

# NOR 005 – Norma de monitoramento de ativos

## Sumário

1. Objetivo.....	1
2. Âmbito de Aplicação .....	1
3. Considerações Gerais .....	1
4. Vínculos .....	1
5. Conceitos .....	2
6. Diretrizes.....	2
7. Disposições Finais .....	3
8. Controle e histórico de versões .....	4
9. Aprovações.....	4

## **1. Objetivo**

Esse documento define as regras que regulam o monitoramento de todos os serviços fornecidos por TI e ativos de tecnologia da informação do GRUPO LUFT.

## **2. Âmbito de Aplicação**

- 2.1. A presente norma aplica-se ao GRUPO LUFT e às empresas controladas ou a ela afiliadas, cada qual doravante individualmente designada “Empresa”.
- 2.2. As regras definidas neste documento aplicam-se a todos os serviços fornecidos por TI e ativos de tecnologia da GRUPO LUFT.

## **3. Considerações Gerais**

- 3.1. O conteúdo desta norma é propriedade da Empresa, e é destinado para uso interno. Para garantir que seja sempre considerada a versão mais atualizada, não é recomendado que este documento seja reproduzido, armazenado ou transmitido, em qualquer formato ou por quaisquer meios, sejam eletrônicos ou físicos.
- 3.2. O conteúdo desta norma deve ser conhecido e observado por todos os funcionários e terceiros que trabalhem internamente nos ambientes da empresa, sendo o seu descumprimento passível de aplicação de medidas legais e disciplinares.
- 3.3. Com o objetivo de proteger suas informações e validar se o comportamento de seus colaboradores está de acordo com a política e normas, ao GRUPO LUFT efetua o monitoramento de todos os ativos da informação e ativos de tecnologia.
- 3.4. Durante o monitoramento, ao GRUPO LUFT, sem qualquer notificação ou aviso poderá interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar a pessoas autorizadas qualquer tipo de informação relacionada ou contida nos recursos ou serviços de tecnologia da informação.
- 3.5. Em caso de dúvidas sobre a aplicação adequada das diretrizes constantes da presente norma, os Funcionários devem consultar o seu Gestor imediato e/ou a Área de Compliance.
- 3.6. A infração a esta norma estará sujeita às regras estabelecidas na Norma de Penalidades.
- 3.7. Os casos omissos serão decididos pelo Comitê de Conduta.

## **4. Vínculos**

PS01 - Política de Segurança da Informação

## 5. Conceitos

- 5.1 Ativos de tecnologia – Qualquer recurso tecnológico utilizado por funcionários e ou terceiros pertencentes ao GRUPO LUFT.
- 5.2 Serviços fornecidos por TI – Qualquer serviço utilizado no GRUPO LUFT através de ativos de tecnologia.
- 5.3 Funcionário – Refere-se a todo e qualquer conselheiro, administrador, diretor e funcionário que compõe o quadro da Empresa.
- 5.4 Informação – É todo e qualquer dado, informe, elemento, notícia, comunicação, material, instrução ou direção que sejam disponibilizados por escrito, oralmente ou de qualquer outra forma, gravados ou não com a expressão “confidencial”, em decorrência do desenvolvimento das atividades profissionais da Empresa.
- 5.5 Recursos de Tecnologia da Informação (“TI”) – São ferramentas de tecnologia da informação disponibilizadas ao Funcionário ou Terceiro para utilização a serviço da Empresa, tais como, mas não se limitando a: internet, intranet, rede corporativa com seus respectivos diretórios, correio eletrônico (e-mail), notebooks, computadores, impressoras, scanners, softwares e sistemas aplicativos.
- 5.6 Terceiro – Refere-se, mas não está limitado, a toda e qualquer pessoa física ou jurídica, que a Empresa se relacione ou venha a se relacionar, prestador de serviços, fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, locatário, cessionário de espaço comercial, independentemente de contrato formal ou não, incluindo aquele que utiliza o nome da Empresa para qualquer fim ou que presta serviços, fornece materiais, interage com Funcionário Público, com o Governo ou com outros Terceiros em nome da Empresa.
- 5.7 Usuário – Qualquer Funcionário, Terceiro ou qualquer outra pessoa que venha a ter acesso à Informação ou Informação Confidencial que transitam no âmbito dos Recursos de Tecnologia da Informação da Empresa, seja através de uma Conta de Usuário ou de uma Conta de Terceiro.

## 6. Diretrizes

O GRUPO LUFT reserva-se do direito de promover o monitoramento de seus recursos ou serviços de tecnologia da informação para detectar atividades não autorizadas, realizadas, sendo que os eventos de segurança da informação devem ser devidamente registrados.

Os sistemas de monitoramento deverão ser implantados nas estações de trabalho, servidores, correios eletrônicos (corporativo), navegação, internet, dispositivos móveis ou *wireless* e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos e manuseios efetuados.

Casos de exceção deverão documentados com a equipe de TI no documento de dispensa de política e norma.

O GRUPO LUFT poderá inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente que lhe pertença, incluindo dispositivos móveis, visando assegurar o rígido cumprimento da PSI e NORMAS.

Os registros de *logs* que contenham atividade dos usuários e demais informações que sejam pertinentes aos eventos de segurança da informação, ou ainda, que sejam pertinentes a questões trabalhistas, deverão ser armazenados pelo período mínimo de cinco anos, a fim de auxiliar em futuras investigações e monitoramento de controle de acesso.

Deverão ser instalados sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso às mesmas;

O monitoramento deverá ocorrer de forma genérica, sem atuação direta em relação a determinado colaborador para que não se caracterize discriminação ou “perseguição”, devendo ser formalizados os procedimentos internos pela área de TI, tão logo tais procedimentos tenham sido adotados, como, por exemplo, mas não se limitando, a monitoramento por software específico e inspeção física por amostragem.

As informações de monitoramento deverão ser analisadas por equipe específica em caráter confidencial, sendo que possíveis incidentes, quando não prevista solução e/ou encaminhamento em norma, deverão ser analisados pelo Comitê de Conduta.

As informações obtidas por monitoramento poderão tornar-se públicas, isto é, divulgadas para pessoas que não os respectivos gestores e as equipes envolvidas, apenas por ordem judicial, devendo a empresa armazená-las em local seguro e protegido contra falsificação e acesso não autorizado.

O nível de monitoramento requerido para os recursos individuais deve ser determinado de acordo com o seu valor, sensibilidade e criticidade.

O monitoramento deverá ser utilizado também para verificar a eficácia dos controles. Para eficácia e maior nível de segurança jurídica do monitoramento, os relógios de todos os sistemas de processamento de informações relevantes devem ser sincronizados.

## **7. Disposições Finais**

Esta norma entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

## 8. Controle e histórico de versões

<b>Data</b>	<b>Versão</b>	<b>Sumário</b>
01/07/2021	001	Criação do instrumento normativo

## 9. Aprovações

<b>Código</b>	<b>Descrição</b>	<b>Versão</b>	<b>Vigência</b>
NOR-005	Norma de monitoramento de ativos	001	

Emissor(es):

Revisor(es):

Aprovador(es):