regras de firewall.

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

13.7. Conexões de Internet através de firewall - Todas as conexões de ou para Sistemas de Informação e qualquer rede externa, incluindo a Internet, devem passar por um firewall e / ou servidor proxy, e quaisquer outros mecanismos de controle de acesso adicionais exigidos pelo CISO. Os usuários não podem configurar nenhuma conexão com qualquer rede externa que não passe pelo firewall e por mecanismos de controle de acesso adicionais, incluindo por meio do uso de dispositivos sem fio, celulares ou outros dispositivos de acesso de banda larga.

13.8. Criptografia de rede sem fio - Os administradores do sistema irão configurar todos os pontos de acesso sem fio para utilizar WPA2 ou criptografia mais forte.

13.9. Acesso sem fio para convidados - Os visitantes só têm permissão para acessar a rede sem fio do convidado. Os administradores do sistema irão configurar esta rede para utilizar WPA2 ou criptografia mais forte e irão alterar esta senha a cada 7 dias. Os visitantes que tiveram o acesso devidamente permitido às instalações podem obter a senha atual do hóspede com seu acompanhante.

13.10. Implementação de rede sem fio - Somente administradores de sistema ou contratados autorizados pelo CISO podem instalar ou configurar pontos de acesso sem fio. Os usuários estão proibidos de configurar qualquer ponto de acesso sem fio não aprovado CISO. A FUSA pode realizar periodicamente testes de direção e outros testes de descoberta de rede para determinar a presença de redes sem fio não autorizadas ou não seguras.

13.11. Acesso a sites externos - Todo o acesso do usuário a sites externos deve passar por um servidor proxy, que pode ser configurado para bloquear os usuários de visitar qualquer site que, até o limite permitido por lei, o CISO determinou que pode conter material questionável ou de outra forma inseguro.

13.12. Servidores configurados pelo usuário - Os usuários não têm permissão para instalar e configurar qualquer servidor acessível externamente, incluindo, mas não se limitando a, qualquer site, serviço de compartilhamento de arquivos, site de mídia social ou serviço de streaming de vídeo.

Encriptação

14.1. Criptografia de disco completo de mídia eletrônica em dispositivos portáteis - Todas as informações confidenciais armazenadas em dispositivos portáteis (ou seja, laptops, tablets ou

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

smartphones) devem utilizar criptografia de disco completo usando um programa de criptografia aprovado.

14.2. Criptografia de informações confidenciais transmitidas - Todas as informações confidenciais transmitidas fora da rede da FUSA devem ser criptografadas usando um método de criptografia aprovado.

14.3. Criptografia de e-mail ou arquivos transmitidos - Qualquer e-mail ou arquivo usado para transmitir informações confidenciais deve ser criptografado usando um método de criptografia aprovado pelo CISO. Qualquer chave de descriptografia necessária para descriptografar o e-mail ou arquivo deve ser enviada por um canal de comunicação diferente.

14.4. Servidores de gerenciamento de chaves de criptografia - Os administradores do sistema gerenciarão os servidores de gerenciamento de chaves de criptografia ou serão responsáveis pelo armazenamento seguro de todas as chaves de criptografia. O servidor de gerenciamento de chaves exigirá pelo menos dois (2) Administradores de sistema para acessar ou modificar uma chave de criptografia armazenada e todos os acessos ou modificações de tais chaves serão registrados.

14.5. Backup de chaves de criptografia - Os administradores do sistema farão backup e armazenarão as chaves de criptografia usadas em toda a organização usando um método de criptografia aprovado de uma força pelo menos tão forte quanto a segurança oferecida pelas chaves de criptografia. As chaves usadas para criptografar esse backup serão armazenadas física e logicamente separadas da cópia de backup das chaves de criptografia.

14.6. Armazenamento de chaves de criptografia - O CISO armazenará quaisquer chaves de criptografia e / ou frases secretas mantidas em papel ou outra forma física em um cofre com acesso mínimo.

14.7. Atualizações regulares da chave de criptografia - Quando possível, os administradores do sistema alterarão regularmente todas as chaves de criptografia usadas para criptografar os dados armazenados em uma programação determinada pelo CISO. Se tecnologicamente viável, os dados criptografados com a chave antiga não precisam ser atualizados com a nova chave quando a chave é atualizada dessa maneira.

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

14.8. Atualizações da chave de criptografia comprometida - Se uma chave de criptografia foi comprometida ou suspeita de ter sido comprometida, o CISO deverá gerar uma nova chave de criptografia e qualquer informação criptografada com a chave antiga deve ser;

a) criptografado usando a chave antiga e criptografado novamente usando a nova chave em um ambiente seguro separado de quaisquer conexões de rede;

b) criptografado uma segunda vez usando a nova chave, ou

c) destruído com segurança de acordo com esta política. A chave comprometida deve ser revogada se tecnologicamente viável.

