Norma de segurança da informação:

Política de Expurgo

Código	**NSI-18**
Versão	V2023.1
Data da Versão	21/07/2023
Criado por	Danilo Goes
Aprovado por	Rodrigo Vieira
Nível de confidencialidade	Interno
Número do Controle	

Histórico de alterações

Data Alteração	Versão	Alterado por	Descrição alteração
10/12/2024	V2024.1	Danilo Goes	Revisão

Sumário

Norma de segurança da informação: 1
1 Introdução 3
2 Propósito 3
3 Diretrizes 3
8 Sanções e Punições 4
9 Revisões 4
10 Gestão da Norma 4

1 INTRODUÇÃO

1.1. A Norma de segurança da informação **NSI-18** complementa Política Geral de Segurança da Informação, definindo as diretrizes para expurgo dos dados.

1.2. O objetivo desta política é fornecer diretrizes claras e consistentes para a destruição segura de informações confidenciais e sensíveis, a fim de minimizar os riscos de violação de dados e garantir a proteção adequada das informações durante todo seu ciclo de vida.

1.3. Esta política se aplica a todos os funcionários, colaboradores, contratados e terceiros que tenham acesso a informações confidenciais ou sensíveis mantidas pela organização, independentemente do meio em que tais informações estejam armazenadas (papel, eletrônico, digital, etc).

2 PROPÓSITO

2.1 Estabelecer um padrão de criação e utilização de senhas fortes, no intuito de evitar que que pessoas mal-intencionadas as descubram e se passem por outras pessoas, acessando, por exemplo: contas de correio eletrônico, de rede, de computador e de sistemas; sites indevidos ou informações privilegiadas da YUP CHAT como se proprietário fosse do ativo ou da informação.

3 DIRETRIZES

1. Classificação da Informação: Todas as informações devem ser devidamente classificadas de acordo com sua confidencialidade e sensibilidade, utilizando-se de uma política de classificação já estabelecida pela organização.
2. Tempo de retenção: Cada tipo de informação deve ter um período de retenção definido, baseado em requisitos legais, regulatórios e de negócios. Esses períodos de retenção devem ser monitorados e revisados periodicamente, a fim de garantir que as informações estejam sendo retidas pelo tempo necessário e de acordo com as obrigações legais aplicáveis.
3. Métodos de Expurgo: O expurgo das informações deve ser realizado de forma segura, garantindo que a recuperação ou reconstrução das informações seja impossível ou altamente improvável.

a) Informações impressas: Documentos impressos devem ser destruídos através de uma fragmentadora de papel, de modo que a reconstrução seja inviável.

b) Informações eletrônicas: Todos os dispositivos eletrônicos contendo informações sensíveis ou confidenciais devem ser devidamente limpos antes de serem descartados. Isso inclui a exclusão segura de dados de discos rígidos, cartões de memória ou qualquer outro dispositivo de armazenamento eletrônico. Caso a limpeza segura não seja possível, os dispositivos devem ser fisicamente destruídos, garantindo a total inutilização.

4. Registro do Expurgo: Um registro detalhado de todas as informações expurgadas deve ser mantido, incluindo a data de expurgo, tipo de informação, método utilizado e responsável pela destruição. Esses registros devem ser mantidos com segurança por um período de tempo determinado, de acordo com as obrigações legais aplicáveis.
5. Conscientização e Treinamento: Todos os funcionários envolvidos no manuseio de informações confidenciais devem receber treinamento adequado sobre a política de expurgo, suas responsabilidades e os procedimentos a serem seguidos. É fundamental manter uma cultura de segurança da informação por meio de conscientização e treinamento regular.
6. Auditoria e Monitoramento: A organização deve conduzir auditorias regulares para garantir o cumprimento desta política de expurgo. Quaisquer desvios devem ser tratados prontamente e ações corretivas devem ser implementadas.
7. Revisão e Atualização: Esta política deve ser revisada regularmente para garantir sua eficácia contínua e estar em conformidade com as leis e regulamentos aplicáveis. Quaisquer alterações devem ser comunicadas a todos os envolvidos e treinamentos adicionais devem ser fornecidos, se necessário.

4 SANÇÕES E PUNIÇÕES

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

5 REVISÕES

Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

6 GESTÃO DA NORMA

- A norma **NSI-18** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da YUP CHAT.
- A Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da YUP CHAT. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.
- Cumprimento desta política é uma responsabilidade individual e sua violação pode resultar em medidas disciplinares, conforme estabelecido pelas políticas e procedimentos da organização.
- A presente norma foi aprovada no dia 21/07/2027