Política de Segurança da Informação

PI –Política de Segurança da Informação.002/24

Histórico de Revisão

Versão	Data	Autor da Revisão	Sumário de Mudanças
1.0	21/06/2022	Alexandre Urbano	
2.0	28/11/2024	Alexandre Urbano	

Aprovação

Nome	Posição	Assinatura	Data
Alexandre Urbano	Consultor de Tecnologia		01/02/2023
Gustavo Santi	Gerente Geral		01/02/2023
Robison Santos	Diretor		01/02/2023
Alexandre Urbano	Consultor de Tecnologia		01/12/2024
Gustavo Santi	Gerente Geral		01/12/2024
Robison Santos	Diretor		01/12/2024

Conteúdo

1. Introdução

Este documento define a política de segurança da informação o GRUPO SAURA.

Como uma empresa moderna e voltada para o futuro, GRUPO SAURA reconhece a necessidade de garantir que seus negócios operem sem problemas e sem interrupções, isto, para o benefício de seus clientes e outras partes interessadas.

Para fornecer tal nível de operação contínua, GRUPO SAURA implementou um conjunto de controles de segurança da informação para tratar os riscos identificados.

A segurança da informação tem muitos benefícios para o negócio, incluindo:

- Proteção de fluxos de receita e lucratividade da empresa
- Garantir o fornecimento de bens e serviços aos clientes
- Manutenção e aprimoramento do valor do negócio
- Cumprimento dos requisitos legais e regulamentares

Esta política se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas o GRUPO SAURA.

Os documentos de suporte a seguir são relevantes para esta política de segurança da informação e fornecem esclarecimentos adicionais sobre como ela é aplicada:

- *Política de Computação em Nuvem*
- *Política de Dispositivos Móveis*
- *Política de Controle de Acesso*
- *Política Criptográfica*
- *Política de Segurança Física*
- *Política Antimalware*
- *Política de Segurança de Rede*
- *Política de Mensagens Eletrônicas*
- *Política de Proteção de Dados*

2. Política de Segurança da Informação

2.1. Requisitos de segurança da informação

Uma definição clara dos requisitos para a segurança da informação na GRUPO SAURA será acordada e mantida com os clientes internos do negócio e do Google e Amazon onde temos serviços de armazenamos em nuvem, de modo que toda a atividade de segurança da informação seja focada no cumprimento desses requisitos. Requisitos estatutários, regulatórios e contratuais também serão documentados e inseridos no processo de planejamento. Requisitos específicos com relação à segurança de sistemas ou serviços novos ou alterados serão identificados em cada projeto.

É um princípio fundamental do programa de segurança da informação GRUPO SAURAque os controles são implementados em razão da necessidade do negócio, e isso será comunicado regularmente a todos os funcionários por meio de reuniões de equipe e documentos informativos.

2.2. Quadro de configuração dos objetivos

Um ciclo regular será usado para a definição de objetivos de segurança da informação, para coincidir com o ciclo de planejamento orçamentário. Isso garantirá que um financiamento adequado seja obtido para as atividades de melhoria identificadas. Esses objetivos serão baseados em uma compreensão clara dos requisitos do negócio, informados pelo processo de revisão da administração, durante o qual as visões das partes interessadas podem ser obtidas.

Objetivos de segurança da informação serão documentados por um período de tempo, juntamente com detalhes de como eles serão alcançados. Estes serão avaliados e monitorados como parte das revisões de gestão para garantir que eles permaneçam válidos. Se forem necessárias emendas, elas serão gerenciadas por meio do processo de gerenciamento de mudanças.

Os controles de segurança da informação serão adotados, quando apropriado, pelo GRUPO SAURA. Estes serão revistos regularmente considerando o resultado das avaliações de risco e de acordo com os planos de tratamento de riscos de segurança da informação.

Além disso, controles aprimorados e adicionais de códigos serão adotados e implementados quando apropriado. A adoção desses códigos fornecerá garantia adicional aos nossos clientes e ajudará ainda mais com nossa conformidade com a legislação de proteção de dados.

2.3. Melhoria continua da segurança da informação

A política GRUPO SAURA em relação à melhoria contínua é:

- Melhorar continuamente a eficácia dos controles de segurança da informação
- Aprimorar os processos atuais para adequá-los às boas práticas, conforme definido.
- Aumentar o nível de proatividade (e a percepção da proatividade das partes interessadas) em relação à segurança da informação
- Tornar os processos e controles de segurança da informação mais mensuráveis, para fornecer uma base sólida para decisões.
- Revisar métricas relevantes anualmente para avaliar se é apropriado alterá-las, com base nos dados históricos coletados
- Obter ideias para melhoria por meio de reuniões regulares e outras formas de comunicação com as partes interessadas
- Analisar ideias para melhoria nas reuniões regulares de gestão, a fim de priorizar e avaliar prazos e benefícios

Ideias para melhorias podem ser obtidas de qualquer fonte, incluindo funcionários, clientes, fornecedores, equipe de TI, avaliações de risco e relatórios de serviço. Uma vez identificados, elas serão registradas e avaliadas em revisões administrativas.

2.4. Conjuntos de políticas de segurança da informação

O GRUPO SAURA, define a política em uma ampla variedade de áreas relacionadas à segurança da informação, descritas em detalhes em um conjunto abrangente de políticas que acompanha este documento.

Cada uma dessas políticas é definida e acordada por uma ou mais pessoas com competência na área específica e, uma vez formalmente aprovada, é comunicado ao público-alvo, dentro e fora da organização.

A tabela A abaixo mostra as políticas individuais, resume o conteúdo de cada política e o público-alvo das partes interessadas.

2.5. Aplicação da política de segurança da informação

As declarações de políticas feitas neste documento e no conjunto de políticas de suporte listadas na *Tabela 1* foram revisadas e aprovadas pela alta direção GRUPO SAURA e devem ser cumpridas. A falha de um funcionário em cumprir essas políticas pode resultar na tomada de medidas disciplinares de acordo com o processo interno da organização.

Perguntas relacionadas a qualquer política GRUPO SAURA deve ser abordada, em primeira instância, ao supervisor imediato do funcionário.

3. Introdução – Política da Dispositivos Moveis

A computação móvel é uma parte cada vez maior da vida cotidiana, à medida que os dispositivos se tornam menores e mais poderosos. No entanto, à medida que as capacidades aumentam, os riscos também aumentam. Os controles de segurança que evoluíram para proteger o ambiente de trabalho estático são facilmente ignorados quando se usa um dispositivo móvel além dos limites dos escritórios.

Dispositivos móveis incluem itens como:

- Laptops
- Tablets
- Smartphones
- Relógios inteligentes

O objetivo desta política é definir os controles que devem estar em vigor ao usar dispositivos móveis. Destina-se a conter os seguintes riscos:

- Perda ou roubo de dispositivos móveis, incluindo os dados neles
- Introdução de vírus e malwares para a rede
- Perda da reputação

É importante que os controles estabelecidos nesta política sejam observados em todos os momentos, inclusive no uso e transporte de dispositivos móveis.

Esta política se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas GRUPO SAURA.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de Controle de Acesso*
- *Política Criptográfica*

4. Política de Dispositivos Móveis

4.1. Dispositivos fornecidos - GRUPO SAURA

A menos que especificamente autorizado, somente dispositivos móveis fornecidos GRUPO SAURA devem ser usados para manter ou processar informações internas em nome da organização.

Se você precisar usar equipamentos móveis, receberá um dispositivo adequado, que será configurado para cumprir as políticas da organização. O suporte será fornecido pelo Suporte de TI, que pode, às vezes, precisar de acesso ao seu dispositivo para resolução de problemas e manutenção.

Você deve garantir que o dispositivo seja transportado em um invólucro protetor quando possível e não seja exposto a situações nas quais possa ser danificado. Não deixe o dispositivo à vista do público, como na parte de trás de um carro ou em uma sala de reunião ou lobby de hotel.

Não remova nenhuma marca de identificação no dispositivo, como uma etiqueta de patrimônio da empresa ou um número de série. Verifique se o dispositivo está bloqueado, quais informações estão sendo armazenadas e se a chave de acesso pode ser facilmente identificada.

Não adicione hardware periférico ao dispositivo sem a aprovação do Suporte de TI. O Suporte de TI deve ser consultado antes que o dispositivo seja retirado. Isso é para garantir que funcionará e para considerar quaisquer implicações de seguro.

Você não manterá informações internas no dispositivo, a menos que isso tenha sido autorizado e que os controles apropriados (por exemplo, criptografia) sejam implementados. Não deixe tokens de acesso, números de identificação pessoal ou outros itens de segurança com o dispositivo.

Certifique-se de que a tela do dispositivo "trave" após um curto período de inatividade e que exija um código de acesso ou senha para desbloqueá-lo. As senhas usadas devem ser fortes. Nenhum logins não seguro, ou seja, aqueles que não exigem uma senha podem ser configurados no dispositivo.

O dispositivo fornecido pela organização é apenas para uso comercial; não deve ser compartilhado com familiares ou amigos ou usado para atividades pessoais. Você pode ser solicitado a devolver o dispositivo ao Suporte de TI a qualquer momento para inspeção e auditoria. Você não deve instalar nenhum software não autorizado ou alterar a configuração do dispositivo sem antes consultar o Suporte de TI.

Sempre que possível, o dispositivo será protegido para que todos os dados nele contidos sejam criptografados e, portanto, só estarão acessíveis se a senha for conhecida. Se o dispositivo for fornecido com criptografia, não o desative.

As alterações nos arquivos contidos no dispositivo podem não sofrer backup regularmente se não estiverem conectados à rede corporativa por um período. Tente agendar algum tempo para fazer isso regularmente. Não faça seus próprios backups não criptografados de informações internas.

Quando possível, a proteção contra vírus será instalada no dispositivo pela organização. Verifique se o dispositivo está conectado à rede corporativa regularmente para permitir a atualização das assinaturas de vírus. Não desabilite a proteção contra vírus no dispositivo.

O dispositivo não deve estar conectado a redes não corporativas, como as sem fio, a menos que uma VPN (Rede privada virtual) seja usada. Quando estiver em locais públicos, certifique-se de que é uma rede privada, de modo que pessoas não autorizadas não possam ver (ou tirar fotos ou filmar) a tela.

Uso de Dispositivos Móveis Pessoais

O baixo custo e disponibilidade geral de tais dispositivos tem alimentado o desejo entre os funcionários e outras partes interessadas de usar seus próprios dispositivos para uso comercial. Isso é comumente chamado de "Traga seu próprio dispositivo" (TSPD). Em alguns casos, isso pode fornecer maior flexibilidade e eliminar a necessidade de o funcionário levar mais de um dispositivo regularmente.

No entanto, o conceito de permitir que um funcionário use seu(s) próprio(s) dispositivo(s) para fins comerciais pode resultar na necessidade de tais dispositivos estarem sujeitos a controles adicionais.

Problemas comuns e desafios de segurança com TSPD:

- Uso do dispositivo por outros membros da família
- Armazenamento padrão de dados e instalações de backup em nuvem
- Aumento da exposição a potenciais perdas em ambientes sociais
- Acesso potencial a sites que não atendem à política de uso aceitável das organizações
- Conexão a redes inseguras, por ex. pontos de acesso sem fio inseguros

- Proteção antivírus e com que frequência o dispositivo é corrigido
- Instalação de aplicativos potencialmente mal-intencionados no dispositivo (geralmente sem que o usuário saiba que é malicioso)

Essas questões devem ser consideradas ao avaliar a adequação de qualquer dispositivo como apto para conter dados específicos pertencentes à organização.

É uma decisão conjunta entre a organização e o proprietário do dispositivo. Esse uso não é obrigatório, e o funcionário tem o direito de decidir se os controles adicionais colocados no dispositivo pela organização são aceitáveis e se eles optam por usar o dispositivo para fins comerciais.

É importante que os controles definidos nesta política sejam observados em todos os momentos, no uso e no transporte de dispositivos móveis TSPD.

Os indivíduos não devem usar seus próprios dispositivos para manter e processar informações da empresa, a menos que tenham enviado uma solicitação para fazê-lo, e essa solicitação tenha sido formalmente aprovada. É política da GRUPO SAURA avaliar cada solicitação TSPD para estabelecer:

- A identidade da pessoa que faz a solicitação
- O motivo comercial da solicitação
- Os dados que serão mantidos ou tratados no dispositivo
- O dispositivo específico que será usado

As solicitações devem ser enviadas para o Suporte de TI.

O princípio geral desta política é que o grau de controle exercido pela organização sobre o dispositivo TSPD seja apropriado para a sensibilidade dos dados contidos nela.

Orientações sobre a decisão de quem deve ter acesso, quais informações e qual dispositivo, está resumido na *Tabela B* abaixo.

Para garantir que seus dados sejam protegidos adequadamente, é importante que GRUPO SAURA possa monitorar e auditar o nível de conformidade com essa política. O nível de monitoramento e auditoria será deve ser apropriado para cada informação armazenada no dispositivo.

Os métodos e o tempo de monitoramento e auditoria deverão respeitar a privacidade do proprietário do dispositivo, em conformidade com a

legislação aplicável. Em geral, o monitoramento do uso fora do horário comercial será evitado.