14.9. Algoritmo de criptografia e tamanho da chave - Toda criptografia simétrica deve usar o Advanced Encryption Standard (AES). O CISO deve aprovar o tamanho da chave a ser usado em cada Sistema de Informação. O CISO deve aprovar o algoritmo e o tamanho da
chave usados para criptografia assimétrica, incluindo quaisquer algoritmos assimétricos usados para trocas de chaves ou assinaturas digitais.

14.10. Módulos criptográficos - Os administradores de sistema não implantarão nenhum software criptográfico ou dispositivo que utilize software de código aberto que não seja mantido regularmente com pelo menos atualizações anuais.

14.11. Divulgação de chaves de criptografia - A menos que especificamente autorizado pelo CISO, os usuários não devem divulgar as chaves de criptografia a terceiros.

Vírus e Outro Software Malicioso

15.1. Software Anti-Malware - Todos os sistemas de informação capazes de executar software que detecta, previne ou remove código malicioso ("Software antivírus") devem executar a versão estável mais recente de tal software e utilizar os arquivos de definições de vírus mais recentes. Todos os sistemas de informação com esse recurso e sem a versão mais recente do software anti-malware devem ser imediatamente removidos da rede.

15.2. Envio de atualizações de definição de vírus - Os administradores do sistema garantirão que os arquivos de definição de vírus mais recentes usados pelo software antivírus sejam

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

instalados automaticamente em cada sistema de informação que usa este software. Os usuários estão proibidos de desativar o mecanismo de atualização.

15.3. Quarentena de sistemas infectados - Os usuários devem remover imediatamente qualquer Sistema de Informação suspeito de infecção por um vírus de computador, worm, spyware ou outro malware da rede, desconectando imediatamente o Sistema de Informação da rede e contatando imediatamente o Serviço de Apoio. Os usuários não devem tentar remover tal malware sem orientação do Administrador do sistema e os usuários não devem desconectar ou desligar o Sistema de Informação.

15.4. Transferências - Os usuários não devem baixar software da Internet ou introduzir software não aprovado nos Sistemas de Informação. Somente os administradores do sistema podem instalar o software após as varreduras apropriadas de malware.

15.5. Arquivos recebidos de terceiros - Os usuários devem digitalizar todos os arquivos recebidos de terceiros antes que o arquivo seja usado nos Sistemas de Informação.

15.6. Desativação de antimalware - Os usuários não devem desativar o software anti-malware instalado em qualquer sistema, incluindo qualquer dispositivo móvel.

15.7. Malware instalado pelo usuário - Os usuários não devem desenvolver ou introduzir intencionalmente malware de qualquer tipo em qualquer Sistema de Informação.

Configurações Padrão e Gerenciamento de Mudanças

16.1. Configuração do sistema - Os Administradores do Sistema criarão configurações padrão para cada tipo de Sistema de Informação de acordo com a configuração aprovada pelo CISO. Os administradores do sistema irão configurar todos os novos sistemas de informação de acordo com uma das configurações padrão.

16.2. Padrões de Segurança da Informação - Todos os sistemas implantados utilizarão os padrões de segurança da informação, conforme definido pela politica.

16.3. Desativando componentes de segurança - Os usuários e administradores de sistema não devem desabilitar, ignorar, desconectar ou desligar qualquer componente da infraestrutura de segurança (temporária ou permanentemente) sem a aprovação prévia do CISO.

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

16.4. Desativar IDs de usuário e senhas padrão - Os administradores do sistema devem desativar ou renomear todos os nomes de usuário e senhas com privilégios padrão em cada sistema de informação.

16.5. Remoção de software não essencial - Os administradores do sistema devem, por padrão, desabilitar todos os softwares não essenciais e desabilitar todas as portas não essenciais em cada Sistema de Informação.

16.6. Versão mais recente do software - Os administradores de sistema devem obter cada nova versão de cada sistema operacional, firewall, antimalware e outro software de sistema relacionado diretamente do fornecedor aplicável e, quando possível, verificar a integridade do software por comparação com mecanismos de autenticação válidos conhecidos. Os Administradores do Sistema devem testar cada nova versão do software assim que possível e, assim que a estabilidade do software for verificada, implantar o novo software em todos os Sistemas de Informação aplicáveis.

16.7. Envio de atualizações de software - Sempre que possível, os Administradores do Sistema enviarão atualizações de software para todos os Sistemas de Informação. Os usuários estão proibidos de desativar os mecanismos de atualização automática de software.

16.8. Registro de todas as atualizações e mudanças - Os administradores do sistema irão configurar cada sistema para registrar todos os patches, correções, atualizações e mudanças de software. Para componentes críticos do Sistema de Informação, os Administradores do Sistema também registrarão, no mínimo, a data e hora da mudança, o Administrador do Sistema que fez a mudança, quem testou a mudança e uma explicação ou justificativa para a mudança em formato escrito em papel, seguramente localizado o mais próximo possível do componente do Sistema de Informação afetado.

