Norma de segurança da informação:

Política de Criptografia

Código	**NSI-15**
Versão	V2023.1
Data da Versão	31/07/2023
Criado por	José Jardel Luciano Ferreira da Silva
Aprovado por	Rodrigo Vieira
Nível de confidencialidade	Interno
Número do Controle	

Histórico de alterações

Data Alteração	Versão	Alterado por	Descrição alteração
16/03/2022	V2022.1	André Iesca Rodrigues	Revisão
24/05/2022	V2022.2	André Iesca Rodrigues	Edição do padrão de cripto
31/07/2023	V2023.1	Danilo Goes	Edição
05/12/2024	V2024.1	Danilo Goes	Revisão

Sumário

1 INTRODUÇÃO 3
2 PROPÓSITO 3
3 ESCOPO 3
4 CONCEITOS E DEFINIÇÕES 3
5 REGRAS GERAIS 5
5.1 Compete ao Analista de Segurança da Informação: 6
6 CONTROLES CRIPTOGRÁFICOS 7
7 GERENCIAMENTO DE CHAVES 7
7.1 Padrões, métodos e procedimentos 7
8 GUARDA E USO DE CHAVES DE CRIPTOGRAFIA PRIVADAS 9
9 SANÇÕES E PUNIÇÕES 10
10 REVISÕES 10
11 GESTÃO DA NORMA 11

1 INTRODUÇÃO

A Norma de segurança da informação **NSI-15** complementa Política Geral de Segurança da Informação, regras para o uso de controles de criptografia, bem como as regras para o uso de chaves criptográficas, a fim de proteger a confidencialidade, integridade, autenticidade e não-repúdio de informações.

Este documento é aplicado ao alcance de todo o Sistema de Gestão da Segurança da Informação (SGSI), e todas as atividades de processamento de dados pessoais.

2 PROPÓSITO

Estabelecer diretrizes para gestão dos sistemas criptográficos da YUP CHAT.

3 ESCOPO

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação, definindo as regras e procedimentos gerais para o acesso e uso de chaves de criptografia, considerando os requisitos para: Armazenamento, Transporte e Certificado Eletrônico.

4 CONCEITOS E DEFINIÇÕES

4.1 **CRIPTOGRAFIA** - arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

4.2 **CRIPTOGRAFIA DE CHAVE PÚBLICA -** também conhecida como criptografia assimétrica, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas, e chaves privadas que são conhecidas apenas pelo proprietário. Isto realiza duas funções: autenticação, onde a chave pública verifica que um portador da chave privada parelhada enviou a mensagem, e encriptação, onde apenas o portador da chave privada parelhada pode decriptar a mensagem encriptada com a chavepública;

4.3 **RESUMO CRIPTOGRÁFICO** - resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor – conhecida como resultado hash - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (utilizando-se apenas o hash não é possível recuperar a mensagem que o gerou);

4.4 **ASSINATURA DIGITAL** – tipo de assinatura eletrônica que usa operações matemáticas com base em algoritmos criptográficos de criptografia assimétrica para garantir segurança na autenticidade das documentações. Para assinar digitalmente um documento é necessário possuir um certificado digital. Entre as principais vantagens do uso de assinatura digital estão o não repúdio (não deixa dúvidas quanto ao seu remetente) e tempestividade (a AC pode verificar data e hora da assinatura de um documento);

4.5 **TOKEN –** algo que o usuário possui e controla (tipicamente uma chave, senha e/ou módulo criptográfico) que é utilizado para autenticar a identidade do requerente e/ou a requisição em si;

4.6 **CERTIFICADO -** documento assinado criptograficamente, que é destinado a assegurar para outros a identidade do terminal que utiliza o certificado. Um certificado é confiável se esse certificado é assinado por outro certificado confiável, como uma autoridade de certificação, ou se ele próprio é um certificado confiável;

4.7 **CERTIFICADO DIGITAL** – conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação;

4.8 **CHAVE CRIPTOGRÁFICA -** valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

4.9 **ALGORITMO CRIPTOGRÁFICO** – função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente nas informações classificadas;

4.10 **CIFRAÇÃO -** ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

4.11 **INFRAESTRUTURA DE CHAVE PÚBLICA (PKI) -** sistema de recursos, políticas, e serviços que suportam a utilização de criptografia de tecla pública para autenticar as partes envolvidas na transação. Não há nem um único padrão que define os componentes de uma infraestrutura de chave pública, mas uma infraestrutura de chave pública geralmente inclui Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs). O padrão ITU-T X.509 fornece a base para a infraestrutura de chave pública padrão de mercado;

4.12 **INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL)** – cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Essa infraestrutura é um conjunto elaborado de práticas, técnicas e procedimentos que serve para suportar um sistema criptográfico baseado em certificados digitais. O modelo adotado no Brasil para a infraestrutura de chaves públicas é chamado de certificação com raiz única, em que existe uma Autoridade Certificadora Raiz (AC-Raiz). Além de desempenhar esse papel, a AC-Raiz credencia os demais participantes da cadeia, além de supervisionar e auditar os processos.