No caso de perda ou roubo do dispositivo, o proprietário deve informar o Suporte de TI o mais rápido possível, fornecendo detalhes sobre as circunstâncias da perda e a sensibilidade das informações comerciais armazenadas nele. GRUPO SAURA reserva o direito de apagar remotamente o dispositivo, sempre que possível, como medida de segurança. Isso pode envolver a exclusão de dados não comerciais pertencentes ao proprietário do dispositivo.

Ao sair da organização, o proprietário do dispositivo deve permitir que o dispositivo seja auditado e todos os dados e aplicativos relacionados ao negócio sejam removidos.

5. Introdução – Controle de Acesso

O controle do acesso aos nossos ativos de informação é parte fundamental da estratégia de defesa para a segurança da informação. Se quisermos proteger efetivamente a confidencialidade, a integridade e a disponibilidade de dados confidenciais, devemos garantir que haja uma combinação abrangente de controles.

A política de controle de acesso deve garantir que as medidas implementadas sejam adequadas a proteção e não sejam desnecessariamente rigorosas. A política, portanto, deve se basear em um entendimento claro dos requisitos do negócio.

Esses requisitos podem depender de fatores como:

- A classificação de segurança das informações armazenadas e tratadas por um determinado sistema ou serviço
- Legislação relevante que pode ser aplicada, por ex. a LGPD
- Obrigações contratuais com terceiros externos
- As ameaças, vulnerabilidades e riscos envolvidos
- A preferência da organização com relação ao risco

Essa política de controle de acesso é projetada para levar em conta os requisitos de segurança dos negócios e informações da organização, e está sujeita a revisão regular para garantir que ela permaneça apropriada.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros

diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas GRUPO SAURA.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de Dispositivos Móveis*
- *Política de Segurança de Rede*
- *Política de Computação em Nuvem*

5.1. Requisitos do Controle de Acesso

Os requisitos de segurança da informação devem estar claramente definidos e devem levar em consideração os padrões da organização.

Além dos requisitos específicos, vários princípios gerais serão usados ao projetar controles de acesso para os sistemas e serviços da GRUPO SAURA.

Esses são:

- ***Defesa em Profundidade -*** a segurança não deve depender de um único controle, mas sim a soma de um número de controles complementares
- ***Necessidade-*** o acesso é concedido apenas às informações necessárias ou para desempenhar uma função, e não mais que isso
- ***Necessidade de uso -*** os usuários só poderão acessar as instalações necessárias para sua função

A adesão a esses princípios básicos ajudará a manter os sistemas seguros, reduzindo as vulnerabilidades e, portanto, o número e a gravidade dos incidentes de segurança.

Como parte da seleção de provedores de serviços em nuvem especificamente, as seguintes considerações relacionadas a acesso devem ser levadas em consideração:

- Funções de registro e cancelamento de registro do usuário
- Instalações para gerenciar os direitos de acesso ao serviço em nuvem
- Disponibilidade de autenticação para contas de administrador
- Procedimentos para destinação de informações secretas, como senhas

Abordar esses requisitos como parte do processo de seleção garantirá que as providencias desta política são atendidas.

6. Gerenciamento de acesso do usuário

Os procedimentos formais de controle de acesso do usuário devem ser documentados, implementados e mantidos atualizados para cada aplicativo e sistema de informações, isto para garantir o acesso de usuário autorizado e impedir o acesso não autorizado. Eles devem abranger todos os estágios do ciclo de vida do usuário, desde o registro inicial até o cancelamento final.

Os direitos de acesso do usuário devem ser revisados em intervalos regulares. As contas de administração do sistema só devem ser fornecidas aos usuários que realmente irão executar tarefas de administração do sistema.

6.1. Registro de usuário

Uma solicitação de acesso à rede e aos sistemas de computadores da organização deve primeiro ser enviada ao Suporte de TI para aprovação. Todas as solicitações serão tratadas de acordo com um procedimento formal que garanta que as verificações de segurança sejam realizadas e que a autorização seja obtida antes da criação da conta de usuário.

Cada conta de usuário terá um nome de usuário exclusivo que não será compartilhado e será associado a um indivíduo específico, ou seja, não um cargo. Contas de usuário genéricas, ou seja, contas individuais a serem usadas por um grupo de pessoas não devem ser criadas, pois não fornecem garantias suficiente de responsabilidade.

Uma senha inicial forte deve ser criada na configuração da conta e comunicada ao usuário por meios seguros. O usuário deve ser obrigado a alterar a senha no primeiro uso da conta.

Quando o funcionário se retira da organização, em circunstâncias comuns, seu acesso aos sistemas e dados deve ser suspenso no último dia de trabalho. É responsabilidade do supervisor solicitar a suspensão dos direitos de acesso por meio de e-mail ao Suporte de TI.

Em circunstâncias excepcionais, em que haja um risco de o funcionário tomar providências que possam prejudicar a organização antes ou após a rescisão, uma solicitação para remover o acesso pode ser aprovada e acionada antes da notificação da rescisão. Esta precaução será aplicável nos casos em que o funcionário tem acessos privilegiados, por ex. administrador de domínio.

As contas de usuário devem ser inicialmente suspensas ou desativadas apenas, e não excluídas. Os nomes das contas de usuários não devem ser

reutilizados, pois isso pode causar confusão no caso de uma investigação posterior.

Fornecimento do acesso

Cada usuário deve ter direito de acesso e permissões a sistemas de computador e dados que sejam compatíveis com as tarefas que deve executar. Em geral, isso será baseado na função, ou seja, uma conta de usuário será adicionada a um grupo com as permissões de acesso exigidas para essa função.

As funções de grupo devem ser mantidas de acordo com os requisitos do negócio e quaisquer alterações devem ser formalmente autorizadas e controladas por meio do processo de gerenciamento de mudanças.

As permissões adicionais não devem ser concedidas a contas de usuário fora da função do grupo; se tais permissões forem necessárias, isso deve ser tratado como uma modificação e formalmente solicitado.

6.2. Remoção ou adequação dos direitos de acesso

Quando é necessário um ajuste de direitos ou permissões de acesso, por exemplo, devido a uma alteração individual da função, isso deve ser feito como parte da mudança de função. É preciso garantir que os direitos de acesso, que não são mais necessários na nova função sejam removidos da conta do usuário. No caso de um usuário assumir uma nova função além da existente (e não em vez de), deve ser solicitado mudanças.

Sob nenhuma circunstância os administradores poderão alterar suas próprias contas de usuário ou permissões.

6.3. Gestão dos direitos de acesso privilegiado

Os direitos de acesso privilegiados, como aqueles associados a contas de nível de administrador, devem ser identificados para cada sistema ou rede e rigorosamente controlados. Em geral, os usuários técnicos (como a equipe de suporte de TI) não farão o uso diário de contas de usuário com acesso privilegiado. Em vez disso, uma conta de usuário "admin" separada deve ser criada e usada somente quando necessário. Estas contas devem ser específicas para um indivíduo, por ex. "João da Silva Admin". Contas de administração genéricas não devem ser usadas, pois fornecem identificação insuficiente do usuário.

O acesso a permissões no nível de administrador só deve ser destinado a indivíduos com essas funções e que receberam treinamento suficiente para entender as implicações de seu uso.

O uso de contas de usuário com acesso privilegiado em rotinas automatizadas, deve ser evitado sempre que possível. Quando isso for inevitável, a senha usada deve ser protegida e alterada regularmente.

6.4. Autenticação do usuário para conexões externas

De acordo com a Política de segurança de rede, o uso de modems em PCs ou dispositivos não pertencentes à organização conectados à rede da organização pode comprometer seriamente a segurança da rede. A aprovação específica deve ser obtida antes de conectar qualquer equipamento à rede da organização.

Quando o acesso remoto à rede é necessário via VPN, uma solicitação deve ser feita por meio do Suporte de TI. A autenticação para acesso remoto será usada para reduzir o risco de acesso não autorizado da Internet.

Para mais informações, consulte a *Política de Dispositivos Móveis*.

6.5. Acesso remoto do fornecedor à rede da organização

As agências parceiras ou fornecedores terceirizados não devem receber detalhes sobre como acessar a rede da organização sem a permissão do Suporte de TI. Todas as permissões e métodos de acesso devem ser controlados pelo Suporte de TI.

Os parceiros ou fornecedores terceirizados devem entrar em contato com o Suporte de TI em cada ocasião para solicitar permissão para se conectar à rede e um log de atividades deve ser mantido. O software de acesso remoto e as contas de usuário devem ser desativados quando não estiverem em uso.

6.6. Revisão dos direitos de acesso ao usuário

Anualmente, os responsáveis de ativos e sistemas serão obrigados a analisar quem tem acesso às suas áreas de responsabilidade e o nível de acesso. Isto para identificar:

- Pessoas que não devem ter acesso (por exemplo, saiu da empresa)
- Contas de usuário com mais acesso do que o exigido pela função
- Contas de usuário com alocações de função incorretas
- Contas de usuário que não fornecem identificação adequada, por exemplo contas genéricas ou compartilhadas

- Quaisquer outros problemas que não estejam em conformidade com esta política

Esta revisão será realizada por um procedimento formal e quaisquer ações corretivas identificadas e realizadas.

Uma revisão das contas de usuários com acesso privilegiado será realizada trimestralmente pelo Felipe Daniel Ribeiro para assegurar que esta política esteja sendo cumprida.

6.7. Política de autenticação e senha do usuário

Uma senha forte é uma barreira essencial contra o acesso não autorizado.

A GRUPO SAURA utiliza métodos de autenticação adicionais com base em uma avaliação de riscos que leve em consideração:

- O valor dos ativos protegidos
- O grau de ameaça que se acredita existir
- O custo do(s) método(s) adicional(is) de autenticação
- A facilidade de uso e praticidade do(s) método(s) proposto(s)
- Quaisquer outros controles relevantes

O uso de métodos de autenticação de múltiplos fatores deve ser justificado com base nos fatores acima, e implementados e mantidos de maneira segura.

Se a autenticação de um ou vários fatores é usada, a qualidade das senhas de usuários deve ser aplicada, conforme os seguintes parâmetros:

Parâmetro	Valor
Comprimento mínimo	12
Comprimento máximo	16
Caracteres necessários	Pelo menos uma letra maiúscula Pelo menos um símbolo Pelo menos um numero
Mudar a frequência	Pelo menos a cada 90 dias
Bloqueio de conta	Em 5 tentativas incorretas de logon
Ação de bloqueio de conta	A conta deve ser reativada pelo Suporte de TI
Outros controles	A senha não pode conter o nome do usuário

Quaisquer exceções a estas regras devem ser autorizadas pelo Felipe Daniel Ribeiro.

Responsabilidades do usuário

Para exercer o devido cuidado e tentar garantir a segurança de suas informações, GRUPO SAURA gasta uma quantidade significativa de tempo e dinheiro na implementação de controles eficazes para diminuir o risco e reduzir as vulnerabilidades.

No entanto, muito ainda depende do grau de cuidado exercido pelos usuários de redes e sistemas em suas funções do dia a dia. Muitas violações recentes de segurança foram, em grande parte, causadas por acesso não autorizado a contas de usuários, por meio de senhas roubadas ou descobertas.

É vital, portanto, que todos os usuários desempenhem sua parte na proteção do acesso que receberam e garantam que sua conta não seja usada para prejudicar a organização.

Para maximizar a segurança de nossas informações, todo usuário deve:

- Ter uma senha forte, ou seja, que esteja de acordo com as regras definidas nesta política
- Nunca informar sua senha ou permitir que alguém use sua conta
- Não anotar sua senha por escrito ou eletronicamente, por exemplo. em um arquivo ou e-mail
- Evitar usar a mesma senha para outras contas de usuário, pessoais ou relacionadas a negócios
- Assegurar de que qualquer PC ou dispositivo conectado à rede esteja bloqueado ou desconectado, quando não estiver por perto
- Informar o Suporte de TI sobre quaisquer alterações em suas funções e requisitos de acesso

O não cumprimento desses requisitos pode resultar na aplicação de ações disciplinares contra o(s) indivíduo(s) envolvido(s).

7. Controle de acesso de sistemas e aplicativos

No processo de avaliação de sistemas novos ou significativamente modificados, os requisitos para o controle de acesso devem ser abordados e as medidas adequadas implementadas.

Eles devem consistir em um modelo de segurança abrangente que inclua suporte para o seguinte:

- Criação de contas de usuários individuais
- Definição de funções ou grupos aos quais as contas de usuário podem ser atribuídas
- Atribuição de permissões a objetos (por exemplo, arquivos, programas, menus) de tipos diferentes (por exemplo, ler, gravar, excluir, executar) de assuntos (contas e grupos de usuários)
- Fornecimento de visualizações variadas de opções de menu e dados de acordo com a conta do usuário e seus níveis de permissão
- Administração de conta de usuário, incluindo capacidade de desativar e excluir contas
- Controles de login do usuário, como
  - Não exibição da senha quando está sendo inserida
  - Bloqueio da conta, quando o número de tentativas incorretas de login exceder um limite especificado
  - Fornecer informações sobre o número de tentativas de login malsucedidas e o último login bem-sucedido
  - Restrições de login baseadas em data e hora
  - Restrições de login de dispositivos e locais
- Tempo limite de inatividade do usuário
- Gerenciamento de senhas, incluindo
  - Capacidade de usuário alterar senha
  - Controlar as senhas aceitáveis
  - Expiração da senha
  - Armazenamento e transmissão de senhas criptografadas

- Recursos de auditoria de segurança, incluindo login/logoffs, tentativas de login malsucedidas, acesso a objetos e atividades de administração de contas

Quando é realizado o desenvolvimento de software personalizado, o código-fonte do programa deve ser protegido contra acesso não autorizado.

