Segurança da Informação para Fornecedores

Edição: 1

Índice

1 Propósito

O principal objetivo do Manual de Segurança da Informação para Fornecedores é reduzir o número de possíveis riscos associados ao acesso a dados, sistemas de informação ou recursos da Indra por Prestadores de serviços, independentemente do tipo de trabalho prestado ou da relação que ligue o fornecedor à Indra (jurídica, baseada em contrato ou qualquer outra relação não trabalhista), visando proteger a confidencialidade, integridade e disponibilidade das informações da Indra e dos seus clientes.

A Indra reserva-se o direito de modificar esta política quando for necessário. As alterações realizadas serão divulgadas para todas as empresas prestadoras de serviços às quais sejam aplicáveis, empregando meios considerados adequados. Cabe a cada empresa fornecedora a responsabilidade de garantir que seus colaboradores leram e tomaram conhecimento das políticas de segurança mais recentes da Indra, assim como obter seu compromisso de obedecer e respeitar essas normas.

Caso qualquer uma dessas obrigações não seja cumprida, a Indra reserva-se o direito de adotar, em relação à empresa contratada, medidas de penalização consideradas apropriadas, as quais poderiam chegar à dissolução de contratos em vigor com tal empresa.

2 Princípios gerais de segurança

Sempre que necessário, os prestadores de serviços fornecerão à Indra uma lista de pessoas, sua descrição de perfil, funções e responsabilidades associados ao serviço prestado, comunicando todas as eventuais alterações realizadas referentes à relação com a Companhia (admissão, demissão, substituição ou alteração de funções ou cargos).

Os prestadores de serviços deverão garantir que todos os seus colaboradores possuem a instrução adequada e estão devidamente capacitados para executar o serviço prestado, seja especificamente em relação aos campos que correspondam às atuações associadas com a prestação de serviço ou com referência à segurança da informação.

Os prestadores de serviços deverão garantir, no mínimo, que todos os seus colaboradores associados ao serviço prestado tomaram conhecimento e se comprometem a obedecer ao descrito na presente política. A Indra poderá solicitar, em qualquer momento dado, evidências do processo de divulgação destas informações.

Os prestadores de serviços deverão permitir que a Indra realize as auditorias de segurança que lhe sejam solicitadas, colaborando com a equipe auditora e proporcionando todas as evidências e registros requeridos.

O alcance e a profundidade das auditorias serão expressamente definidos pela Indra caso por caso. As auditorias serão realizadas de acordo com o planejamento estabelecido conforme o caso com o prestador de serviço.

A Indra reserva-se o direito de realizar auditorias extraordinárias adicionais, sempre que isto esteja devidamente justificado por causas específicas.

2.1 Confidencialidade das informações

Todas as informações, documentações, programas e/ou aplicativos, métodos, organizações, estratégias de negócio e atividades relacionadas com a Indra ou com o seu negócio, aos quais os prestadores de serviços tenham acesso para poder desempenhar o serviço acordado, serão considerados informações confidenciais. Portanto, o acesso, troca e tratamento dessas informações deverão ser realizados de acordo com as finalidades previstas, descritas no contrato de prestação de serviços, observando o dever de manter segredo ao longo da prestação do serviço e depois que a relação com a Indra concluir.

Todos os recursos e informações aos quais possam ter tido acesso ou que tenham precisado ser elaborados, modificados ou copiados para desempenhar os serviços corretamente, serão devolvidos ao término da execução dos trabalhos. A Indra poderá solicitar que seja realizada a exclusão segura de dados de dispositivos com os quais as informações da Indra tenham sido acessadas.

2.2 Propriedade intelectual

Deverá ser garantida a observância das restrições legais relativas à utilização de material protegido pelas normas de propriedade intelectual. Os prestadores de serviços poderão utilizar apenas materiais da Indra expressamente autorizados para o desempenho das suas funções. É estritamente proibido utilizar programas computadorizados em sistemas de informação da Indra se não tiverem a licença correspondente.

Do mesmo modo, é proibido utilizar, reproduzir, emprestar, transformar ou divulgar publicamente qualquer tipo de criação ou invenção protegida pela Lei de Propriedade Intelectual, sem a devida autorização por escrito.

A Indra autorizará apenas a utilização de material produzido por ela mesma ou materiais autorizados ou fornecidos pelo seu titular, de acordo com os termos e condições estabelecidos e determinados nas normas em vigor.