16.9. Registro de todas as atualizações rejeitadas - Mediante aprovação por escrito do CISO, os Administradores do Sistema podem adiar ou recusar a atualização para o patch, correção ou atualização mais recente de qualquer software. Os administradores do sistema manterão um registro de qualquer decisão de adiar ou rejeitar a versão mais recente de qualquer software.

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

Problemas de Relatório

17.1. Divulgação de informações - Os usuários devem relatar imediatamente qualquer divulgação não autorizada de Informações Sensíveis ao CISO.

17.2. Fraquezas de segurança conhecidas ou suspeitas - Os usuários devem relatar imediatamente qualquer fraqueza conhecida ou suspeita aos Sistemas de Informação ou Informação apenas ao CISO ou aos Administradores do Sistema via telefone, se possível. Os usuários devem abster-se de usar o Sistema de Informação potencialmente vulnerável e relatar tais deficiências.

17.3. Violações - Os usuários devem relatar todas as violações de segurança conhecidas ou suspeitas, reais ou tentadas, ao CISO imediatamente após a descoberta. Os outros usuários não devem interferir, impedir, obstruir ou dissuadir um usuário de relatar qualquer violação de segurança ou vulnerabilidade conhecida ou suspeita.

17.4. Eventos de Segurança - Os usuários devem relatar imediatamente todos os eventos potenciais relacionados à segurança ao CISO. Os eventos relatáveis relacionados à segurança incluem qualquer solicitação incomum de informações (incluindo senha, ID de usuário ou outras informações confidenciais) de terceiros, bem como resultados ou atividades incomuns observadas nos sistemas de informação.

17.5. Equipamento perdido ou roubado - Equipamento de TI perdido ou roubado pode resultar em violação de dados ou perda de serviço e a FUSA pode ser obrigada por lei a relatá-lo. O equipamento de TI deve ser armazenado em um local seguro sempre que não estiver em uso. Os usuários não devem deixar o equipamento de TI em um local não seguro, como um local destrancado ou veículo desacompanhado, por um longo período de tempo ou durante a noite.

A notificação de perda ou roubo de equipamentos emitidos pela FUSA é obrigatória. Os usuários devem tomar as seguintes ações se o equipamento de TI for perdido ou roubado:

17.5.1. Participar a ocorrência na polícia local, posto ou esquadra mais próxima, se o usuário suspeitar que o equipamento de TI foi roubado. Uma cópia da ocorrência deverá ser fornecida ao Departamento de TI.

17.5.2. Relatar a perda ao seu supervisor directo imediatamente após a descoberta.

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

17.5.3. Relate a perda para o Serviço de Apoio e por chamada telefónica se possível a um dos Administradores de Sistemas imediatamente após a descoberta. O Serviço de Apoio fornecerá as orientações sobre as próximas etapas para garantir que os dados sejam protegidos de forma adequada.

17.6. Confidencialidade de relatórios - Na medida do possível, a FUSA manterá a identidade de todos os Usuários que fizerem denúncias de violação de segurança de boafé estritamente confidenciais e não permitirá qualquer tipo de retaliação.

17.7. Aplicação da lei – Exceto para emergências que possam colocar em perigo a vida de um indivíduo ou apresentar um risco imediato de danos à propriedade da FUSA, o Usuário deve entrar em contato com o Departamento de Legal e Compliance antes de fazer qualquer denúncia às autoridades policiais ou antes de discutir ou participar de qualquer investigação pelas autoridades legais tendo em conta que o Usuário devera estar acompanhado de um responsável do Departamento de Legal e Compliance.

Midia Removível

18.1. Uso de mídia eletrônica removível - Os usuários só podem usar meios eletrônicos removíveis autorizados pela TI.

18.2. Acesso a dispositivos de mídia eletrônica removíveis - Por padrão, os administradores do sistema desabilitarão todos os dispositivos de mídia eletrônica removíveis em todas as estações de trabalho. O usuário pode solicitar aprovação para o uso de dispositivos de mídia eletrônica removíveis ao demonstrar uma necessidade comercial legítima de tal uso pelo Serviço de Apoio.

18.3. Criptografia de informações confidenciais - Os usuários devem criptografar todas as informações confidenciais armazenadas em mídia eletrônica removível de qualquer forma, usando um método de criptografia aprovado pelo CISO.

18.4. Verificação de vírus em todas as mídias eletrônicas removíveis - Os usuários devem usar um software antivírus aprovado antes de acessar qualquer uma das Informações armazenadas em mídia eletrônica removível.