8. Introdução – Política de Criptografia

Um componente chave no conjunto de controles disponíveis para as organizações protegerem suas informações é o uso de técnicas criptográficas para "embaralhar" dados, de modo que eles não possam ser acessados sem o conhecimento de uma chave.

Controles criptográficos podem ser usados para alcançar vários objetivos relacionados à segurança da informação, incluindo:

- ***Confidencialidade*** - garantindo que as informações não possam ser lidas por pessoas não autorizadas
- ***Integridade*** - provando que os dados não foram alterados em trânsito ou no armazenamento
- ***Não-repúdio*** – demonstrando se um evento ocorreu ou não ou que uma mensagem foi enviada por um indivíduo

A necessidade de controles criptográficos será destacada na avaliação de risco GRUPO SAURA e obviamente não será aplicável em todos os casos. No entanto, quando seu uso puder fornecer o nível de proteção exigido, ele deverá ser aplicado de acordo com as disposições estabelecidas nesta política.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas GRUPO SAURA.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de Aceitação pelo Usuário*
- *Política de Dispositivos Móveis*
- *Política de Segurança de Rede*

9. Política sobre o uso de controles criptográficos

Para identificar as áreas nas quais a implantação de técnicas criptográficas será útil, GRUPO SAURA adotará uma abordagem gerenciada da seguinte maneira.

9.1. Avaliação de riscos

O primeiro passo será realizar uma avaliação de risco. Para cada um dos ativos de informação identificados dentro da organização, possíveis ameaças serão avaliadas juntamente com sua probabilidade e impacto, caso ocorram.

Os requisitos para o uso de técnicas criptográficas serão identificados em um plano de tratamento de risco. Isso mostrará em visão geral onde as técnicas de criptografia devem ser aplicadas e de que forma atingir o nível de proteção necessário.

Em termos gerais, o uso de criptografia poderá ser aplicado na proteção de informações sensíveis.

Além disso, a criptografia deve ser considerada nos seguintes cenários:

- Em dispositivos móveis, como laptops, tablets e smartphones
- Para uso autorizado de mídia removível, como cartões de memória USB e Pen Driver
- Quando dados sensíveis são transmitidos através de linhas de comunicação que se estendem além dos limites da organização, por exemplo, na internet
- Quando os serviços em nuvem são usados, independentemente do tipo de serviço em nuvem (por exemplo, IaaS, PaaS, SaaS)

9.2. Seleção de técnica

Uma vez que a necessidade geral de uso da criptografia foi identificada pela avaliação de risco, é necessário tomar uma decisão sobre quais técnicas específicas serão implantadas. Isso também envolverá a seleção e possível compra de software ou hardware para implementar a técnica. As instalações fornecidas pelos provedores de serviços em nuvem (PSN) também podem ser usadas - em alguns casos, a escolha pode ser restringida pelas ferramentas disponíveis ou aprovadas para uso pelo PSN.

Observe que a seleção de tais técnicas deve levar em conta quaisquer regulamentações atuais ou restrições nacionais sobre a aquisição e uso de tecnologia criptográfica.

Em geral, a política GRUPO SAURA é usar as seguintes técnicas para o processo ou situação:

Processo/Situação	Técnica	Orientação Específica
Armazenamento de dados na nuvem	Criptografia AES-256 em repouso	Chaves que não devem ser mantidas pelo CSP
Proteção de dados em mídia removível, NAS e Storage	Criptografia simétrica	Criptografia AES-256 a ser usada quando disponível
Proteção de senhas em sistemas	Todas as senhas devem ser hash	Hash MD5 para ser usado quando disponível
Segurança de e-mail	Criptografia simétrica / assimétrica usando S/ MIME e SSL/TLS	Os recursos disponíveis no cliente de e-mail relevante devem ser usados para simplificar o processo
Acesso remoto	Rede Privada Virtual (RPV) usando TLS	Uma VPN IPSec ou OpenVPN pode ser usada quando permitido pela *Política de Segurança de Rede*

Tabela 1 – Técnicas Criptográficas

O uso continuado das técnicas especificadas será avaliado em cada revisão desta política.

9.3. Implementação

A implantação de técnicas criptográficas deve ser gerenciada cuidadosamente para garantir que o nível desejado de segurança seja de fato alcançado. Sempre que possível, mais de um membro estará envolvido na implantação, a fim de evitar falhas e permitir a segregação de funções.

9.4. Teste e Revisão

Uma vez implantado, é essencial que a segurança da criptografia seja testada sob condições tão realistas quanto possível, a fim de identificar quaisquer pontos fracos. Esses testes devem cobrir o uso de:

- ferramentas de software comumente disponíveis para tentar quebrar a criptografia
- métodos de engenharia social para tentar descobrir a chave
- interceptação de dados criptografados em vários pontos de sua transmissão

Os resultados dos testes serão formalmente revisados e as lições aprendidas serão aplicadas.

Observe que, no caso de serviços em nuvem, a aprovação pode ser necessária antes da realização de testes.

10. Introdução – Política de Segurança Física

A proteção do ambiente físico é uma das tarefas mais óbvias e mais importantes, na área de segurança da informação. A falta de controle de acesso físico pode desfazer precauções técnicas mais cuidadosas e potencialmente colocar vidas em risco.

A GRUPO SAURA está comprometida em garantir a segurança de seus funcionários, contratados e ativos e leva a questão da segurança física muito a sério. Esta política define as principais precauções que devem ser tomadas e, juntamente com o suporte documentado, forma uma parte significativa do nosso conjunto de controle de segurança da informação.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas GRUPO SAURA.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de Dispositivos Móveis*

10.1. Áreas Seguras

Informações confidenciais devem ser armazenadas com segurança. Uma avaliação de risco deve ser realizada para identificar o nível apropriado de proteção a ser implementado, para proteger as informações armazenadas.

A segurança física deve começar com o próprio edifício e uma avaliação da vulnerabilidade do perímetro deve ser realizada. Um edifício deve ter mecanismos de controle adequados para as informações sensíveis e equipamentos armazenados nele.

Estes podem incluir, mas não estão restritos, aos seguintes:

- Alarmes instalados e ativados fora do horário de trabalho
- Fechaduras de janelas e portas
- Barras na janela nos níveis do piso inferior
- Mecanismos de controle de acesso instalados em todas as portas acessíveis (onde os códigos são utilizados, eles devem ser trocados regularmente e conhecidos apenas pelas pessoas autorizadas a acessar a área / prédio)
- Câmeras de CFTV
- Área de recepção pessoal
- Proteção contra danos - por ex. fogo, inundação, vandalismo

A equipe que trabalha em áreas segurança deve interpelar qualquer um que não esteja usando um crachá.

As ferramentas de identificação e acesso (por exemplo, crachás, chaves, códigos de entrada, etc.) devem ser mantidos apenas por pessoas autorizadas a entrar nessas áreas e não devem ser emprestados/fornecidos a qualquer outra pessoa.

As chaves para todas as áreas que abrigam equipamentos de TI e gabinetes de TI bloqueáveis são realizadas especificamente pelo Suporte de TI.

Quando ocorrerem violações ou quando um funcionário fizer a rescisão, todas as ferramentas de identificação e acesso (por exemplo, crachás, chaves, etc.) devem ser recuperados e qualquer porta/códigos de acesso devem ser alterados imediatamente.

10.2. Papel e Segurança do Equipamento

Informações baseadas em papel (ou similares não eletrônicas) devem receber um proprietário e uma classificação. Controles apropriados de segurança da informação devem ser colocados em prática para protegê-lo de acordo com as disposições dos procedimentos de manuseio de ativos.

A documentação física de um escritório deve ser protegida pelos controles do prédio e pelas medidas apropriadas que podem incluir, mas não estão restritas, ao seguinte:

- Armários de arquivamento que são bloqueados com as chaves armazenadas longe do gabinete
- Cofres trancados
- Armazenado em uma área segura protegida por controles de acesso

Todo o equipamento informático geral deve estar localizado de forma adequada que:

- Limite os riscos de perigos ambientais - por ex. calor, fogo, fumaça, água, poeira e vibração
- Limite o risco de roubo - por ex. se necessário, itens como laptops devem estar fisicamente conectados à mesa
- Permita que as estações de trabalho que manipulam dados confidenciais sejam posicionadas de modo a evitar o risco de os dados serem vistos por pessoas não autorizadas

Os dados devem ser armazenados em servidores de arquivos de rede, quando disponíveis. Isso garante que as informações perdidas, roubadas ou danificadas por meio de acesso não autorizado possam ser restauradas e sua integridade mantida.

Todos os servidores localizados fora do data center devem ser instalados em um ambiente fisicamente seguro.

Os sistemas críticos para os negócios devem ser protegidos por uma fonte de alimentação interrupta para reduzir o risco de falhas no sistema operacional e no risco de corrupção de dados.

Todos os itens do equipamento devem ser registrados no inventário do Suporte de TI. Os procedimentos devem estar em vigor para garantir que o inventário seja atualizado assim que os ativos forem recebidos ou descartados.

Todos os equipamentos devem ser marcados com segurança e ter um número de ativo exclusivo alocado a ele. Este número de ativo deve ser registrado no inventário do Suporte de TI.

Os cabos que transportam dados ou suportam serviços de informações importantes devem ser protegidos contra interceptação ou danos.

Os cabos de energia devem ser separados dos cabos de rede para evitar interferência. Os cabos de rede devem ser protegidos por conduítes e, sempre que possível, evitar rotas através de áreas públicas.

10.3. Gestão do ciclo de vida dos equipamentos

Os fornecedores de serviços e fornecedores terceirizados devem garantir que todos os equipamentos de TI da GRUPO SAURA sejam mantidos de acordo com as instruções do fabricante, e quaisquer procedimentos internos documentados para garantir que permaneçam em funcionamento efetivo.

O pessoal envolvido na manutenção deve:

- Guardar todas as cópias das instruções do fabricante
- Identificar quando deve haver manutenção recomendada
- Ativar um processo de chamada em caso de falha
- Registrar detalhes de todo o trabalho de reparação realizado
- Identificar quaisquer requisitos de segurança
- Registrar detalhes das falhas ocorridas e ações necessárias

Um registro de histórico de serviço do equipamento deve ser mantido para que as decisões possam ser tomadas em relação ao tempo apropriado para a substituição.

As instruções de manutenção do fabricante devem estar documentadas e disponíveis para uso pela equipe de suporte ao organizar os reparos.

O uso de equipamentos fora do local deve ser formalmente aprovado pelo supervisor do usuário.

O equipamento que deve ser reutilizado ou descartado deve ter todos os seus dados e software apagados/destruídos.

As entregas de equipamento devem ser assinadas por um indivíduo autorizado usando um processo formal. Este processo deve confirmar que os itens entregues correspondem totalmente à lista na nota de remessa. Os ativos reais recebidos devem ser registrados.

As áreas de carregamento e as instalações de armazenamento devem ser adequadamente protegidas contra acesso não autorizado e todo o acesso deve ser registrado.

Os arranjos de segurança da informação devem estar sujeitos a auditorias independentes regulares e melhorias de segurança recomendadas quando necessário.

10.4. Gestão-Chave

É vital que as chaves criptográficas sejam protegidas contra modificação, perda, destruição e divulgação não autorizada. Uma abordagem do ciclo de vida para o gerenciamento da chave exigirá a criação de procedimentos específicos para cobrir as seguintes etapas:

- Geração de chaves
- Distribuição de chaves para ponto de uso
- Armazenamento no ponto de uso
- Backup como proteção contra perda
- Recuperação em caso de perda
- Atualização de chaves quando expirado
- Revogação quando comprometido
- Destruição quando não é mais necessário
- Registro e auditoria de atividades relacionadas ao gerenciamento de chaves

Esses procedimentos levarão em consideração as circunstâncias específicas em que a criptografia será usada.

Em princípio, chaves assimétricas privadas e chaves simétricas devem existir apenas nas seguintes formas seguras:

1. Como texto não criptografado dentro da memória de um dispositivo de criptografia baseado em hardware
2. Como texto cifrado fora da memória de um dispositivo de criptografia baseado em hardware
3. Como dois ou mais fragmentos de chave em texto não criptografado ou texto cifrado, gerenciados usando o controle duplo com conhecimento dividido

O uso de uma dessas três formas garantirá que a confidencialidade das chaves privadas assimétricas e simétricas seja mantida em todos os momentos. As chaves públicas assimétricas estão geralmente disponíveis e, portanto, não requerem proteção. Sua integridade e autenticidade, no entanto, precisam ser protegidas e isso deve ser feito através do uso de uma assinatura de autoridade de certificação respeitável.