5 REGRAS GERAIS

5.1 Os notebooks que armazenam arquivos sigilosos devem ter seus discos rígidos (HD) criptografados com ESET Endpoint Encryption tem validação FIPS 140-2 com criptografia AES de 256 bits. disponível em todos os notebooks da YUP CHAT.

5.2 Utilizar criptografia sempre que enviar ou receber dados com informações sensíveis.

5.3 Quando permitido por norma de tratamento da informação, documentos restritos que forem armazenados em dispositivos móveis (notebook, tablet, smartphone etc.) ou em mídias removíveis (cd, dvd, pen drive etc.) devem ser criptografados para evitar a sua divulgação indevida em caso de perda ou furto do equipamento ou da mídia

5.4 A escolha dos tipos, da qualidade e da força de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e processo de negócio, tomará como base, sempre que possível, o resultado do processo de gerenciamento de riscos de segurança da informação.

5.5 Uma tabela relacionando os controles criptográficos, seus parâmetros e sua aplicação na proteção de informações classificadas, será mantida e comunicada aos proprietários e custodiantes de ativos de informação;

5.6 Os controles criptográficos serão usados para assegurar, dentre outros:

a) a confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transporte físico ou de transmissão eletrônica;

b) o não-repúdio: provar a ocorrência de um evento ou ação alegados e suas entidades originárias, de forma a resolver disputas sobre a ocorrência ou não ocorrência do evento ou ação e do envolvimento das entidades no evento.

c) a autenticação: confirmar a identidade de usuários ou de sistemas automatizados

5.1 COMPETE AO ANALISTA DE SEGURANÇA DA INFORMAÇÃO:

Deliberar sobre os seguintes procedimentos elaborados e mantidos pela YUP CHAT

a) procedimentos de certificação digital da Infraestrutura de Chaves Públicas da YUP CHAT

b) procedimentos de recuperação de informações cifradas, no caso de chaves criptográficas perdidas, comprometidas ou danificadas;

6 CONTROLES CRIPTOGRÁFICOS

Esta etapa de controles criptográficos é composta por um conjunto de regras que assegura a padronização das técnicas criptográficas, sua aplicação adequada e responsabilidades, de modo a garantir a segurança no transporte ou armazenamento das informações sem afetar o negócio da organização. Neste contexto, cada Gestor da Informação deverá fazer uma avaliação de risco para determinar o nível de proteção necessária às informações. Essa avaliação será usada para determinar se um controle criptográfico é apropriado, que tipo de controle deverá ser aplicado e para quais propósitos.

7 GERENCIAMENTO DE CHAVES

O gerenciamento das chaves criptográficas é essencial para o uso eficaz das técnicas de criptografia. O setor de Tecnologia da Informação, e o Analista de Segurança da Informação devem ter uma atenção especial para evitar o comprometimento ou perda das chaves criptográficas que podem impactar a confidencialidade, autenticidade e/ou integridade das informações.

7.1 PADRÕES, MÉTODOS E PROCEDIMENTOS

7.1.1 O setor de Tecnologia da Informação e o Analista de Segurança da Informação devem possuir um sistema de gerenciamento de chaves baseado em um conjunto acordado de padrões, procedimentos e métodos seguros.

7.2.1 Para reduzir a probabilidade de comprometimento, as chaves devem ter datas definidas de ativação e desativação, de modo que possam ser usadas apenas por um período limitado de tempo. Esse período de tempo deve ser dependente das circunstâncias em que o controle criptográfico está sendo usado e do risco percebido.

7.3.1 Além da questão de chaves secretas e privadas gerenciadas de forma segura, a proteção das chaves públicas também deve ser considerada. Existe a ameaça de que seja forjada uma assinatura digital substituindo uma chave pública do usuário por uma chave falsa. Esse problema é solucionado com o uso de um certificado de chave pública.

7.4.1 Estes certificados devem ser produzidos de maneira que associem informações relativas ao proprietário do par de chaves pública/privada com a chave pública. Portanto, é importante que se possa confiar no processo de gerenciamento que gera esses certificados. Esse processo é normalmente conduzido por uma autoridade de certificação, que deve ser uma organização reconhecida com controles adequados e procedimentos implantados para propiciar o grau exigido de confiança.

7.5.1 Os conteúdos de acordos ou contratos de níveis de serviço com fornecedores externos de serviços criptográficos, como uma autoridade de certificação, devem cobrir as questões de responsabilidades, confiabilidade dos serviços e tempos de resposta para o provimento dos serviços.

7.6.1 Um sistema de gerenciamento deve ser implantado para dar suporte setor de Tecnologia da Informação e o Analista de Segurança da no uso dos dois tipos de técnicas criptográficas, que são:

a) A geração das chaves deverá garantir as propriedades adequadas para a aplicação e uma aleatoriedade que torne baixíssima a probabilidade da chave ser previsível.
b) Técnicas de chave pública, nas quais cada usuário tem um par de chaves, uma chave pública (que pode ser revelada a qualquer um) e uma chave privada (que tem que ser mantida em segredo). As técnicas de chave pública podem ser usadas para criptografia e para produzir assinaturas digitais.

