Política Geral Segurança da Informação

Código	**PGSI-01**
Versão	V2023.1
Data da Versão	10/08/2023
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
08/11/2020	V2020.2	José Jardel L. F da Silva	Revisão
10/03/2022	V2022.01	André Iesca Rodrigues	Revisão
10/08/2023	V2023.01	Danilo Goes	Revisão
18/10/2024	V2024.01	Danilo Goes	Revisão

Sumário

1 OBJETIVO

O objetivo é estabelecer diretrizes que permitam aos colaboradores da YUP CHAT seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e da proteção legal da instituição, preservando as informações no tocante a:

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

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

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Dessa forma, busca-se desenvolver um comportamento ético e profissional, para que todos possam utilizar da melhor forma as ferramentas de TI e as informações por elas geradas, ao mesmo tempo, busca-se reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que tragam prejuízos à instituição.

2 INTRODUÇÃO

2.1 A YUP CHAT entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos produtos ofertados a seus clientes.

2.2 A YUP CHAT compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

2.3 Dessa forma, a YUP CHAT estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

3 PROPÓSITO

3.1 Esta política tem por proposito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da YUP CHAT adotar padrões de comportamento seguro, adequados às metas e necessidades da YUP CHAT;

3.2 Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

3.3 Resguardar as informações da YUP CHAT, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

3.4 Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;

3.5 Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da YUP CHAT como resultado de falhas de segurança.

4 ESCOPO

Esta política se aplica a todos os usuários da informação da YUP CHAT, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a YUP CHAT, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da YUP CHAT e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura YUP CHAT.

5 DIRETRIZES

5.1 O objetivo da gestão de Segurança da Informação da YUP CHAT é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

5.2 A Diretoria Executiva e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na YUP CHAT. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da YUP CHAT.

6 É POLÍTICA DA YUP CHAT

6.1 Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da YUP CHAT sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

6.2 Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Empregados, terceiros contratados e, onde pertinente, clientes.

6.3 Garantir a educação e conscientização sobre as práticas adotadas pela YUP CHAT de segurança da informação para Empregados, terceiros contratados e, onde pertinente, clientes.

6.4 Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

6.5 Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

6.6 Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

6.7 Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

7 CONCEITOS E DEFINIÇÕES

7.1 Para os fins dessa Política, considera-se:

- **Acesso Não Autorizado** - Acesso indevido ou não previsto obtido, por quaisquer meios, procedimentos e a qualquer título, à revelia da política ou do controle de acesso vigentes, ou ainda decorrente de falhas ou imperfeições nos mecanismos de controle de acesso. Contrasta com acesso autorizado.

- **Acesso Lógico** – acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;

- **Acesso Remoto** – ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

- **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

- **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos;

- **Ativo** - qualquer bem, tangível ou intangível, que tenha valor para a organização;

- **Ativo da Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

- **Auditoria** – verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

- **Autenticação** – é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

- **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;

- **Banco de Dados (ou Base de Dados)** – é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

- **Bloqueio de acesso** – processo que tem por finalidade suspender temporariamente o acesso;

- **Classificação da informação** - atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

- **Colaborador** – servidores, empregados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito da YUP CHAT.

- **Confidencialidade** – propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

- **Contingência** - descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

- **Controle de Acesso** - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

- **Cópia de Segurança (Backup)** – copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

- **Correio Eletrônico** - é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

- **Credenciais ou contas de acesso** - permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada

pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

- **Criptografia** – é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");

- **Dado** – representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

- **Disponibilidade** - propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

- **Download** - (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;

- **Gestão de Continuidade de Negócios** - Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

- **Gestão de Risco** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

- **Gestão de Segurança da Informação e Comunicações** - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

- **Gestor da Informação** - pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

- **Gestor de Segurança da Informação e das Comunicações** – é responsável pelas ações de segurança da informação e comunicações no âmbito da YUP CHAT

- **Hardware** – É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

- **Incidente de Segurança** - é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

- **Informação** - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

- **Informação sigilosa** - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

- **Integridade** – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

- **Internet** – rede mundial de computadores;

- **Intranet** – rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

- **Log** - é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

- **Logon** - Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;

- **Norma** - Documento interno que regulamenta formal e administrativamente, de maneira geral ou específica, aspectos ou diretrizes expressas na PSI, no todo ou em parte da instituição. As normas mapeiam a PSI na organização técnico-administrativa da instituição, estabelecendo regras para a sua implementação.

- **Peer-to-peer (P2P)** – (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

- **Perfil de acesso** - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

- **Política de Segurança da Informação (PSI)** – documento aprovado pela diretoria da YUP CHAT, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação na instituição;

- **Protocolo** - convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

- **Proxy** - é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;

- **Recursos Computacionais** - recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

- **Rede Corporativa** - conjunto de todas as redes locais sob a gestão da instituição;

- **Rede Pública** – rede de acesso a todos;

- **Responsabilidade** - Obrigações e deveres decorrentes da legislação vigente, ofício, cargo, função ou por força de contrato, na proteção dos ativos de informação de qualquer natureza.

- **Senha ou Credencial de Acesso** - Credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado ativo de informação de qualquer natureza, ou local que o abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes.

- **Servidor de Rede** - recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

- **Software** - são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

- **Site** - Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

- **Streaming** - transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

- **Termo de Responsabilidade** - termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

- **Tratamento de Incidentes de Segurança em Redes Computacionais** - serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

- **Usuário** - servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APE, formalizada por meio da assinatura do Termo de Responsabilidade;

- **VLAN (Virtual Local Area Network ou Virtual LAN)** – (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;

- **VPN (Virtual Private Network)** – (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;

- **Vulnerabilidade** - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

- **Wireless (rede sem fio)** - rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

8 PAPÉIS E RESPONSABILIDADES

8.1 Comitê Gestor de Segurança da Informação

Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, contando com a participação de, pelo menos, um representante da diretoria e um membro das seguintes áreas: Tecnologia da Informação, Segurança da Informação e Recursos Humanos.

É responsabilidade do CGSI:

- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da informação;

- Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;

- Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da YUP CHAT.

8.2 Analista de Segurança da Informação

É responsabilidade do Analista de Segurança da Informação:

- Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

- Apoiar o CGSI em suas deliberações;

- Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PGSI;

- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

- Tomar as ações cabíveis para se fazer cumprir os termos desta política;

- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

8.3 Gestores da Informação

É responsabilidade dos Gestores da Informação:

- Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela YUP CHAT;

- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela YUP CHAT;

- Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela YUP CHAT.

8.4 Usuários da Informação

É responsabilidade dos Usuários da Informação:

- Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos ao Analista de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

- Comunicar ao Analista de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da YUP CHAT;

- Assinar o Termo de Uso de Sistemas de Informação da YUP CHAT, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

- Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

9 SANÇÕES PUNIÇÕES

9.1 As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

9.2 A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

9.3 No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

9.4 Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a YUP CHAT, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens desta política.

10 CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da YUP CHAT adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da YUP CHAT.

11 REVISÕES

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

12 GESTÃO DA POLÍTICA GERAL DA SEGURANÇA DA INFORMAÇÃO

- A Política Geral da Segurança da Informação é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da YUP CHAT.

- 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 política foi aprovada no dia 10/09/2020.