Quando a funcionalidade de gerenciamento de chaves é fornecida como parte de um serviço de nuvem, as seguintes informações devem ser solicitadas sobre os recursos fornecidos pelo CSP:

- Tipo de chaves
- Especificações do sistema de gerenciamento de chaves
- Procedimentos recomendados de gerenciamento de chaves para cada estágio do ciclo de vida, conforme definido acima

No caso de chaves criptográficas estarem sujeitas a uma solicitação de um órgão governamental, GRUPO SAURA cumprirá todas as solicitações legalmente autorizadas de maneira oportuna. O processo de conformidade estará sujeito à supervisão e controle da alta direção.

11. Introdução – Política Anti-Malware (Gestão de Vulnerabilidade)

A ameaça representada pelo malware nunca foi tão séria como atualmente. Os sistemas e usuários da GRUPO SAURA estão sob constante bombardeio de tentativas de contornar a segurança, a fim de obter algum tipo de ganho ou interromper o funcionamento normal da organização.

Essa ameaça pode vir de várias fontes, incluindo:

- Gangues organizadas que tentam roubar dinheiro ou cometer chantagem
- Organizações concorrentes tentando obter informações confidenciais
- Grupos politicamente motivados
- Funcionários desonestos dentro da organização
- Unidades de "guerra cibernética" patrocinadas por outros locais
- Indivíduos com curiosidade ou testando suas habilidades

Seja qual for a fonte, o resultado de uma violação de segurança bem-sucedida é que a organização e seus interessados são afetados, podendo causar dano.

Uma das principais ferramentas usadas por esses invasores é o malware, e é essencial que sejam tomadas precauções efetivas pela GRUPO SAURA para se proteger contra essa ameaça.

Este documento define a política da organização em relação à defesa contra malware. Seu público-alvo é o pessoal de gerenciamento e suporte de TI e segurança da informação que implementará e manterá as defesas da organização. As informações e conselhos relacionados a malware para usuários estão incluídos nos documentos de políticas referenciados abaixo.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas GRUPO SAURA.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de Dispositivos Móveis*
- *Política de Aceitação pelo Usuário*
- *Política de Mensagens Eletrônicas*
- *Procedimento de Resposta a Incidentes de Segurança da Informação*

12. A Ameaça Malware

12.1. Definição

Não existe uma definição única do termo "Malware", mas para os propósitos desta política é usada a seguinte definição:

"Malware é qualquer código ou software que possa ser prejudicial ou destrutivo para as capacidades de processamento de informações da organização"

O termo é derivado da expressão "Software Malicioso" e também pode ser chamado de código malicioso ou comumente (mas imprecisamente) "um vírus".

12.2. Tipos de Malware

O malware vem de várias formas e está em constante mudança, já que as formas de ataque anteriores vão se extinguindo e novas são encontradas. Os tipos mais comuns de malware encontrados hoje são:

- ***Vírus*** – um programa que executa uma função indesejada no computador infectado. Isso pode envolver ações destrutivas ou a coleta de informações que podem ser usadas pelo invasor
- ***Trojan*** – um programa que finge ser um código legítimo, mas que esconde outras funções indesejadas. Muitas vezes disfarçado como um jogo ou programa utilitário
- ***Worm*** – um programa capaz de se copiar em outros computadores ou dispositivos sem interação do usuário
- ***Logic bomb*** – código malicioso que foi configurado para ser executado em uma data e hora específica ou quando certas condições são atendidas
- ***Rootkit*** – um programa usado para disfarçar atividades maliciosas em um computador, ocultando os processos e arquivos do usuário
- ***Keylogger*** – código que registra as teclas digitadas pelo usuário
- ***Backdoor*** – um programa que permite acesso não autorizado ao invasor
- ***Ransomware*** –é um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos. O resgate é cobrado em criptomoedas, que, na prática, o torna quase impossível de se rastrear o criminoso.

Geralmente, esses tipos de malware serão usados em combinação uns com os outros.

12.3. Como o Malware se propaga

Para que um software mal-intencionado execute sua finalidade, ele precisa ser instalado no dispositivo ou no computador de destino. Há várias maneiras principais de o malware infectar computadores e redes, embora novas formas estejam sendo criadas o tempo todo.

As técnicas de infecção mais comuns são as seguintes.

Phishing

Esse método envolve enganar o usuário para realizar alguma ação que faça com que um programa malicioso seja executado e infecte o computador que está sendo usado. Geralmente é conseguido através do envio geral de e-mails não solicitados (Spam) com anexos de arquivos ou links da web. Quando o usuário abre o arquivo ou clica no link, a ação mal-intencionada é acionada.

Os ataques de Phishing se tornaram mais sofisticados nos últimos anos e podem ser muito convincentes e atraentes para o usuário. Versões mais segmentadas de Phishing apareceram, como o Spear Phishing (destinado a uma determinada organização) e até a Whaling (destinada a um indivíduo).

Websites e Código Móvel

O uso disseminado de códigos móveis, como o JavaScript, forneceu outra rota para infectar computadores com malware. Muitas vezes sites serão criados para hospedar o malware que é ativado ou clicando em um link ou, em alguns casos, simplesmente visitando o site.

Cada vez mais, sites legítimos são comprometidos e feitos para hospedar malware sem o conhecimento do proprietário, o que facilita muito esse tipo de ataque para o usuário.

Mídia Removível

Cartões de memória USB, CDs, DVDs e outros dispositivos de mídia removível fornecem uma maneira eficaz de espalhar malwares em computadores. Quando a mídia é inserida na máquina, o malware é executado e infecta o alvo ou se copia na mídia removível para se preparar para infectar a próxima máquina em que for conectado.

Hacking

Ou "Cracking", é um método mais direcionado e, portanto, menos comum de introduzir malware em um computador ou rede, obtendo acesso não autorizado à rede de fora (e às vezes dentro) da organização. Este método requer mais conhecimento por parte do agressor e, muitas vezes, explora as vulnerabilidades existentes no software ou nos dispositivos de rede utilizados. Depois que o acesso for obtido, o malware será instalado remotamente na máquina comprometida.

13. Política Anti-Malware

Para evitar a infecção de computadores e redes da GRUPO SAURA e evitar as consequências potencialmente terríveis de tal infecção, há uma série de controles importantes que serão adotados como política.

O conceito chave adotado nesta política é "defesa em profundidade" e nenhum controle individual deve ser usado para fornecer proteção adequada. Portanto, esta não é uma escolha entre os controles, mas uma lista de controles necessários, os quais devem ser implementados sempre que possível para proteger contra as ameaças anteriormente descritas.

13.1. Firewall

Um firewall será instalado em todos os pontos em que a rede interna estiver conectada à Internet.

Sempre que possível, os firewalls individuais serão ativados nos computadores. As permissões de acesso devem ser definidas de forma que o usuário não possa desabilitar o firewall.

13.2. Antivírus

Uma plataforma antivírus comercial com suporte será instalada na organização em locais chave:

- Firewall
- Servidores de e-mail
- Servidores proxy
- Todos os outros servidores
- Todos os computadores do usuário
- Dispositivos móveis, incluindo laptops (telefones e tablets, sempre que possível)

Todos antivírus serão configurados para obter atualizações de assinatura regularmente, diretamente do site do fornecedor ou de um servidor central da organização.

Por padrão, a varredura de acesso deve estar ativada para fornecer proteção em tempo real. Varreduras completas regulares também devem ser realizadas pelo menos uma vez por semana.

Os usuários não devem poder desativar a proteção configurada centralmente.

13.3. Filtragem de Spam

Um sistema será instalado para filtrar e-mails não solicitados e potencialmente prejudiciais (spam). Os tipos de anexos que costumam conter malware devem ser bloqueados ou removidos antes da entrega ao usuário.

13.4. Instalação do Software e Digitalização

Os usuários não devem ter acesso administrativo ao computador para permitir que instalem software nele. Somente software aprovado será permitido e isso deve ser instalado pelo departamento de TI mediante solicitação autorizada.

A varredura regular de computadores de usuários para detectar software não autorizado deve ser realizada.

13.5. Gestão de Vulnerabilidade

Informações sobre vulnerabilidades de software serão coletadas de fornecedores e fontes de terceiros e atualizações aplicadas quando disponíveis.

A varredura de vulnerabilidades deve ser realizada regularmente, particularmente em redes e servidores críticos para os negócios.

Para novas vulnerabilidades identificadas pelos funcionários da GRUPO SAURA, será feito o registro da ocorrência e um plano de ação deve ser criado para tratar o caso.

13.6. Treinamento de conscientização do usuário

Os usuários devem estar cientes quando começarem a trabalhar na organização da política de segurança da informação e receberem treinamento para evitar serem vítimas de ataques.

Esse treinamento de conscientização deve ser repetido a cada três meses para todos os funcionários que fazem uso de equipamentos de TI.

13.7. Monitoramento de ameaças e alertas

Informações sobre ameaças emergentes serão obtidas de fontes adequadas e usuários alertados sobre possíveis ataques, fornecendo o máximo de detalhes para maximizar a chance de reconhecimento.

Tais informações devem ser divulgadas a semanalmente pelo Suporte de TI via e-mail.

13.8. Revisões Técnicas

Avaliações regulares serão realizadas em redes e servidores essenciais aos negócios para identificar qualquer malware que tenha sido instalado desde a última revisão.

Tais revisões devem ser realizadas conforme calendário de manutenção preventiva e corretivas do Suporte de TI.

13.9. Gestão de Incidentes de Malware

No caso de um malware ser detectado em um servidor, cliente, rede ou outro componente de TI, um incidente de segurança das informações será gerado. Isso será gerenciado de acordo com os procedimentos estabelecidos no *Procedimento de Resposta a Incidentes de Segurança da Informação*.

14. Introdução – Política de Segurança de Rede

O uso de redes é uma parte essencial dos negócios do dia a dia da GRUPO SAURA. As redes não apenas conectam, internamente, muitos dos componentes e processos de negócios, mas também vincula a organização a seus fornecedores, clientes, partes interessadas e ao mundo externo.

As redes da organização evoluíram ao longo de um período de tempo para se tornar um sistema circulatório da empresa, transportando as informações para onde precisam ir e permitindo que os negócios sejam realizados de forma eficaz.

Mas o fato de tantas informações percorrerem nossas redes, as torna um alvo para aqueles que tentam roubar essas informações e atrapalhar nossos negócios. Portanto, essas redes precisam ser protegidas para garantir que a confidencialidade, integridade e disponibilidade das nossas informações sejam garantidas a todo momento.

A proteção efetiva de nossas redes exige que adotemos boas práticas de segurança da informação e garantimos que todos os envolvidos sigam essas práticas.

Essa política define as regras e os padrões da GRUPO SAURA para proteção da rede e atua como um guia para aqueles que criam e mantêm nossa infraestrutura de TI. Seu público-alvo é o pessoal de gerenciamento e suporte de TI e segurança da informação que implementará e manterá as defesas da organização.

Como um provedor de serviços de nuvem (PSN), essa política também se aplica aos métodos usados para projetar e criar as redes físicas e virtuais para fornecer serviços a nossos clientes na nuvem.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas GRUPO SAURA.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de dispositivos móveis*
- *Política anti-malware*

15. Política de Segurança de Rede

15.1. Projeto de Segurança de Rede

O design de redes é um processo complicado que requer um bom conhecimento dos princípios e tecnologia de rede. Cada projeto provavelmente será diferente, com base em um conjunto específico de requisitos estabelecidos no início do processo. Esta política não tenta especificar como redes individuais devem ser projetadas e construídas, mas fornece orientação para padrões que devem ser usados.

15.1.1. Requisitos

Um projeto de rede deve se basear em uma definição clara de requisitos, incluindo os seguintes fatores relacionados à segurança:

- A classificação da informação a ser transportada através da rede e acessada através dela
- Uma avaliação de risco das ameaças potenciais à rede, levando em consideração quaisquer vulnerabilidades inerentes
- O nível de confiança entre os diferentes componentes ou organizações que serão conectadas
- A expansão geográfica da rede
- Os controles de segurança nos locais onde a rede será acessada
- Recursos de segurança de computadores ou dispositivos existentes que serão usados para acesso

Os requisitos devem ser documentados e acordados antes do início do trabalho de design.

15.1.2. Defesa em Profundidade

Uma abordagem de "Defesa em Profundidade" será adotada para segurança de rede, através da qual várias camadas de controles são usadas para garantir que a falha de um único componente não comprometa a rede. Por exemplo, os firewalls de rede podem ser complementados por firewalls de software baseados em servidores hospedados, a fim de fornecer vários níveis de proteção.

Em pontos chave da rede, uma abordagem de "diversidade de defesa" também deve ser adotada para que as vulnerabilidades sejam minimizadas. Por exemplo, isso pode envolver o uso de firewalls de diferentes fornecedores, de modo que, se uma vulnerabilidade for explorada em um dispositivo, o outro não estará sujeito a ela. Isso pode ser estendido para o uso de mais de um scanner de vírus de rede.