7.7.1 Todas as chaves devem ser protegidas contra modificação e destruição, e chaves secretas e privadas precisam de proteção contra divulgação não autorizada. Técnicas criptográficas também podem ser usadas para esse propósito. Proteção física deve ser utilizada para proteger o equipamento usado para gerar, armazenar e arquivar as chaves.

8 GUARDA E USO DE CHAVES DE CRIPTOGRAFIA PRIVADAS

8.1 O Departamento de TI e a Área de Segurança da Informação devem garantir que cada chave privada de criptografia, incluindo os arquivos e dispositivos contendo os certificados digitais da YUP CHAT, possuam pelo menos uma cópia de segurança, guardada em local seguro, preferencialmente em cofre trancado.

8.2 O Analista de Segurança da Informação será a responsável por definir o custodiante de cada chave privada, bem como será o responsável pela guarda segura da cópia daquela chave.

8.3 Os custodiantes devem ser escolhidos levando em consideração critérios éticos, além de seu histórico e reputação. Devem também ter, ao menos, conhecimentos mínimos de computação e de como manipular arquivos digitais de forma segura.

8.4 O Analista de Segurança da Informação deve orientar os custodiantes acerca de sua responsabilidade, das práticas corretas de manuseio com segurança das chaves privadas e do prazo de custódia.

8.5 Deve também exigir que os custodiantes assinem o Termo de Compromisso e Responsabilidade de chaves Criptográficas.

8.6 O Analista de Segurança da Informação deve garantir que os custodiantes das chaves privadas não tenham acesso ao ambiente de produção das bases de dados criptografados, incluindo dados de cartões.

8.7 O Analista de Segurança da Informação deve solicitar a chave privada ao custodiante quando:

a. O método de criptografia se tornar obsoleto. Neste caso, a chave será usada parar e fazer o banco de dados usando os métodos mais recentes e seguros;

b. Houver comprometimento ou suspeita de comprometimento da chave privada ou do banco de dados; ou

c. O tempo máximo de armazenamento estiver expirado.

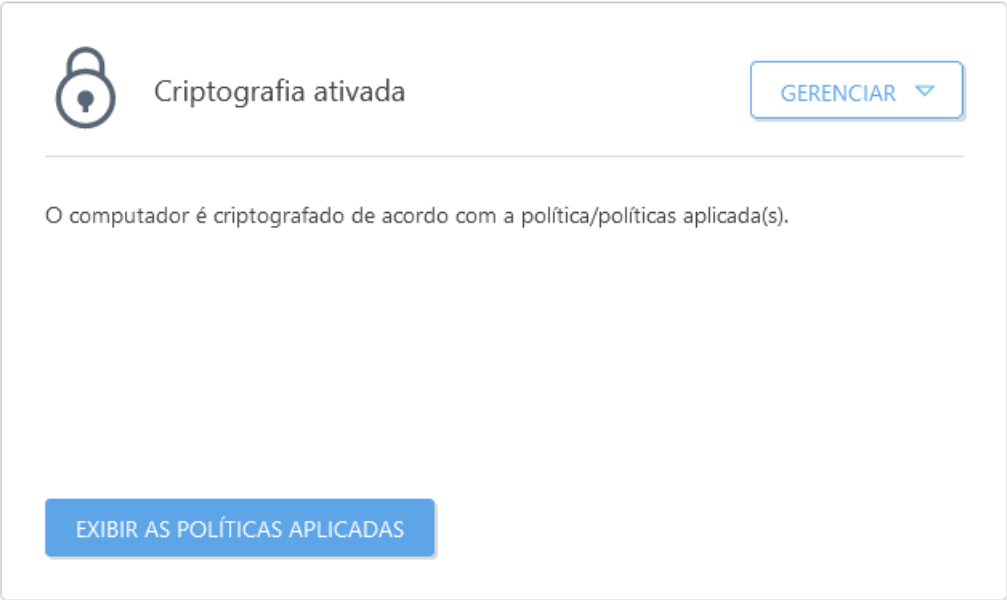
8.8 A solicitação da chave privada deve ser feita por escrito e aprovada pela direção da YUP CHAT

8.9 O custodiante, mediante a entrega da CHAVE PRIVADA, deve assinar o termo específico para este fim, onde se encerra sua responsabilidade

8.10 O Analista de Segurança da Informação deve garantir que os Termo de Responsabilidade e Compromisso, os nomes e os dados dos custodiantes estejam armazenados dentro de um ambiente seguro no ambiente da YUP CHAT, sob a classificação CONFIDENCIAL.

8.11 O Analista de Segurança da Informação deve manter uma lista dos "hash" das chaves que já foram utilizadas e descartadas, para que elas não sejam reaproveitadas no futuro.

8.12



9 SANÇÕES E PUNIÇÕES

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

10 REVISÕES

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

11 GESTÃO DA NORMA

- A norma **NSI-15** 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.

- A presente norma foi aprovada no dia 07/11/2020