2.3 Intercâmbio de informações

Qualquer tipo de intercâmbio de informações produzido entre a Indra e os prestadores de serviços será considerado como realizado dentro do escopo estabelecido pelo respectivo contrato de prestação de serviços, de tal forma que essas informações não poderão ser empregadas fora desse escopo ou para outras finalidades.

A distribuição de informações em formato eletrônico ou físico será realizada utilizando os recursos determinados no contrato de prestação de serviços para essa finalidade e exclusivamente para facilitação das funções associadas ao contrato em questão.

Tendo em vista o risco detectado, a Indra reserva-se o direito de implementar medidas de controle, registro e auditoria em relação a esses recursos de divulgação. Quanto ao intercâmbio de informações no escopo do contrato de prestação de serviços, serão consideradas não autorizadas as atuações a seguir:

- Transmitir ou receber material protegido por direitos autorais, violando a Lei de Proteção Intelectual.
- Transmitir ou receber qualquer tipo de material pornográfico, de natureza sexual explícita, declarações discriminatórias raciais ou qualquer outro tipo de declaração ou mensagem classificável como ofensiva ou ilegal.
- Transmitir ou receber informações sigilosas, exceto se a comunicação por via eletrônica estiver codificada e sua remessa autorizada por escrito.
- Transferir informações protegidas para terceiros não autorizados.
- Transmitir ou receber aplicativos não relacionados com o negócio.
- Participar de atividades na Internet, como grupos de notícias, jogos ou outras atividades que não estejam diretamente relacionadas com a prestação de serviços.
- Todas as atividades que possam danificar a imagem e reputação da Indra na Internet e em qualquer outro lugar estão proibidas.

2.4 Utilização inadequada de recursos corporativos da Indra

Os recursos corporativos da Indra, aos quais os prestadores de serviços tenham acesso, deverão ser utilizados exclusivamente para cumprir com as obrigações e finalidades da prestação de serviços.

Não poderão ser usados, de forma alguma para atuações não relacionadas com a finalidade do serviço ou para realizar atividades que possam ser consideradas ilícitas, como violar a propriedade intelectual de terceiros, desobedecer à norma de proteção de dados, etc.

Os prestadores de serviços se comprometem a empregar os recursos corporativos da Indra aos quais tenham acesso de acordo com a política de segurança da Indra.

A Indra poderá implementar mecanismos de monitoramento e auditoria que considerar adequados, tanto periodicamente ou quando resultar conveniente por questões específicas de segurança, para poder garantir a utilização adequada dos recursos mencionados.

Caso seja detectado que algum prestador de serviços ou seus colaboradores utilizam recursos ou informações da Indra de maneira indevida, essa circunstância será comunicada ao provedor para que tome as medidas adequadas. A Indra reserva-se o direito de tomar as medidas cabíveis de acordo com as leis de proteção dos seus direitos.

Qualquer arquivo inserido na rede da Indra ou qualquer equipamento conectado a ela através de meios automáticos, pela Internet, e-mail ou de qualquer outra forma, deverá cumprir com os requisitos estabelecidos nas presentes normas e, principalmente, aqueles referentes à propriedade intelectual, à proteção de dados pessoais e ao controle de vírus e malware.

2.5 Responsabilidades do usuário

Os prestadores de serviços deverão garantir que todos os colaboradores que possam ter acesso a dados, sistemas de informação ou recursos da Indra, no desempenho das suas funções para a Indra, deverão respeitar os princípios básicos a seguir no âmbito das suas atuações:

- Cada pessoa que tenha acesso a informações da Indra é responsável pelas atuações realizadas com seu identificador de usuário e tudo aquilo disso derivado. Portanto, é imprescindível que cada pessoa mantenha os sistemas de autenticação associados ao seu próprio identificador de usuário devidamente controlados, garantindo que o código correspondente é do conhecimento exclusivo do próprio usuário, não devendo ser divulgado, em hipótese alguma, a nenhuma outra pessoa.
- Os usuários não deverão empregar identificadores de nenhum outro usuário, mesmo que tenham a autorização do proprietário.
- Os usuários devem saber quais são e aplicar os requisitos e procedimentos existentes relativos aos dados com que trabalha.
- Qualquer usuário que tenha acesso a informações da Indra deverá escolher senhas qualificadas (de, no mínimo, 8 caracteres, contendo letras maiúsculas, minúsculas, dígitos e caracteres especiais, e que não tenham nenhum tipo de informação que possa ser descoberta com facilidade).
- Qualquer usuário que tenha acesso a informações da Indra deverá alterar as senhas predefinidas e as temporárias na primeira vez que fizer login e, no mínimo, a cada 90 dias, bem como sempre que existir a possibilidade de que outros usuários tenham tomado conhecimento da senha.
- Qualquer pessoa que tenha acesso a informações da Indra deverá tomar precauções para que os equipamentos estejam protegidos quando não estiverem sob supervisão.
- Qualquer pessoa que tenha acesso a informações deverá respeitar, no mínimo, as normas de mesa limpa descritas a seguir, visando proteger documentos em papel, meios computadorizados e dispositivos de armazenamento portáteis, e diminuir os riscos de acesso não autorizado, perda e violação de informações durante o horário normal de trabalho e fora dele (Guardar documentos em papel e meios computadorizados em compartimentos trancados com chave, bloquear as sessões de usuário ou desligar o computador quando estiver sem supervisão, proteger os locais de recebimento e remessa de informações, destruir os dados quando não forem mais necessários, etc)
- Pessoas que tenham acesso a sistemas de informação da Indra não deverão realizar, de forma alguma, testes de detecção e/ou verificação de eventuais pontos fracos ou incidentes de segurança, sem a devida autorização por escrito.
- Nenhuma pessoa que tenha acesso a sistemas de informação da Indra deverá tentar violar, de forma alguma, o sistema de segurança e as autorizações sem a devida autorização por escrito. Os usuários estão proibidos de realizar coleta de dados de tráfego de rede, exceto em caso de realização de tarefas de auditoria autorizadas por escrito.

2.6 Requisitos de segurança para dispositivos

Todos os dispositivos que tenham acesso a informações da Indra, independentemente de quem seja seu titular, deverão obedecer às políticas de segurança estabelecidas pela Indra, observando, principalmente, as seguintes condições:

- Os sistemas sempre deverão ser acessados com a devida autenticação, ou seja, empregando pelo menos o identificador pessoal e a senha correspondente.
- Todo software instalado ou conteúdo no dispositivo deve estar licenciado, dentro do ciclo de vida do produto e em um estado que esteja conforme à licença de uso.
- Os dispositivos deverão ser continuamente atualizados com a última versão de patches de segurança disponível para o software e o sistema operacional instalados.
- Os dispositivos devem possuir um sistema de proteção antimalware instalado, ativo e atualizado com a última versão disponível, tanto do programa quanto do arquivo de assinaturas.
- A proteção de tela deve estar configurada para ser ativada após 10 minutos sem atividade. O desbloqueio da proteção de tela deverá incluir a utilização de senhas, padrões de desbloqueio ou mecanismos equivalentes, que garantam que o dispositivo não poderá ser utilizado por um usuário não autorizado.

- Os dispositivos não terão nenhuma ferramenta ou arquivo que não esteja em conformidade com a política de segurança da Indra ou que possa interferir no software da companhia. Este caso inclui aqueles que procurem detectar informações diferentes daquelas pertencentes ao próprio usuário ou tentem obter acessos não autorizados, como, por exemplo, sniffers, ferramentas de varredura de redes, detecção de senhas, etc.

2.7 Comunicação de incidentes de segurança

Os prestadores de serviços se comprometem a comunicar imediatamente qualquer incidente, ponto fraco ou ameaça (observados ou suspeitados) que forem detectados nos sistemas de informação da Indra ou que possam ter afetado informações que sejam de propriedade da Indra ou de seus clientes, informando o **Departamento de Segurança da Informação** pelo endereço de e-mail csirt@indra.es do usuário genérico do Indra CSIRT ou pela pessoa responsável pelo serviço.

Em caso de colaboradores do fornecedor que trabalhem internamente na Indra, todos os incidentes, pontos fracos ou ameaças relacionados com as informações ou recursos da Indra deverão ser comunicados através do endereço de e-mail csirt@indra.es do usuário genérico do Indra CSIRT ou do Centro de Atendimento ao Usuário (CAU) da Indra.

3 Princípios específicos de segurança

3.1 Segurança física

Obrigatório para todos os prestadores de serviços que trabalhem nas instalações do próprio fornecedor.