15.1.3. Segregação em rede

Uma rede consistirá de um conjunto de redes menores segregadas umas das outras com base em níveis de confiança ou limites organizacionais (ou ambos).

Para uma rede grande, isso pode ser alcançado usando domínios separados, particularmente onde as redes de organizações separadas estão sendo vinculadas. Um nível apropriado de confiança deve ser configurado no nível do domínio e os perímetros de domínio devem ser protegidos usando um firewall, quando apropriado.

Nas redes, as redes locais virtuais (RLV) serão usadas para segregar as unidades organizacionais.

Em um ambiente de nuvem, é importante que os requisitos para segregar redes para obter isolamento de inquilino sejam definidos e a capacidade do provedor de serviços de nuvem de atender a esses requisitos seja verificada.

Onde GRUPO SAURA está agindo como um PSN, é importante impor a segregação entre nossos clientes multilocatários e entre o ambiente do cliente de serviço de nuvem e nossa própria rede interna.

15.1.4. Segurança do Perímetro

Em todos os perímetros entre a rede interna e uma rede externa (como a Internet), medidas efetivas devem ser tomadas para assegurar que apenas o tráfego de rede autorizado seja permitido. Isso geralmente consistirá em pelo menos um firewall de inspeção com informações de estado e, para os principais links com a Internet, um firewall de aplicativo (ou gateway de aplicativos) deve ser usado. Para conexões como banda larga em locais menores, um firewall de Filtragem de Pacotes pode ser suficiente, dependendo dos resultados de uma avaliação de risco.

Os servidores destinados a serem acessados a partir de uma rede externa e insegura (como servidores da Web) devem estar localizados em uma zona desmilitarizada (ZM) do firewall para fornecer proteção adicional à rede interna.

15.1.5. Redes Públicas

Onde a informação deve ser transferida através de uma rede pública como a Internet, uma criptografia forte via TLS deve ser usada para garantir a confidencialidade dos dados transmitidos.

Servidores que serão acessados a partir de dispositivos na rede pública estarão localizados na ZM do firewall.

15.1.6. Redes sem fio

As redes sem fio devem ser protegidas usando criptografia WPA2. WEP e WPA não devem ser usados.

As redes sem fio devem ser tratadas como inseguras, mesmo se o WPA2 for usado como o método de criptografia e um firewall instalado entre a rede sem fio e a LAN principal.

Uma rede sem fio para convidados pode ser fornecida para visitantes. Isso deve ser fisicamente separado de todas as redes internas (incluindo redes sem fio internas) e também protegido usando um firewall.

Os pontos de acesso sem fio devem ser configurados para não transmitir seu SSID e não permitir conexão segura usando o WPS (Wi-Fi Protected Setup) por meio do acesso físico ao próprio ponto de acesso.

As senhas de login do administrador do ponto de acesso sem fio sempre devem ser alteradas do padrão.

15.1.7. Segurança Física

Equipamentos de rede remota serão alojados em gabinetes seguros que serão trancados em todos os momentos. Somente a equipe de suporte terá acesso à chave de cada gabinete.

O backbone e o equipamento de rede centralizado serão alojados em gabinetes ou racks com chave apropriados em uma sala de servidores segura à qual somente a equipe de suporte autorizado terá acesso (com exceção da equipe de instalações locais por questões de saúde e segurança).

Pontos de acesso sem fio localizados em áreas públicas devem ser ocultados da vista quando possível e devem ser colocados em posições em que o acesso do público seja difícil, por exemplo. dentro ou perto do teto.

Um invólucro de proteção com trava deve ser instalado onde um ponto de acesso está localizado em uma área pública desprotegida, por exemplo, em um estacionamento.

15.1.8. Acesso remoto

Onde houver um requisito para acesso remoto à rede interna, os seguintes controles serão usados:

- Uma rede virtual privada (VPN) será usada fornecendo criptografia de sessão usando SSL / TLS
- Autenticação de dois fatores no cliente, quando apropriado
- Autenticação segura usando um servidor RADIUS
- O Controle de Acesso à Rede (NAC) será usado para restringir o acesso a clientes remotos que não atendam aos requisitos mínimos. controle de vírus

O acesso remoto deve ser concedido "conforme necessário" e não para todos os usuários por padrão.

15.1.9. Detecção de Intrusão na Rede

Um Sistema de Detecção de Intrusão baseado em Rede (NIDS) deve ser instalado no perímetro da rede e em todos os pontos chave dentro da rede, e. em servidores críticos.

Para redes com requisitos de alta segurança, um Sistema de Prevenção de Intrusão (IPS) pode ser considerado, embora sua implementação deva ser abordada com cautela para evitar um alto grau de falsos positivos com a correspondente interrupção do serviço aos usuários.

15.2. Padrões de Segurança de Rede

Os seguintes padrões serão adotados com relação à configuração e segurança da rede.

15.2.1. Hardware de rede

Sempre que possível, uma única política de fornecedor será usada para hardware de rede. Uma exceção será feita quando o uso de hardware de

vários fornecedores puder aumentar o nível de segurança fornecido, por ex. em uma configuração de firewall baseada em rede dupla.

Roteamento de rede será baseado no appliance pfsense. Os switches TP-LINK Gigabit serão usados como padrão para conectividade. As portas de switch, incluindo as portas de diagnóstico, serão configuradas para serem desativadas administrativamente até serem necessárias. Os hubs não serão usados devido a suas deficiências de segurança inerentes.

O Cat 5e UTP será usado para cabeamento de rede, a menos que circunstâncias específicas (como interferência excessiva) impeçam seu uso. A topografia de rede usada será Ethernet de acordo com a família de padrões IEEE 802.3.

15.2.2. Endereçamento IP

O IPv4 será usado em redes internas. No entanto, os novos dispositivos de rede adquiridos devem suportar o IPv6 em preparação para o futuro.

O intervalo de endereços IP interno usado será 172.16.40.1 – 172.16.41.254. a atribuição e o uso de sub redes devem ser monitorados cuidadosamente.

Endereços IP e informações de rede associadas para clientes de desktop e laptop serão controlados usando o DHCP. Servidores DNS internos serão usados no controlador de domínio.

15.2.3. Protocolos de Rede

O protocolo usado em todas as redes será o TCP / IP. O UDP será usado quando apropriado, mas outros protocolos de rede da camada 4 OSI não devem ser usados.

Somente protocolos e portas necessários em um servidor específico serão habilitados por padrão para reduzir a superfície de ataque. Isto é especialmente verdadeiro para servidores dentro da DMZ do firewall.

15.3. Gerenciamento de Segurança de Rede

Uma vez que as redes tenham sido projetadas e implementadas com base em um conjunto claro de requisitos de segurança, há uma responsabilidade contínua de gerenciar e controlar o ambiente de rede seguro para proteger as informações da organização em sistemas e aplicativos. Isso deve ser alcançado por meio de controles nas seguintes áreas.

15.3.1. Funções e Responsabilidades

Papéis e responsabilidades pela gestão e controle de redes devem ser claramente definidos. A fim de proporcionar uma separação efetiva de tarefas, a operação das redes é gerenciada separadamente da operação do restante da infraestrutura, como servidores e aplicativos.

Essa segregação de funções é detalhada na tabela a seguir.

Função do gerente	Equipe	Responsabilidades Principais
Suporte de TI	Gestão de computadores, Redes e Comunicações	Design e implementação de redes novas e alteradas, Instalação e remoção de equipamentos de rede, Configuração de equipamentos de rede, Gerenciamento de incidentes de terceira linha, Monitoramento de disponibilidade de rede, Monitoramento de intrusão de rede, Gerenciamento de incidentes de segunda linha, Backups de configuração, Patch e atualizações, Configuração e gerenciamento de usuários de acesso remoto

15.3.2. Registro e Monitoramento

Os níveis de registro em dispositivos de rede devem ser configurados de acordo com a política da organização e os registros monitorados regularmente.

Os logs de firewall serão monitorados em busca de sinais de varredura excessiva de portas, o que pode ser um precursor de um ataque remoto. Onde instalado, um sistema de detecção de invasões baseado em rede deve ser configurado para alertar a equipe de operações de rede sobre essa atividade.

O monitoramento de rede para disponibilidade pode ser obtido usando uma ferramenta de gerenciamento de rede baseada em SNMP e ações de recuperação automatizadas sempre que possível.

Os alertas do sistema Network Access Control (NAC) devem ser endereçados imediatamente para garantir que os clientes que não atendem aos requisitos mínimos de segurança tenham acesso permitido apenas a um subconjunto de sistemas em quarentena na rede.

15.3.3. Mudanças na Rede

Todas as alterações nos dispositivos de rede estarão sujeitas ao processo de gerenciamento de alterações e aos métodos adequados de avaliação de riscos, planejamento e retorno estabelecidos. Os registros de configuração devem ser atualizados sempre que tais mudanças forem executadas, de modo que uma imagem atual e precisa da rede seja mantida todo o tempo.

15.3.4. Incidentes de Segurança de Rede

Os eventos de rede que são considerados incidentes de segurança devem ser registrados e gerenciados de acordo com o Procedimento de Resposta a Incidentes de Segurança da Informação.

16. Conclusão

A segurança de rede é uma pedra angular das defesas de GRUPO SAURA contra muitas das ameaças com as quais nos deparamos. Somente projetando segurança efetiva em todos os novos sistemas e redes desde o início, o controle efetivo pode ser mantido e o risco reduzido. Além disso, controles adicionais devem ser implementados, garantindo que a segregação de funções seja alcançada e que as mudanças no ambiente de rede ocorram de maneira gerenciada.

Combinado com o monitoramento atento da própria rede e das ferramentas implementadas para gerenciá-la, isso deve garantir que o número e a gravidade dos incidentes de segurança de rede sejam minimizados e que nossa exposição daqueles que ocorrem não seja tão grande quanto de outra forma poderia ter sido.

17. Introdução – Política de Mensagens Eletrônicas

As mensagens eletrônicas agora se tornaram uma ferramenta comercial necessária para a comunicação interna, e com clientes e fornecedores. No entanto, devido à sua flexibilidade e disponibilidade geral, o uso de mensagens eletrônicas traz consigo uma série de riscos significativos, e todos os usuários devem permanecer vigilantes, adotando boas práticas ao enviar e receber mensagens.

As mensagens eletrônicas abrangem e-mails e também várias formas de mensagens instantâneas, de armazenamento e encaminhamento, como mensagens de texto, aplicativos de mensagens, chats na web e recursos de mensagens nas plataformas de mídia social.

Este documento de política informa como você pode usar os recursos de mensagens eletrônicas fornecidos GRUPO SAURA, incluindo o que você deve e não deve fazer. Aplica-se a todas as utilizações destas inst3alações, independentemente do meio ou localização de acesso, e. através de dispositivos móveis ou fora do escritório.

Se você não entender as implicações desta política ou como ela pode se aplicar a você, você deve abordar seu supervisor.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas GRUPO SAURA.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de Aceitação pelo Usuário*

18. Política de Mensagens Eletrônicas

18.1. Enviando e recebendo mensagens eletrônicas

Os recursos de mensagens eletrônicas fornecidos pela organização sempre devem ser usados ao se comunicar com outras pessoas em negócios oficiais. Você não deve usar uma conta pessoal para essa finalidade. Orientações sobre o envio de informações via mensagens eletrônicas devem ser observadas em todos os momentos.

Todas as mensagens enviadas de uma conta da organização permanecem como propriedade da GRUPO SAURA e são consideradas parte do registro corporativo. Todas as mensagens da organização devem ser consideradas comunicações oficiais da organização e tratadas de acordo.

A organização mantém seu direito legal de monitorar e auditar o uso de mensagens eletrônicas por usuários para avaliar a conformidade com essa política. Isso será feito de acordo com as disposições da legislação pertinente.

A exclusão de uma mensagem de uma conta individual não significa necessariamente que ela foi permanentemente removida dos sistemas de TI da organização e que essas mensagens ainda podem estar sujeitas a auditoria e revisão.

Os usuários devem permanecer cientes de que não é possível garantir que uma mensagem será recebida ou lida por um destinatário e que as mensagens podem ser interpretadas de maneiras diferentes de acordo com a cultura, o papel e o humor predominante do indivíduo que a lê. Portanto, você deve sempre considerar se o uso de mensagens eletrônicas é um meio apropriado de transmitir as informações envolvidas e se uma alternativa como o telefone seria preferível, particularmente se a mensagem é urgente ou complexa.

Deve-se tomar cuidado ao endereçar mensagens que incluam informações importantes, para impedir a transmissão acidental a destinatários não autorizados. Cuidado com o recurso de preenchimento automático de texto e e-mail em que o sistema sugere destinatários com base nos caracteres digitados até o momento.

Os usuários devem evitar o envio de mensagens desnecessárias para listas de distribuição, particularmente aquelas com ampla circulação, como a "lista global" de todos os funcionários. Quando necessário, essas mensagens devem ser enviadas pelo departamento de comunicações da organização.

Em particular, os usuários não devem enviar mensagens que contenham material que seja difamatório, obsceno, não esteja em conformidade com a política de igualdade e diversidade da organização ou que, de outra forma, o destinatário consideraria inapropriado. Se você não tiver certeza se a mensagem pertence a essa categoria, consulte seu supervisor antes de enviá-la.