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

Monitoramento e Registro

19.1. Propriedade legal e acesso - A FUSA reserva-se toda a propriedade legal de todos os equipamentos, arquivos e mensagens armazenados ou transmitidos em seus Sistemas de Informação, e pode acessar essas Informações sem aviso prévio.

19.2. Digitalização e monitoramento de comunicações – Em caso de suspeita de um dos colaboradores, a FUSA pode verificar e monitorar rotineiramente o conteúdo de todas as comunicações eletrônicas usando seus Sistemas de Informação, incluindo qualquer e-mail, actividade de navegação na web, correio de voz, mensagem de texto ou mensagem de vídeo, usando ferramentas automatizadas ou manuais na medida do permitido por lei.

19.3. Má conduta do funcionário - Se qualquer monitoramento de comunicação revelar qualquer conduta imprópria de funcionário (incluindo violações de qualquer política da FUSA, como as violações do Código de Ética da FUSA, que proíbe o assédio com base em sexo ou raça) ou qualquer atividade criminosa, os resultados de qualquer monitoramento podem ser usados para documentar qualquer conduta e pode ser revelada à FUSA ou a funcionários responsáveis pela aplicação da lei.

19.4. Monitoramento e Alertas - Os administradores do sistema devem configurar e habilitar o monitoramento dos recursos do sistema e sistemas de informação para alertar os administradores do sistema em tempo real sobre eventos que podem indicar uma violação da segurança da informação. Os administradores do sistema responderão imediatamente a qualquer dos alertas.

19.5. Coleção de Logs - No caso de um incidente de segurança do sistema, os Administradores do Sistema ou outros investigadores devem copiar imediatamente e com segurança todos os arquivos de log relevantes para armazenamento off-line e externo protegido.

19.6 Logs do sistema - Os administradores do sistema devem configurar e habilitar o registro de atividades críticas em sistemas de informação. O registro deve incluir;

i adições, modificações e exclusões no software do sistema e arquivos de configuração;

ii login de usuário bem ou malsucedido e datas e horas de logoff;

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

iii quaisquer alterações no acesso ou privilégios de qualquer usuário (incluindo a criação, desativação, ou remoção de qualquer usuário);

iv qualquer tentativa de um usuário de exceder os privilégios concedidos;

v qualquer registro de qualquer usuário ou processo específico autorizado pelo CISO, e;

vi todo o acesso ou modificação de chaves de criptografia armazenadas em um servidor de gerenciamento de chaves. Todos logs devem ser protegidos contra desativação, acesso ou modificação não autorizados e devem conter dados suficientes para suportar auditorias ou análises forenses. Os registros devem ser revisados regularmente para qualquer actividade anormal.

19.5 Análise de vulnerabilidade de segurança - Pelo menos uma vez por semana, os Administradores do Sistema revisarão todos os avisos de vulnerabilidade de segurança emitidos por organizações confiáveis, incluindo os bancos de dados US-CERT e CVE para vulnerabilidades que podem afetar os Sistemas de Informação da FUSA.

19.6 Vulnerabilidade anual e teste de penetração - Pelo menos uma vez por ano, o CISO, seja diretamente ou por meio de uma parte independente de confiança que esteja no negócio e conduza regularmente análises de segurança e testes de penetração, deve conduzir testes de vulnerabilidade e penetração em todos os sistemas da FUSA. Esse teste deve ser sem aviso prévio. Este teste de vulnerabilidade inclui testes para detectar quaisquer vulnerabilidades.

Violações

Qualquer violação desta política pode resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho e outras ações legais. A FUSA reserva-se o direito de notificar as autoridades responsáveis pela aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade. A FUSA não considera que a conduta em violação a esta política esteja dentro do curso e âmbito de emprego do Usuário, ou a consequência direta do cumprimento das obrigações do Usuário. Consequentemente, na medida do permitido por lei, a FUSA reserva-se o direito de não defender ou pagar quaisquer danos atribuídos a quaisquer Usuários que resultem da violação desta política.

Este documento é propriedade exclusiva da **Fundação Salmina.** É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.

Qualquer Usuário que seja solicitado a realizar uma atividade que acredita estar em violação desta política, deve apresentar uma reclamação por escrito ou verbal ao seu supervisor, ou ao Departamento de Recursos Humanos o mais rápido possível.

Excepções

Excepções a esta política devem ser feitas por escrito pelo CISO. Todas as exceções aprovadas serão armazenadas de acordo com os requisitos de retenção do Regulamento Interno da FUSA. Qualquer não aplicação do Regulamento referido a qualquer momento não constitui consentimento.

PELAS PESSOAS. PELA VIDA.

Este documento é propriedade exclusiva da **Fundação Salmina**. É estritamente proibida a reprodução total ou parcial, a distribuição, a divulgação ou a utilização sem autorização da pessoa responsável.