- Os prédios e instalações devem ser sólidos fisicamente (por exemplo: no perímetro ou nas áreas, não devem existir orifícios pelos quais seja fácil abrir brechas); os muros externos das instalações devem ser de construção resistente.
- Todas as portas externas deveriam estar bem protegidas contra acessos não autorizados por meio de mecanismos de controle, como, por exemplo, barras, alarmes, fechaduras, catracas, câmeras de monitoramento, etc.
- Sempre que possível, é recomendado instalar barreiras físicas que exijam que os colaboradores sejam identificados por um método de identificação e autenticação (crachás de identificação, cartões eletrônicos, identificação biométrica, etc.), para evitar a entrada física de pessoas não autorizadas.
- Nos prédios e instalações deveriam existir sistemas automáticos de detecção e reação automática instalados em caso de condições ambientais adversas (principalmente incêndio). Quando não for possível contar com um sistema de extinção automática de incêndio, deverá haver medidas de extinção manuais instaladas que deverão ser do conhecimento de todo o pessoal da empresa.
- As condições ambientais básicas de temperatura, higiene, isolamento elétrico e sonoro, bem como outras medidas similares, devem ser estabelecidas de acordo com os requisitos específicos do equipamento de computação.
- Caso sejam mantidas cópias de informações que sejam de responsabilidade da Indra, os sistemas onde essas informações estejam hospedadas e/ou sejam processadas deverão estar situados em uma área protegida de modo específico e que inclua, no mínimo, as seguintes medidas de segurança:
    - Presença de um sistema de controle de acesso independente do da sede.
    - Existência de log de entradas realizadas.
    - Designação de acesso de pessoal externo apenas quando for necessário e com permissão, sob supervisão contínua de pessoal autorizado.
    - Pessoal externo não poderá permanecer em áreas com proteção especial nem executar trabalhos nelas sem supervisão.
    - Existência de proteção em caso de falhas de alimentação elétrica.

3.2 Segurança no desenvolvimento

Obrigatório para todos os prestadores de serviços que realizarem trabalhos de desenvolvimento e/ou testes de aplicativos para a Indra.

- Os ambientes nos quais essas atividades sejam realizadas deverão estar isolados entre eles e também dos ambientes de produção.
- Todos os acessos aos sistemas de informação que hospedarem ou processaram informações deverão estar protegidos no mínimo por um "firewall" que limite a possibilidade de conexões a eles.
- Todos os processos de desenvolvimento de software terceirizado serão controlados e supervisionados pela Indra.
- As especificações dos aplicativos deverão conter, de forma específica, os requisitos de segurança a serem observados conforme o caso.
- Os mecanismos de identificação, autenticação, controle de acesso, auditoria e integridade deverão ser incluídos em todo o ciclo de criação, desenvolvimento, implementação e operação de aplicativos.
- Os aplicativos que forem desenvolvidos deverão incluir validações dos dados de entrada que confiram que os dados estão corretos e são adequados, e que evitem a entrada de códigos executáveis.
- Os processos internos desenvolvidos pelos aplicativos deverão incluir todas as validações necessárias para garantir que as informações não estão corrompidas.
- Sempre que necessário, deverão ser incluídas funções de autenticação e controle de integridade das comunicações entre os componentes dos aplicativos.
- As informações de saída, emitidas pelos aplicativos, deverão ser limitadas, garantindo que somente são disponibilizadas aquelas que forem apropriadas e necessárias.
- O acesso ao código-fonte dos aplicativos deverá estar limitado ao pessoal que presta o serviço.
- No ambiente de testes serão empregados dados reais apenas quando tiverem sido devidamente dissociados ou sempre que for possível garantir que as medidas de segurança aplicadas são equivalentes àquelas existentes no ambiente de produção.
- Durante os testes dos aplicativos, será verificado se existem vias não controladas de vazamento de informações e se as vias predefinidas recebem apenas as informações previstas.
- O ambiente de produção receberá apenas os aplicativos que tenham sido aprovados expressamente.

3.3 Segurança dos sistemas

Obrigatório para todos os prestadores de serviços cujos serviços sejam prestados empregando sua infraestrutura de TIC.

3.3.1 Gestão de ativos

- Os prestadores de serviços deverão contar com um registro de ativos atualizado no qual seja possível conferir os ativos empregados para a prestação do serviço.
- Os prestadores de serviços deverão informar à Indra as baixas de ativos empregados para a prestação do serviço. Se esse ativo contiver outra propriedade da Indra (hardware, software ou outro tipo de ativo), essa deverá ser entregue à Indra antes do procedimento de baixa, de forma que os ativos pertencentes à companhia possam ser retirados.
- Sempre que um ativo contiver informações consideradas sigilosas, os Prestadores de serviços deverão dar baixa nos ativos garantindo que essas informações foram eliminadas de maneira segura aplicando medidas de eliminação segura ou destruindo o ativo fisicamente de tal forma que as informações que continha não possam ser recuperadas.
- Deverá haver uma pessoa responsável pelos ativos utilizados para a prestação de serviços, a qual terá que garantir que esses ativos incluem as medidas mínimas de segurança definidas pela Indra, que devem ser, pelo menos, as especificadas na presente norma:
- Observar o que está definido no item Requisitos de segurança de dispositivos.
    - Documentar os eventos mais relevantes relacionados com o seu funcionamento. Esses logs de atividades deverão estar previstos nas normas de backup do fornecedor. Deverão ser documentados principalmente todos os eventos realizados com permissões privilegiadas.
    - Os relógios dos sistemas deverão estar sincronizados entre eles e com o horário oficial.