As mensagens eletrônicas da organização não devem ser usadas:

- para a distribuição de material comercial ou publicitário não solicitado ou lixo eletrônico de qualquer tipo, para outras organizações
- enviar material que infrinja os direitos autorais ou direitos de propriedade intelectual de outra pessoa ou organização
- para atividades que corrompem ou destroem os dados de outros usuários ou, de outra forma, interrompem o trabalho de outros usuários
- distribuir imagens, dados ou outros materiais ofensivos, obscenos ou indecentes
- enviar qualquer conteúdo que possa causar aborrecimento, inconveniência desnecessária
- transmitir mensagens abusivas ou ameaçadoras para outros
- transmitir material que discrimine ou incentive a discriminação com base em raça, sexo, orientação sexual, estado civil, deficiência, crenças políticas ou religiosas
- para a transmissão de material difamatório ou falsas alegações de natureza enganosa
- para atividades que violam a privacidade de outros usuários
- para enviar mensagens anônimas - ou seja, sem uma identificação clara do remetente
- para quaisquer outras atividades que tragam ou possam trazer a organização um descrédito

Se você receber mensagens indesejadas não solicitadas ou spam, é recomendável excluí-las sem lê-las. Não responda à mensagem, pois isso pode confirmar a existência de um endereço válido para o remetente, resultando em mais comunicações indesejadas.

18.2. Monitoramento de instalações de mensagens eletrônicas

O uso de mensagens eletrônicas dentro do sistema da organização é monitorado e registrado para:

- planejar e gerenciar sua capacidade de recursos de forma eficaz
- avaliar a conformidade com políticas e procedimentos
- garantir que os padrões sejam mantidos
- prevenir e detectar crimes
- investigar o uso não autorizado

O monitoramento será realizado por pessoal especificamente autorizado para esse fim. Procedimentos de monitoramento consistentes serão aplicados a todos os usuários e podem incluir a verificação do conteúdo das mensagens.

No caso de um gerente suspeitar que as facilidades de mensagens eletrônicas estão sendo abusadas por um usuário, ele deve entrar em contato com o Suporte de Ti. Todos esses relatórios serão investigados de acordo com procedimentos documentados e, quando apropriado, evidências fornecidas. Existe também um requisito para fornecer tais informações aos órgãos reguladores ou legislativos de acordo com a lei.

Os usuários não devem acessar a conta de mensagens eletrônicas de outro usuário, a menos que tenham obtido permissão do proprietário da conta ou de seu supervisor. Em tais casos, isso deve ser motivado e o acesso, apenas, para mensagens que possam ser consideradas relevantes.

18.3. Uso de e-mail

Além das declarações de política em outros tópicos deste documento, o seguinte se aplica especificamente ao uso de e-mail.

Todos os e-mails enviados dos endereços da organização para destinatários fora da organização terão automaticamente o seguinte aviso:

"Em cumprimento a Lei Geral de Proteção de Dados - LGPD (Lei nº13.709/48), esclarecemos que o conteúdo deste e-mail contém informação confidencial e encontra-se protegido por direitos de autor e/ou de propriedade intelectual. O uso da presente mensagem é restrito e exclusivo ao destinatário e remetente, sendo que nenhum assunto ou documento relacionado a esta pode ser

retransmitido para terceiros sem consentimento prévio, por escrito, do remetente. Se, por engano, receber conteúdo desta natureza, apague imediatamente e destrua todas as cópias do mesmo."

Sua caixa de correio será configurada com uma limitação de espaço. Isso, para evitar que a capacidade de armazenamento disponível seja excedida e para garantir o uso econômico do e-mail.

Você deve gerenciar sua(s) conta(s) de e-mail para permanecer dentro do limite de espaço da caixa de correio, fazendo uso do recurso de arquivamento. Se sua caixa de correio estiver cheia, entre em contato com o Suporte de Ti para obter orientação.

Quando possível, faça uso de links para arquivos em mensagens de e-mail em vez de anexar uma cópia do arquivo, especialmente se a mensagem de e-mail tiver uma distribuição ampla. Isso impedirá que as caixas de correio fiquem cheias e evitará a consequente interrupção.

Existe um limite de tamanho para todos os e-mails, que é de 20 MB. Se você precisar enviar um e-mail maior para fins comerciais, entre em contato com o Suporte de Ti para obter orientação.

Vírus de computador, adware e outros malwares são pequenos programas que podem ter um efeito negativo em seu computador e no uso da Internet, e podem expor as informações da organização a riscos extremos. Esses vírus podem ser baixados e instalados por meio de e-mails recebidos em sua caixa de entrada. A organização fornece software antivírus que é executado em todos os computadores que têm acesso à rede e destina-se a detectar qualquer vírus antes de eles terem sido instalados.

Se você acredita que pode ter um vírus ou recebeu um e-mail que pode conter um, informe ao Suporte de Ti imediatamente. Não abra anexos que você acredita que possam conter vírus.

Além disso, você não deve:

- transmitir por e-mail anexos de arquivos que você sabe que estão infectados por um vírus
- baixar dados ou programas de qualquer natureza de fontes desconhecidas
- desabilitar ou reconfigurar o sistema antivírus instalado em um computador usado para acessar os recursos de e-mail

Se um vírus de computador for deliberadamente ou acidentalmente enviado para outra organização, GRUPO SAURA poderá ser responsabilizada se a transmissão for considerada negligente.

19. Introdução – Política de Computação em Nuvem

O objetivo deste documento é definir a política da organização na área de computação em nuvem.

GRUPO SAURA faz uso extensivo de serviços de computação em nuvem em seus principais sistemas de negócios. A natureza desses serviços é tal que os dados são armazenados fora da rede interna GRUPO SAURA e estão sujeitos a acesso e gerenciamento por terceiros. Além disso, muitos serviços em nuvem são oferecidos em uma base de múltiplas concessões, na qual a infraestrutura é compartilhada entre vários clientes do Provedor de Serviços em Nuvem (PSN), tornando a segregação eficiente e segura um requisito essencial.

Portanto, é essencial que as regras sejam estabelecidas para a seleção e o gerenciamento dos serviços de computação em nuvem, de modo que os dados sejam adequadamente protegidos de acordo com seu valor comercial e classificação.

A computação em nuvem é geralmente aceita para os seguintes tipos de serviços:

Software como serviço (SaaS) - o fornecimento de um aplicativo hospedado para uso como parte de um processo de negócios. A hospedagem geralmente inclui todos os componentes de suporte para o aplicativo, como hardware, software operacional, bancos de dados etc.

Plataforma como serviço (PaaS) - hardware e software de suporte, como sistema operacional, banco de dados, plataforma de desenvolvimento, servidor da web etc., são fornecidos, mas nenhum aplicativo de negócios

Esta política se aplica ao uso de todos os tipos de serviços de computação em nuvem e é particularmente relevante quando os dados são armazenados.

20. Política

Os dados pertencentes a GRUPO SAURA serão armazenados somente nos serviços em nuvem com a permissão prévia da Diretoria.

Avaliação de risco apropriada deve ser realizada em relação ao uso proposto ou continuado de um serviço em nuvem, incluindo um entendimento completo dos controles de segurança da informação implementados pelo PSN.

As devidas diligências devem ser conduzidas antes da contratação em um provedor de serviços em nuvem para garantir que os controles apropriados sejam implementados para proteger os dados. Será dada preferência a fornecedores que sejam certificados pela norma internacional ISO/IEC 27001:2022 e que cumpram os princípios dos códigos de boas práticas ISO/IEC 27017 e ISO/IEC 27018 para serviços em nuvem.

Os contratos de serviço com provedores de serviços em nuvem devem ser revisados, compreendidos e aceitos antes de ser contratado.

Funções e responsabilidades para atividades como backups, correções, gerenciamento de log, proteção contra malware e gerenciamento de incidentes devem ser acordados e documentados antes do início do serviço em nuvem.

Os procedimentos devem ser estabelecidos para realizar atividades no ambiente de nuvem que sejam irreversíveis, por exemplo, exclusão de servidores virtuais, encerrando um serviço de nuvem ou restauração de backups. A supervisão por uma segunda pessoa adequadamente qualificada deve ser considerada.

Quando disponível, a autenticação de dois fatores deve ser usada para acessar todos os serviços na nuvem.

O log de rastreamento deve estar disponível para permitir que a GRUPO SAURA compreenda as maneiras pelas quais seus dados estão sendo acessados e para identificar se ocorreu algum acesso não autorizado.

Os dados confidenciais armazenados nos serviços em nuvem devem ser criptografados usando tecnologias e técnicas aceitáveis. Sempre que possível, as chaves de criptografia serão armazenadas pala GRUPO SAURA e não pelo fornecedor.

As políticas da GRUPO SAURA para a criação e gerenciamento de contas de usuários serão aplicadas aos serviços em nuvem.

Devem ser feitos backups de todos os dados armazenados na nuvem. Isso pode ser feito diretamente pela GRUPO SAURA ou sob contrato pelo provedor de serviços em nuvem.

Todos os dados da GRUPO SAURA devem ser removidos dos serviços de nuvem no caso de um contrato ser finalizado por qualquer motivo. Os dados não devem ser armazenados na nuvem por mais tempo do que o necessário.

21. Introdução- Procedimento de Resposta a Incidentes de Segurança da Informação

Este documento destina-se a ser usado quando ocorrer algum tipo de incidente que afeta a segurança da informação GRUPO SAURA, incluindo aqueles que potencialmente afetam os dados pessoais, para os quais a organização é uma controladora. Destina-se a garantir uma resposta rápida, eficaz e ordenada a uma violação de segurança da informação.

Os procedimentos descritos neste documento devem ser usados apenas como orientação para resposta a um incidente. A natureza exata de um incidente e seu impacto não podem ser previstos com certezas e, portanto, é importante que o bom senso seja usado ao decidir as ações a serem tomadas.

No entanto, pretende-se que as estruturas apresentadas aqui sejam úteis para permitir que as ações corretas sejam tomadas mais rapidamente e com base em informações precisas.

Os objetivos deste procedimento de resposta a incidentes são:

- fornecer uma visão geral e concisa de como GRUPO SAURA responderá a um incidente
- definir quem responderá a um incidente e suas funções e responsabilidades
- descrever as instalações que irão ajudar na gestão do incidente
- definir como as decisões serão tomadas com relação à nossa resposta a um incidente
- explicar como será a comunicação dentro da organização e com partes externas
- fornecer detalhes de contato para pessoas-chave e agências externas

Todos os membros da equipe mencionados neste documento receberão uma cópia deste, que deverá ficar disponível sempre que necessário.

Os detalhes de contato serão verificados e atualizados pelo menos três vezes por ano. As alterações do contato ou de outros detalhes relevantes que ocorrerem devem ser comunicadas o mais breve possível.

Todas as informações pessoais coletadas como parte do procedimento de resposta a incidentes e contidas neste documento serão usadas exclusivamente para fins de gerenciamento de incidentes de segurança da informação e estão sujeitas à legislação de proteção de dados.

22. Fluxograma de Resposta a Incidentes

O fluxo do procedimento de resposta a incidentes é mostrado no diagrama abaixo.

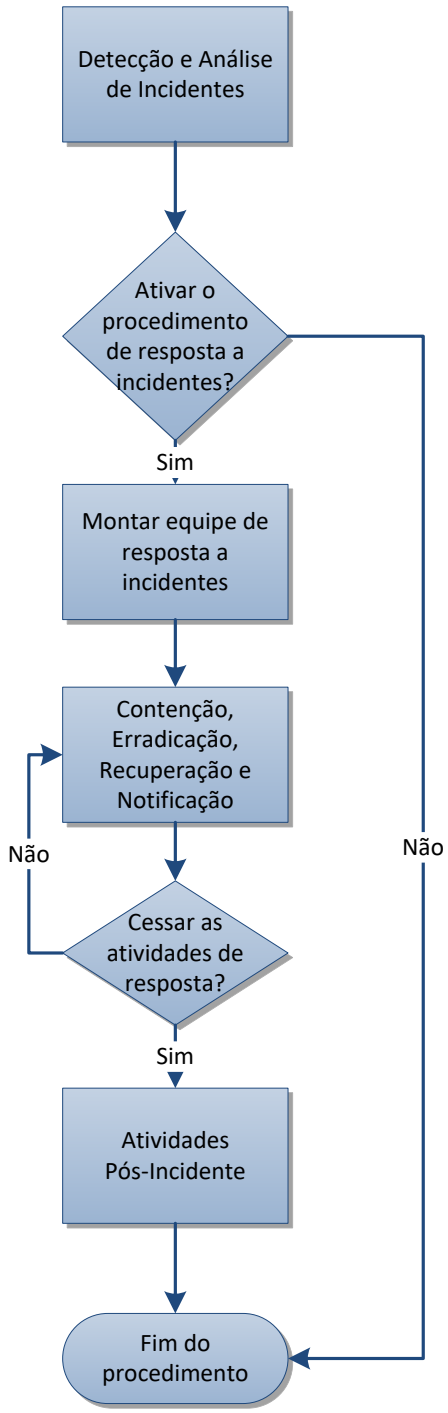

Figura 1 – Fluxograma de Resposta a Incidentes

Essas etapas são explicadas com detalhes nos próximos tópicos.

