somos
natura

Guia de *Cibersegurança e Privacidade* para Fornecedores

natura

SRC natura

1. Governança de Segurança da Informação (SI)

2. Privacidade e Proteção de Dados

3. Treinamento e Conscientização

4. Identidade e Acessos

5. Monitoramento e Resposta a Incidentes

6. Riscos, Continuidade e Dispositivos

7. Proteção da Infraestrutura e Nuvem

8. Glossário

natura

Como cuidar da *segurança* da parceria com a Natura

Este documento visa orientar nossos parceiros de negócio sobre os requisitos mínimos de segurança e proteção de dados esperados para mantermos uma relação comercial segura e resiliente, garantindo que os dados da nossa empresa e os seus estejam protegidos.

natura

1. Governança de Segurança da Informação (SI)

A governança é a base de tudo. Sem regras escritas e responsabilidades definidas, a segurança se torna reativa e falha. É o "manual de instruções" da sua empresa sobre o que pode ou não fazer.

- **Políticas e Documentação:** Sua organização deve possuir uma Política de Segurança da Informação (PSI) aprovada pela diretoria. É um documento que diz como sua empresa cuida das informações. Ela deve ser revisada anualmente ou sempre que houver mudanças significativas no negócio.
- **Revisão das Documentações:** O mundo digital muda rápido. Assim como a PSI, suas Políticas e Normas devem ser revisadas no mínimo uma vez ao ano, para garantir que mudanças internas e novas tecnologias sejam contempladas nas documentações.
- **Responsabilidades:** Deixe claro quem é a pessoa responsável por decidir sobre segurança na sua empresa. Deve haver pessoas (ou um comitê) claramente responsáveis por tomar as decisões de segurança para a companhia.
- **Controle de Ativos e Uso Aceitável:** É essencial definir o que o colaborador pode ou não fazer com os equipamentos da empresa (Política de Uso Aceitável), crie uma regra sobre o que o funcionário pode ou não fazer no PC do trabalho (ex: não baixar programas piratas).
- **Classificação da Informação:** Nem todo dado é igual. Ensine a seus colaboradores a separar o que é dado "Público" (pessoas fora da empresa podem saber), do que é “Interno” (todos dentro da companhia podem saber) e "Confidencial" (somente um grupo de colaboradores específicos dentro da companhia podem saber).
- **Segurança Física e Periféricos:** Controle quem entra fisicamente no seu escritório ou fábrica. O acesso às dependências da empresa deve ser controlado. Ter uma lista de visitantes é um ótimo começo.
- **Periféricos, Pendrives e HDs Externos:** Esses tipos de mídia removível são fáceis de se perder e também são suscetíveis a se infectar com vírus. O uso deve ser restrito ou proibido para evitar vazamento de dados e entrada de malwares nos ambientes da empresa.
- **Mobilidade (BYOD):** Se os funcionários usam dispositivos pessoais (computadores, notebooks, celulares ou tablets) para o trabalho, deve haver uma política de BYOD (Bring Your Own Device) com regras de segurança mínimas, especificando por exemplo o uso de senhas, regras de segurança e requisitos.
- **Contratos e Confidencialidade:** Todos os funcionários e parceiros não devem espalhar segredos da empresa e seus parceiros de negócio, para garantir isso, podem ser incluídas cláusulas no contrato de trabalho especificando essa limitação ou disponibilizar um NDA (Non-Disclosure Agreement) com estas especificações para assinatura dos colaboradores e terceiros.

2. Privacidade e Proteção de Dados

O cumprimento da LGPD não é apenas jurídico, é operacional. Como você cuida dos dados das pessoas (nomes, CPFs, e-mails)?

- **Ciclo de Vida do Dado:** Estabeleça uma Política de Retenção e Descarte. Dados não podem ser guardados para sempre; quando a finalidade termina, o descarte deve ser seguro (trituração física ou limpeza lógica).
- **Higiene no Trabalho:** Implemente a política de "Mesa e Tela Limpa" — ao se ausentar da mesa, a tela deve ser bloqueada e documentos sensíveis guardados.
- **Encarregado (DPO):** A lei (LGPD) pede que empresas tenham alguém responsável por cuidar da privacidade. Nomeie um DPO (Data Protection Officer) para ser o ponto de contato com titulares e autoridades.

3. Treinamento e Conscientização

O elo mais fraco costuma ser o humano. Treinar é investir em prevenção.

- **Cultura de Segurança:** Não basta ter políticas se ninguém as conhece. Realize treinamentos de integração (onboarding) e reciclagens periódicas com seus funcionários.
- **Inclusão de Terceiros:** Se sua companhia subcontrata alguém para prestar serviço à Natura, esse subcontratado também precisa saber as regras de segurança e deve ser treinado.

4. Identidade e Acessos

Quem tem acesso ao quê? O controle rigoroso evita acessos indevidos e espionagem industrial.