- O prestador de serviços garantirá que a capacidade dos sistemas é gerenciada de maneira adequada, evitando paradas em potencial ou erros de funcionamento desses sistemas devido a recursos saturados.
- Erros e falhas detectados nas atividades dos sistemas deverão ser analisados, sendo adotadas as medidas necessárias para resolvê-los.

- O fornecedor definirá uma norma de backup com a qual seja possível garantir a proteção semanal de todos os dados ou informações que sejam importantes para o serviço prestado.

3.3.2 Gerenciamento da continuidade

- Os prestadores de serviços deverão ter um plano de continuidade e um plano de recuperação de TI para casos de desastre que permitam prestar o serviço mesmo nessas circunstâncias. Esse plano deverá ser desenvolvido com base em uma avaliação de riscos (pelo menos uma vez por ano) para fazer um levantamento de perigos que poderiam provocar a interrupção das operações e garantir que são colocadas em práticas as medidas apropriadas para seu gerenciamento e monitoramento.
- Os prestadores de serviços deverão testar o plano de continuidade e o plano de recuperação, para confirmar que eles servem para restaurar o serviço dentro dos prazos estabelecidos. Esses testes deverão ser feitos uma vez por ano ou logo depois que sejam realizadas alterações, aperfeiçoamentos ou modificações importantes que afetem os serviços.

3.3.3 Segurança de rede

- Todas as redes deverão ser administradas e monitoradas de modo adequado para garantir que não existem acessos não controlados ou conexões cujos riscos não sejam gerenciados conforme apropriado, estabelecendo os sistemas de monitoramento e auditoria adequados, necessários para garantir a segurança das conexões.
- Os serviços disponíveis nas redes pelas quais as informações circularem deverão ser limitados na medida do possível.
- As redes que disponibilizem acesso à infraestrutura da Indra deverão estar bem protegidas, observando as seguintes condições:
  - Ser comunicadas e autorizadas pela Unidade de Sistemas de Informação (SIs).
  - O acesso de usuários remotos à rede da Indra estará sujeito à observância de procedimentos de autenticação preliminar e validação de acesso pela SIs.
  - As conexões serão realizadas por um período de tempo limitado empregando redes privadas virtuais ou linhas específicas para essa finalidade.
  - Não serão permitidos equipamentos de comunicação nessas conexões (cartões, modems, etc.) através dos quais seja possível realizar conexões alternativas não controladas.

3.3.4 Gerenciamento de alterações

- Os prestadores de serviços deverão garantir que todas as alterações na infraestrutura de TIC, através da qual o serviço seja prestado, estejam controladas e autorizadas, certificando-se de que nenhum componente não controlado faça parte da infraestrutura de TIC.
- Será necessário verificar se todos os componentes novos incluídos na infraestrutura de TIC empregada para a prestação de serviços funcionam de maneira adequada e obedecem às finalidades para as quais foram incluídos.
- Todas as alterações realizadas deverão obedecer a um procedimento estabelecido e documentado oficialmente, garantindo que as etapas de modificação correspondentes são observadas.
- O procedimento de gerenciamento de alterações deverá garantir que o número de modificações referentes a componentes críticos é minimizado, ficando limitado àquelas estritamente obrigatórias.
- Todas as alterações realizadas em componentes críticos deverão ser verificadas para conferir se não produzem efeitos colaterais ou imprevistos no funcionamento desses componentes ou na sua segurança.
- As vulnerabilidades técnicas produzidas pelas infraestruturas empregadas para prestar os serviços deverão ser analisadas, comunicando à Indra todas aquelas que estejam associadas a componentes críticos, para que essas vulnerabilidades possam ser gerenciadas em conjunto.

Avda. de Bruselas, 35
28018 Alcobendas
Madri - Espanha
Tel. +34 91 480 50 00

indracompany.com