# Propósito

A Norma de Gestão de Logs **NOR-SGSI-008** complementa a Política de Segurança da Informação e Política de Proteção de Dados, definindo as diretrizes para a gestão de logs de segurança dos sistemas e recursos utilizados pela **Demarco**.

# Escopo

Esta norma é aplicável ao escopo definido na Política de Segurança da Informação e Política de Proteção de Dados.

# Glossário

* **Evento de segurança da informação:** Ocorrências identificadas por meio de ferramentas de monitoramento ou situações identificadas pelo usuário final que podem indicar possível incidente de segurança da informação.

#### **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação, com possibilidade significativa de afetar as atividades ou ameaçar as informações da **Demarco**.

* **Logs:** Registro de atividades e eventos dentro de um sistema computacional.
* **Logs de atividade de usuário:** Registro de atividades realizadas por um usuário dentro de um sistema.
* **Logs de status do sistema:** Registro de eventos sistêmicos, que não foram realizados por um usuário.

# Diretrizes

Os logs de atividades realizadas pelos usuários em sistemas são fundamentais para a preservação da segurança da informação e privacidade de dados da **Demarco**. Através destes logs, podemos investigar Incidentes de Segurança da Informação e Privacidade, nos permitindo atuar de maneira preventiva. As seguintes diretrizes devem ser observadas:

## Criação, armazenamento, acesso e manipulação de logs

1. Os sistemas que forem contratados ou criados pela **Demarco** devem possuir a capacidade de criar logs de status do sistema e das atividades realizadas pelos usuários;
2. Convém que os logs contenham no mínimo:

|  |  |
| --- | --- |
| **LOGS DE STATUS DO SISTEMA** | **LOGS DE ATIVIDADES DO USUÁRIO** |
| Situação ocorrida (falha de componente do sistema, capacidade armazenamento excedida etc.) | Responsável pela ação |
| Data e hora | Ação realizada |
| - | Data e hora |
| - | Dado anterior do campo alterado |
| - | Status da ação (sucesso ou falha) |

1. Convém que os logs sejam armazenados em local diferente do original, para que não se percam em caso de incidentes;
2. O período mínimo para armazenamento destes logs nos sistemas é de 365 (trezentos e sessenta e cinco) dias;
3. Os logs que forem transmitidos para outro sistema ou local de armazenamento, devem utilizar protocolos seguros;
4. O acesso aos logs deve ser restrito a pessoas com autorização apropriada;
5. Logs de administradores de sistema devem ser registrados sempre que possível e a eles não deve ser concedida permissão para exclusão de seus próprios registros;
6. A alteração ou exclusão de logs deve ser devidamente registrada e justificada. Convém que o(s) sistema(s) utilizados possuam funcionalidade técnica para este controle.

## Monitoramento de Logs

1. Deve ser estabelecido e mantido monitoramento de segurança dos logs dos seguintes sistemas:

|  |  |  |  |
| --- | --- | --- | --- |
| **SISTEMAS** | **MONITORAMENTO** | **TRATAMENTO DE EVENTOS** | **RESPONSÁVEL** |
| Microsoft Azure | Logs da própria solução | Na própria solução | DCIT e Infraestrutura |
| M365 | Logs da própria solução | Na própria solução | Infraestrutura |
| Firewall | FortiAnalyzer | FortiGate e ADG | NOWCY |
| WAF | Logs da própria solução | Na própria solução | Sistemas |
| Sistemas Demarco | Logs das próprias soluções | Pipefy e Trello | Sistemas |

1. Logs que indiquem um possível evento de Segurança da Informação e Privacidade devem ser analisados e tratados;
2. Se um log indicar um Incidente de Segurança da Informação e Privacidade, deverá ser realizado o registro de incidente com os logs que evidenciam este ocorrido, de acordo com os requisitos da **NOR-SGSI-011 Norma de Gestão de Incidentes de Segurança da Informação e Privacidade.**

# Papéis e Responsabilidades

## INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Assegurar que sistemas contratados possuam a capacidade de gerar logs;
2. Assegurar que existam processos para o monitoramento de segurança dos sistemas.

## RESPONSÁVEIS PELOS SISTEMAS

1. Realizar o monitoramento de segurança dos sistemas que forem criados pela **Demarco;**
2. Contribuir para o tratamento dos eventos de segurança da informação e privacidade que forem identificados através do monitoramento;
3. Notificar os incidentes identificados a partir do monitoramento de segurança dos logs de sistemas;
4. Assegurar que os sistemas criados pela **Demarco** gerem logs de sistema e de atividades dos usuários.

# Gestão de versões

A revisão, aprovação e alteração desta norma segue os requisitos estabelecidos na Política de Segurança da Informação e Política de Proteção de Dados.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 03/10/2023 | CSIP | Criação da política |
| 0.2 | 09/11/2023 | CSIP | Revisão e ajustes |
| 0.3 | 08/07/2024 | CSIP | Revisão Anual |