23. Identificar e Analisar o Incidentes

Um incidente pode ser identificado inicialmente de várias formas e através de várias fontes diferentes, dependendo da natureza e localização do incidente. Alguns incidentes podem ser detectados automaticamente por meio de ferramentas de software usadas GRUPO SAURA ou por funcionários que notam atividades incomuns. Outros podem ser notificados por um terceiro, como um cliente, fornecedor ou agência de aplicação da lei, que tenha conhecimento de uma violação.

É normal que haja uma demora entre a ocorrência do incidente e sua identificação real; um dos objetivos de uma abordagem proativa à segurança da informação é reduzir esse período de tempo. O fator mais importante é que o procedimento de resposta a incidentes deve ser iniciado o mais rápido possível após a identificação, para que uma resposta efetiva possa ser dada.

Uma vez que o incidente tenha sido identificado, uma avaliação de impacto inicial deve ser realizada a fim de decidir a resposta apropriada.

Esta avaliação de impacto deve medir:

- A extensão do impacto na infraestrutura de TI, incluindo computadores, redes, equipamentos e acomodações
- Os ativos de informação que podem estar em risco ou foram comprometidos
- A duração provável do incidente, ou seja, quando pode ter começado
- As unidades de negócio afetadas e a extensão do impacto para elas
- Para as violações que afetam os dados pessoais, o grau de risco para os direitos e liberdades dos titulares dos dados
- Indicação inicial da causa provável do incidente

Essas informações devem ser documentadas para que haja um entendimento claro, disponível para uso atual ou em uma revisão posterior.

Uma lista de ativos de informação, operações negociais, produtos, serviços, equipes e processos de suporte, que possam ter sido afetados pelo incidente, deve ser criada juntamente com uma avaliação da extensão do impacto.

Como resultado desta análise inicial, qualquer membro da equipe de gerenciamento tem autoridade para entrar em contato com o Líder da Equipe de Resposta a Incidentes a qualquer momento para solicitar que se inicie o Procedimento de Resposta a Incidentes.

24. Iniciar o Procedimento de Resposta a Incidentes

Uma vez notificado de um incidente, o Líder da Equipe deve decidir se a escala e o impacto real ou potencial do incidente, justificam a ativação do Procedimento de Resposta a Incidentes e a convocação da Equipe de Resposta a Incidentes.

As seguintes situações servem como diretrizes para determinar se uma resposta formal a um incidente deve ser iniciada:

- Existe uma perda real ou potencial, significativa, de informação, incluindo dados pessoais
- Há uma interrupção, significativa, real ou potencial, nas operações de negócios
- Existe um risco, significativo, para a reputação do negócio
- Qualquer outra situação que possa causar impacto significativo para a organização

Em caso de incerteza sobre ativar ou não uma resposta a um incidente, a decisão do Líder da Equipe será a final.

Se for decidido não ativar o procedimento, um plano deve ser criado para que seja oferecida uma resposta de nível inferior pelos meios normais de gerenciamento. Isso pode envolver a invocação de outros procedimentos e outras pessoas.

Se o incidente justificar a ativação do procedimento de Resposta ao Incidente, o Líder da Equipe deve ativar a equipe.

25. Equipe de Resposta ao Incidente

Uma vez tomada a decisão de ativar o procedimento de resposta a incidentes, o Líder da Equipe garantirá que todos os membros sejam informados sobre a natureza do incidente e o local apropriado para iniciar os procedimentos.

A exceção, será o membro da equipe que irá até o local do incidente para iniciar a coleta de informações para a avaliação do incidente que a equipe conduzirá.

25.1. Membros da Equipe de Resposta a Incidentes

A Equipe de Resposta a Incidentes geralmente consistirá das seguintes pessoas e funções especificadas, embora a composição exata da equipe varie de acordo com a natureza do incidente.

Função/Área de Negócio	**Principal responsável da função**
Líder do Time	Gustavo Santi
Facilitador da Equipe	Gustavo Santi
Ponto de Ligação Incidente	Gustavo Santi
Tecnologia da Informação	Gustavo Santi
Operação de Negócios	Robison Santos
Saúde e Segurança	Robison Santos
Recursos Humanos	Robison Santos
Planejamento de Continuidade de Negócios	Robison Santos
Comunicações (RP e Relações com as mídias)	Robison Santos
Jurídico e Regulatório	Robison Santos

Tabela 2 – Membros da Equipe de Resposta a Incidentes

Os detalhes de contato das pessoas da Equipe estão no *Anexo C* deste documento.

25.2. Funções e Responsabilidades

As responsabilidades das funções da equipe de resposta a incidentes são as seguintes:

Líder do Time

- Decide se deve ou não iniciar uma resposta
- Monta a equipe de resposta a incidentes
- Gerenciamento geral da equipe de resposta a incidentes
- Responsável pela comunicação com a diretoria e outras partes interessadas de alto nível
- Tomador de decisão final em casos de desacordo

Facilitador da Equipe

- Responsável pelo suporte da equipe
- Coordena os recursos com a gerência
- Prepara as reuniões e registra as ações e decisões
- Mantém os resumos e status dos procedimentos atualizados
- Facilita a comunicação via e-mail, telefone ou outros métodos
- Monitora informações externas como notícias

Ponto de Ligação Incidente

- Comparece ao local do incidente o mais rápido possível
- Avalia a extensão e o impacto do incidente
- Fornece as informações para a equipe
- Fornece atualizações e respostas as perguntas necessárias para a tomada de decisões da equipe

Tecnologia da Informação

- Fornece informações sobre questões relacionadas à tecnologia
- Auxilia na avaliação de impacto

Operação de Negócios

- Contribui para a tomada de decisões com base no conhecimento das operações, produtos e serviços da empresa.
- Relata aos outros membros da equipe sobre questões operacionais
- Ajuda a avaliar o impacto provável aos clientes da organização

Saúde e Segurança

- Avalia o risco para a vida
- Garante que as responsabilidades legais pela saúde e segurança sejam cumpridas a todos os momentos
- Contato com serviços de emergência, como polícia, bombeiros e médicos
- Considera questões locais com relação ao incidente

Recursos Humanos

- Avalia e aconselha sobre políticas de RH e questões de contrato de trabalho
- Representa os interesses dos funcionários da organização
- Aconselha sobre questões de capacidade

Planejamento de Continuidade de Negócios

- Fornecer aconselhamento sobre opções de continuidade dos negócios
- Invoca planos de continuidade dos negócios, se necessário

Comunicações (Relações pessoais e Relações com as mídias)

- Responsável por garantir que as comunicações internas sejam eficazes
- Decide o nível, frequência e conteúdo das comunicações com partes externas, como a mídia
- Define a abordagem da comunicação para manter as partes afetadas informadas, por ex. clientes, acionistas

Jurídico e Regulatório

- Aconselha sobre o que deve ser feito para garantir a conformidade com as leis e estruturas regulatórias
- Avalia as implicações legais reais e potenciais do incidente e ações subsequentes

25.3. Gestão, Monitoramento e Comunicação de Incidentes

Uma vez que uma resposta apropriada ao incidente tenha sido identificada, a equipe precisa ser capaz de gerenciar a resposta, monitorar o status do incidente e assegurar que a comunicação efetiva esteja ocorrendo em todos os níveis.

Reuniões regulares da equipe devem ser realizadas com frequência e decidida pelo líder. Uma agenda padrão para essas reuniões está prevista no *Anexo C*. O objetivo dessas reuniões é garantir o gerenciamento de incidentes de forma eficaz e que as decisões-chave sejam tomadas prontamente, com base em informações adequadas. As reuniões serão realizadas pelo *Facilitador da Equipe*.

25.4. Procedimentos de Comunicação

É vital que as comunicações efetivas sejam mantidas entre todas as partes envolvidas na resposta ao incidente.

O principal meio de comunicação durante um incidente será inicialmente pessoal ou por telefone, tanto fixo como móvel. O e-mail não deve ser usado, a menos que a permissão para isso tenha sido dada pela equipe.

As seguintes diretrizes devem ser seguidas em todas as comunicações:

- Seja calmo e evite longas conversas
- Aconselhe os membros da equipe interna sobre a necessidade de encaminhar solicitações de informações para a equipe
- Se a chamada for atendida por alguém que não seja o contato:
  - Pergunte se o contato está disponível em outro local
  - Se não puder ser localizado, deixe uma mensagem para que retorne em um determinado número
  - Não forneça detalhes do incidente
- Sempre documentar detalhes do tempo de chamada, respostas e ações

Todas as comunicações devem ser registradas de forma clara e precisa, pois registros podem ser necessários como parte de uma ação legal em uma data posterior.

25.4.1. Comunicação com Controladores de Dados Pessoais

Quando GRUPO SAURA estiver atuando como um processador de dados pessoais em nome de um ou mais controladores, existe uma obrigação segundo a Lei Geral de Proteção de Dados (LGPD) de informar cada controlador sobre a violação. Caberá então ao controlador decidir se ele precisa e tomar alguma decisão ou realizar alguma ação subsequentes.

25.4.2. Comunicação à Autoridade Fiscalizadora de Proteção de Dados

Quando GRUPO SAURA atua como um controlador, é um necessário que, caso os incidentes que atinjam dados pessoais possam resultar em risco aos direitos e liberdades dos titulares de dados, sejam reportados à autoridade fiscalizadora de proteção de dados imediatamente ou dentro de 48 horas após tomar conhecimento do incidente. O Procedimento de Notificação de Violação de Dados Pessoais da GRUPO SAURA deve ser usado para essa finalidade. No caso de a meta de 48 horas não ser cumprida, as razões para o atraso devem ser reportadas.

Os detalhes de contato para a autoridade fiscalizadora de proteção de dados estão listados no *Anexo B*.

25.4.3. Comunicação com os Titulares dos Dados Pessoais

Quando um incidente afeta dados pessoais, uma decisão deve ser tomada pelo Líder da Equipe em relação à extensão, tempo e conteúdo da comunicação com os titulares dos dados. A LGPD exige que a comunicação seja efetuada imediatamente, se a violação for suscetível de um risco elevado para os direitos e liberdades.

O Procedimento de Notificação de Violação de Dados Pessoais da GRUPO SAURA deve ser usado para essa finalidade.

25.4.4. Outra Comunicação Externa

Dependendo do incidente, pode haver uma variedade de partes externas que serão comunicadas. É importante que as informações divulgadas a terceiros sejam gerenciadas para serem oportunas e precisas.

Chamadas que não são de organismos diretamente envolvidos na resposta a incidentes devem ser passadas para o membro da equipe responsável pelas comunicações.

Pode haver um número de partes externas que, embora não estejam diretamente envolvidas no incidente, podem ser afetadas e precisam ser alertadas sobre esse fato. Estes podem incluir:

- Clientes
- Fornecedores
- Acionistas
- Órgãos reguladores

O membro da equipe de Comunicações deve fazer uma lista dessas partes interessadas e definir a mensagem que deve ser dada a elas. Uma lista de externos é fornecida no *Anexo B*.

As partes interessadas que não tenham sido alertadas pela equipe podem telefonar para obter informações sobre o incidente e os seus efeitos. Essas chamadas devem ser registradas e passadas para o membro de comunicações.

25.4.5. Comunicação com a Mídia

Em geral, a estratégia de comunicação com relação à mídia será a emissão de atualizações via alta direção. Nenhum membro da equipe deve dar uma entrevista com a mídia, a menos que isso seja autorizado pela equipe.

A comunicação preferencial com a mídia será a emissão de comunicados de imprensa. Em circunstâncias excepcionais, uma conferência de imprensa será realizada para responder a perguntas sobre o incidente e seus efeitos. É da responsabilidade do membro da equipe de Comunicações providenciar o local para fazer a ligação com a imprensa que queira participar.

Ao redigir uma declaração para a mídia, as seguintes diretrizes devem ser observadas:

- As informações pessoais devem ser protegidas em todos os momentos
- Atenha-se aos fatos e não especule sobre o incidente ou sua causa
- Garantir que o aconselhamento jurídico seja obtido antes de quaisquer declarações serem emitidas
- Tente antecipar questões que possam ser mencionadas
- Enfatize que uma resposta foi iniciada e que tudo está sendo feito

Os seguintes membros serão nomeados como porta-vozes para a organização, caso sejam necessárias mais informações, por ex. conferência de imprensa:

Nome	**Função**	**Escala de Incidentes**
Gustavo Santi	Comunicações Equipe	Baixo
Gustavo Santi	Gestor Administrativo	Médio
Robison Santos	Diretor Executivo	Alto

Tabela **C** *– Porta-vozes de Mídia*

O porta-voz mais apropriado dependerá da escala do incidente e do seu efeito aos clientes, fornecedores, público e outras partes interessadas.

26. Contenção, Erradicação, Recuperação e Notificação de Incidentes

26.1. Contenção

O primeiro passo será tentar impedir que o incidente se agrave, ou seja, contenha-o. No caso de um surto de vírus, isso pode implicar na desconexão das partes afetadas da rede; para um ataque de hackers, pode envolver a desativação de certos perfis ou portas no firewall ou até mesmo a desconexão completa da rede interna da Internet. As ações específicas a serem executadas dependerão das circunstâncias do incidente.