- **Ciclo de Vida do Acesso:** O acesso a sistemas deve ser concedido com base no "menor privilégio". Revisões periódicas de acesso (ex: trimestrais, semestrais) garantem que pessoas que mudaram de função não mantenham permissões antigas.
- **Desligamento Imediato:** Em casos de rescisão contratual de um colaborador, o acesso aos sistemas (e-mail, ERPs, ferramentas, plataformas) deve ser revogado no mesmo dia, idealmente na hora da comunicação do desligamento.
- **Senhas:** "123456" ou nome da empresa são senhas fáceis de serem adivinhas. Exija senhas complexas (letras, números e símbolos) e, sempre que possível, utilize o MFA (Múltiplo Fator de Autenticação).

5. Monitoramento e Resposta a Incidentes

Não é uma questão de "se" vamos sofrer um ataque, mas de "quando".

- **Plano de Resposta:** Tenha um documento de “passo a passo” que diga exatamente quem deve ser avisado e o que deve ser feito se um ataque ocorrer. Isso minimiza o tempo de interrupção dos seus sistemas ou serviços prestados a seus clientes.

6. Riscos, Continuidade e Dispositivos

A mobilidade traz riscos de perda física e roubo. Quais são os controles para a empresa não parar se algo der errado?

- **Bloqueio Automático:** Configure notebooks para bloquearem a tela após, no máximo, 5 a 10 minutos de inatividade.
- **Instruções de Contingência:** Garanta que o colaborador saiba a quem reportar imediatamente o roubo de um notebook para que o bloqueio remoto ou a limpeza de dados seja realizada.

7. Proteção da Infraestrutura e Nuvem

A segurança técnica impede a entrada de invasores.

- **Backup (Cópia de Segurança):** É o seu seguro de vida. Tenha backups rotineiros, testados e, preferencialmente, uma cópia offline ou imutável.
- **Atualização (Patch Management):** Mantenha sistemas operacionais e softwares sempre atualizados. Sistemas "vulneráveis" são a porta de entrada nº 1 para Ransomwares.
- **Defesa de Perímetro:** Utilize Firewalls e proteções Antimalware (Antivírus) de nível corporativo em servidores e endpoints (estações de trabalho).
- **Segurança em Nuvem:** Se utilizar Cloud, aplique controles de acesso rigorosos e configurações de segurança recomendadas pelo provedor.

Glossário: Entendendo os termos

Para facilitar a nossa comunicação, traduzimos aqui os termos mais comuns que você encontrará no nosso questionário e no dia a dia da segurança:

- **Antimalware / Antivírus:** É o "segurança" digital que fica rodando no seu computador para barrar programas maldosos que tentam roubar dados ou estragar o sistema.
- **Ativos:** É tudo o que tem valor para a empresa. Pode ser físico (notebook, servidor, celular) ou digital (planilhas, banco de dados, senhas).
- **Backup:** É a famosa "cópia de segurança". Se o seu computador pifar hoje, o backup é o que garante que você não perderá o trabalho de meses.
- **BYOD (Bring Your Own Device):** Em português: "Traga seu próprio dispositivo". É quando o funcionário usa o celular ou notebook pessoal dele para acessar e-mails ou sistemas da empresa.
- **Cloud (Nuvem):** É quando você guarda arquivos ou usa sistemas que não estão no seu computador físico, mas sim em servidores acessados pela internet (como Google Drive, iCloud ou Dropbox).
- **DPO (Data Protection Officer):** Também chamado de "Encarregado de Dados". É a pessoa da sua empresa que cuida para que vocês estejam seguindo a lei de proteção de dados (LGPD).
- **Firewall:** Imagine um porteiro que fica na entrada da sua conexão de internet decidindo quem pode entrar e quem deve ser barrado. Isso é o Firewall.
- **Incidente de Segurança:** É qualquer evento estranho que coloque os dados em risco. Pode ser desde um vírus no PC até o roubo de um notebook ou um vazamento de e-mails.
- **LGPD:** Lei Geral de Proteção de Dados. É a lei brasileira que diz como as empresas devem cuidar das informações das pessoas (clientes, funcionários, etc.). Outros países da américa latina possuem legislações similares, como:
  - **México:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP);
  - **Argentina:** Ley de Protección de los Datos Personales (PDPA), [Ley 25.326];
  - **Chile:** Ley Sobre Protección de La Vida Privada [Ley 19.628];
  - **Colômbia:** Ley Estatutaria [Ley 1581 de 2012];
  - **Perú:** Ley de Protección de Datos Personales [Ley N.° 29733];
  - **Uruguai:** Ley de Protección de Datos Personales [Ley N° 18331].
- **Malware:** É o nome genérico para qualquer "programa do mal" (vírus, cavalos de troia, sistemas de sequestro de dados) criado para causar prejuízo.
- **MFA (Múltiplo Fator de Autenticação):** É aquela "camada extra" de segurança. Sabe quando você coloca a senha e o site pede um código enviado por SMS ou aplicativo? Isso é o MFA.
- **Patch (ou Atualização):** É um "remendo" que os fabricantes de software (como Microsoft ou Apple) lançam para consertar buracos de segurança que os hackers descobriram.
- **Política de Segurança:** É o conjunto de regras da casa. Um documento que diz o que é permitido e o que é proibido dentro da empresa em relação à tecnologia.
- **Rescisão Contratual:** Quando um funcionário ou prestador de serviço deixa de trabalhar para a empresa. Nesse momento, todos os acessos dele devem ser cortados.

natura