Nota: se for considerado provável que seja necessário coletar provas digitais que serão posteriormente usadas, devem ser tomadas precauções para garantir que tais evidências permaneçam admissíveis. Isso significa que os dados relevantes não devem ser alterados deliberadamente ou por acidente, por ex. abrindo um laptop. Recomenda-se que seja obtido um aconselhamento especializado neste momento - consulte os contatos no Anexo B.

Particularmente se houver suspeita de crime no incidente, registros precisos devem ser mantidos das ações tomadas e as evidências coletadas de acordo com as diretrizes forenses. Os princípios destas diretrizes são os seguintes:

Princípio 1 – Não altere nenhum dado. Se alguma coisa for feita que resulte na alteração dos dados do sistema, isso afetará qualquer processo judicial subsequente.

Princípio 2 – Acesse somente os dados originais em circunstâncias excepcionais. Um especialista treinado usará ferramentas para fazer uma cópia de qualquer dado armazenado na memória, seja em um disco rígido, memória ou cartão SIM de um telefone. Toda a análise terá local certo na cópia, e a original nunca deverá ser tocada, a menos que em circunstâncias excepcionais (por ex. o tempo é essencial, e obter informações para evitar um novo crime é mais importante do que manter a evidência admissível).

Princípio 3 – Sempre mantenha a trajetória da auditoria do que foi feita. As ferramentas forenses farão isso automaticamente, mas isso também se aplica às primeiras pessoas em cena. Tirar fotografias e vídeos é incentivado desde que nada tenha sido tocado.

Princípio 4 – A pessoa responsável deve assegurar que as diretrizes sejam seguidas.

Antes da chegada de um especialista, as informações básicas devem ser coletadas.

Isso pode incluir:

- Fotografias ou vídeos de mensagens ou informações relevantes
- Registros manuais escritos da cronologia do incidente
- Documentos originais, incluindo registros de quem os encontrou, onde e quando
- Detalhes de quaisquer testemunhas

Uma vez coletadas, as evidências serão mantidas em um local seguro, onde não pode ser adulterado.

A evidência pode ser necessária:

- Para análise posterior sobre a causa do incidente
- Como prova para processos judiciais criminais ou civis
- Em apoio a qualquer negociação de compensação com fornecedores de software ou serviços

Em seguida, uma ideia clara do que aconteceu precisa ser estabelecida. A extensão do incidente e as implicações devem ser averiguadas antes que qualquer tipo de ação de contenção.

Logs de auditoria podem ser examinados para determinar a sequência de eventos; deve-se tomar cuidado para que apenas cópias seguras de registros que não foram adulterados sejam usadas.

26.2. Erradicação

Ações para corrigir os danos causados pelo incidente devem passar pelo processo de gerenciamento de alterações. Essas ações devem ter como objetivo corrigir a causa atual e impedir que o incidente ocorra novamente. Quaisquer vulnerabilidades que tenham sido exploradas como parte do incidente devem ser identificadas.

Dependendo do tipo de incidente, a erradicação pode, às vezes, ser desnecessária.

26.3. Recuperação

Durante a fase de recuperação, os sistemas devem ser restaurados à sua condição anterior ao incidente, embora as ações necessárias devam ser realizadas para resolver quaisquer vulnerabilidades que foram exploradas como parte do incidente. Isso pode envolver atividades como a instalação de patches, alteração de senhas, proteção de servidores e alteração de procedimentos.

26.4. Notificação

A notificação de um incidente de segurança da informação e perda de dados resultante é um assunto delicado que deve ser tratado com cuidado e com total aprovação da gerência. A equipe decidirá, com base em pareceres jurídicos e de outros especialistas, e com uma compreensão total do impacto do incidente, a notificação necessária a ser feita.

A GRUPO SAURA sempre cumprirá integralmente os requisitos legais e regulamentares aplicáveis em relação à notificação de incidentes e avaliará cuidadosamente quaisquer ofertas a serem feitas as partes que possam ser afetadas pelo incidente.

Os registros coletados como parte da resposta a incidentes podem ser exigidos para quaisquer investigações dos órgãos reguladores e a GRUPO SAURA cooperará integralmente com tais procedimentos.

27. Atividade Pós-Incidente

O líder da equipe decidirá, com base nas informações mais recentes, o ponto em que as atividades de resposta devem cessar e a equipe deve ser desativada. Observe que a recuperação e execução de planos podem continuar além desse ponto, mas sob um controle menos formal.

Essa decisão dependerá do julgamento do líder da equipe, mas deve basear-se nos seguintes critérios:

- A situação foi totalmente resolvida ou é razoavelmente estável
- O ritmo de mudança da situação diminuiu a um ponto em que poucas decisões são necessárias
- A resposta apropriada está bem encaminhada e os planos de recuperação estão progredindo
- O grau de risco para o negócio diminuiu para um ponto aceitável
- Responsabilidades legais e regulamentares imediatas foram cumpridas

Se a recuperação do incidente estiver em andamento, o *Líder da Equipe* deve definir as próximas ações a serem tomadas. Estes podem incluir:

- Reuniões menos frequentes da equipe, por ex. semanalmente dependendo das circunstâncias
- Informar todas as partes envolvidas de que a equipe permanece
- Garantir que toda a documentação do incidente está certa
- Solicitar que todos os funcionários não envolvidos em trabalhos futuros retornem às tarefas normais

Todas as ações tomadas devem ser registradas.

Depois que a equipe for desativada, o *Líder da Equipe* apresentará um resumo a todos os membros, idealmente, dentro de 24 horas. Os registros relevantes do incidente serão examinados pela equipe para garantir que eles estejam completos e precisos.

Quaisquer comentários imediatos ou feedback da equipe serão registrados.

Uma revisão pós-incidente mais formal será realizada em um momento a ser decidido pela alta direção de acordo com a magnitude e a natureza do incidente.

ANEXO C –Contatos Internos de Resposta Inicial

A tabela a seguir deve ser usada para registrar contato inicial com membros da Equipe de Resposta ao Incidente:

Nome	Função/Área	Número do escritório	Número do celular	Data/Hora	Resultado (Contactado / Sem Resposta / Mensagem / Inacessível)
Gustavo Santi	Lider do Time		(44) 9145-4860		
Gustavo Santi	Facilitador de equipe		(44) 9145-4860		
Gustavo Santi	Ponto de Ligação Incidente				
RGK4IT	Tecnologia da informação	(44) 3032-8400	(44) 9145-4860		
Robison Santos	Operações de negócios		(44) 9910-0841		
Robison Santos	Saúde e Segurança		(44) 9910-0841		
	Recursos Humanos				
Robison Santos	Planejamento de continuidade de negócios		(44) 9910-0841		
Gustavo Santi	Comunicações (RP e Relações com os Mídias)		(44) 9145-4860		
	Jurídico e Regulatório				
ANEPS	DPO	(11) 3104-5168			

ANEXO D – Contatos Externos Úteis

A tabela a seguir mostra os detalhes de contato de terceiros que podem ser úteis dependendo da natureza do incidente:

Organização	Contato ou Link	Número de Telefone	E-mail
Autoridade de Fisalização de Proteção de Dados	https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico		ouvidoria@anpd.gov.br
Consultoria de segurança da informação	RDC&VL REPRESENTAÇÃO COMERCIAL LTDA – TEC-RDC	(11) 92005-7321	suporte@tec-rdc.com.br
Fornecedor de software de segurança	RDC&VL REPRESENTAÇÃO COMERCIAL LTDA – TEC-RDC	(11) 92005-7321	suporte@tec-rdc.com.br
Provedor de internet	VIVO Fibra e Net Combo		
Associações	Associação Nacional dos Profissionais e Empresas Promotoras de Crédito e Correspondentes no País	(11) 3104-5168 ou 0800 777 4654	ouvidoria@aneps.org.br
Órgãos Reguladores	Federação Brasileira de Bancos	11 3244 9800 ou 3186 9800	
Promotiva S.A	https://www.redepromotiva.com.br/web/site/#contato	(11) 3598-3421 ou 0800-777-6001	Promotiva-qualidade@redepromotiva.com.br

ANEXO E – Agenda de Reunião da Equipe de Resposta a Incidentes

Recomenda-se que a seguinte agenda seja usada para reuniões da Equipe de Resposta a Incidentes.

AGENDA

Participantes: Todos os membros da equipe de resposta a incidentes

Localização: Sala x

Frequência: A cada 4 horas

Presidente: Líder da Equipe

Minutos: Facilitador da Equipe

1. Ações da reunião anterior
2. Atualização do status do incidente
3. Decisões requeridas
4. Atribuição de Tarefas
5. Comunicações internas
6. Comunicações externas
7. Qualquer outra situação

TABELA A

Título da política	Áreas endereçadas	Público-alvo
Política de Computação em Nuvem	Diligências, configuração, gerenciamento e remoção de serviços de computação em nuvem.	Funcionários envolvidos na aquisição e gerenciamento de serviços em nuvem
Política de Dispositivos Móveis	Segurança de dispositivos móveis, como laptops, tablets e smartphones, fornecidos pela organização ou pelo indivíduo para uso comercial.	Usuários de dispositivos móveis fornecidos pela empresa ou próprio dispositivo do funcionário
Política de Controle de Acesso	Registro de usuário e cancelamento de registro, fornecimento de direitos de acesso, acesso externo, revisões de acesso, política de senha, responsabilidades do usuário e controle de acesso ao sistema e ao aplicativo.	Funcionários envolvidos na configuração e gerenciamento do controle de acesso
Política Criptográfica	Avaliação de risco, seleção de técnica, implantação, teste e revisão de criptografia e gerenciamento de chaves	Colaboradores envolvidos na criação e gestão do uso de tecnologia e técnicas criptográficas
Política de Segurança Física	Áreas de segurança local, segurança de papel e equipamento e gerenciamento do ciclo de vida de equipamentos	Todos os funcionários
Política Antimalware	Firewalls, antivírus, filtragem de spam, instalação e verificação de software, gerenciamento de vulnerabilidades, treinamento de conscientização do usuário, monitoramento e alertas de ameaças, revisões técnicas e gerenciamento de incidentes de malware.	Funcionários responsáveis por proteger a infraestrutura da organização contra malware

TABELA A

Título da política	Áreas endereçadas	Público-alvo
Política de Segurança de Rede	Projeto de segurança de rede, incluindo segregação de rede, segurança de perímetro, redes sem fio e acesso remoto; gerenciamento de segurança de rede, incluindo funções e responsabilidades, registro e monitoramento e alterações.	Funcionários responsáveis por projetar, implementar e gerenciar redes
Política de Mensagens Eletrônicas	Envio e recebimento de mensagens eletrônicas, monitoramento de facilidades de mensagens eletrônicas e uso de e-mail.	Usuários de facilidades de mensagens eletrônicas
Política de Retenção e Proteção de Registros	Período de retenção para tipos de registro específicos, uso de criptografia, seleção de mídia, recuperação de registros, destruição e revisão.	Empregados responsáveis pela criação e gestão de registros
Política de Proteção de Dados	Legislação, definições e requisitos de proteção de dados aplicáveis.	Funcionários responsáveis por projetar e gerenciar sistemas usando dados pessoais

Tabela A – Conjunto de documentos de política

TABELA B

Categoria da Informação	Exemplos	Quem pode ter acesso via TSPD	Tipos de dispositivos TSPD	Controles obrigatórios	Comentários
Nível 0 - Público	Catálogos de produtos, informações sobre preços, endereços de localização da empresa e números de contato	Qualquer um	Qualquer um	Nenhum	Esta informação está geralmente disponível ao público e cedida através de meios acessíveis, exemplo, um website
Nível 1 - Protegido	Procedimentos internos, detalhes do produto, comunicações internas da empresa, por exemplo e-mail não restrito ou confidencial	Funcionários e outras partes interessadas aprovadas	Portáteis	Proteção por senha do dispositivo Bloqueio inativo Limpeza remota Proteção de senha do aplicativo Auditorias Periódicas	É o uso mais provável de TSPD dentro da organização
Nível 2 - Restrito	Informações de RH, dados bancários, informações pessoais protegidas pela legislação de proteção de dados	Grupos restritos de funcionários	Tablets Smartphones	Criptografia de disco completo VPN Patch automatizado Antivírus Firewall Auditorias regulares	Essas informações só devem ser acessadas por meio de dispositivos com controles de segurança rígidos. Isso praticamente impossibilitará o uso de um dispositivo TSPD dependendo das circunstâncias

TABELA B

Categoria da Informação	Exemplos	Quem pode ter acesso via TSPD	Tipos de dispositivos TSPD	Controles obrigatórios	Comentários
Nível 3 - Confidencial	Planos de recursos da empresa, propostas comerciais, informações financeiras não publicadas	Ninguém	Apenas computadores portáteis	Não aplicável	Essas informações só devem ser acessadas por meio de dispositivos fornecidos pela organização com controles rígidos de segurança

Tabela B – Orientação TSPD