Requisitos de Segurança da Informação para Fornecedores

ISRS

Introdução

Os Requisitos de Segurança da Informação para Fornecedores da Ericsson (“ISRS”) representam o conjunto de requisitos mínimos de segurança da informação que o Fornecedor deve cumprir em todas as relações com a Ericsson em que o Fornecedor:

1. Processa, armazena e/ou tem acesso às Informações da Ericsson.
2. Tem acesso à rede/infraestrutura da Ericsson.
3. Desenvolve ou personaliza software para a Ericsson.
4. Fornece produtos de hardware ou software de TI, juntamente com serviços de suporte e manutenção.

O ISRS não pretende ser uma lista exaustiva de requisitos de segurança da informação. Além do ISRS, cada oferta de Serviços poderá exigir requisitos específicos , os quais serão definidos em Contrato.

Este documento passa por revisões regularmente e será atualizado de tempos em tempos.

Índice

1 Requisitos de Segurança da Informação

O Fornecedor deve demonstrar uma abordagem sistemática à gestão da segurança da informação através da adesão à última versão da norma internacional ISO/IEC 27001 ou, mediante Acordo por escrito, a uma norma equivalente.

1.1 Gestão de Segurança da Informação

a. A alta gerência do Fornecedor deve definir a direção e demonstrar comprometimento com a segurança da informação. No mínimo, deve haver uma política de segurança da informação de alto nível e um programa de apoio aplicável a toda a empresa.

b. A política de segurança da informação, nos termos da subseção a. acima, deve ser aprovada pela administração do Fornecedor, publicada e comunicada ao seu pessoal.

c. A política de segurança da informação deve ser reavaliada pelo fornecedor com uma periodicidade planejada, mas não inferior a vinte e quatro (24) meses, ou sempre que ocorram alterações significativas, de modo a garantir a sua pertinência, adequação e eficácia contínuas.

d. Deve ser designada uma ou mais pessoas qualificadas e responsáveis pela manutenção do programa de segurança da informação.

e. O Fornecedor organiza campanhas periódicas de sensibilização no domínio da segurança da informação, a fim de informar os funcionários sobre as respetivas responsabilidades na criação e manutenção de um local de trabalho seguro.

f. Sempre que for relevante, o Fornecedor deve manter a devida segregação de funções.

1.2 Gestão de Riscos

O Fornecedor deve dispor de um processo de gestão dos riscos que identifique e responda aos riscos de segurança da informação.

1.3 Segurança de recursos humanos

a. O fornecedor deve realizar verificações de antecedentes criminais para todo o seu pessoal, de acordo com as leis aplicáveis. Evidências dessas verificações devem ser mantidas e fornecidas à Ericsson (mediante solicitação da Ericsson).

b. Antes de obter acesso às informações da Ericsson, o pessoal do Fornecedor deve estar vinculado a restrições de confidencialidade sob um acordo por escrito com o Fornecedor (como um contrato de trabalho ou NDA). Tal acordo proibirá o pessoal do Fornecedor de divulgar Informações da Ericsson a terceiros e não deverá ser menos restritivo do que os compromissos de confidencialidade do Fornecedor com a Ericsson sob o Contrato.

c. O pessoal do fornecedor com acesso à infraestrutura de rede da Ericsson e/ou informações da Ericsson deve assinar o documento de Instruções de acesso e não divulgação (NDI) da Ericsson.

d. O fornecedor deve ter um processo disciplinar em vigor para lidar com violações de segurança da informação.

1.4 Gestão de ativos

a. O Fornecedor deve tratar as Informações da Ericsson como Informações Confidenciais e salvaguardá-las, cumprindo os Requisitos descritos no presente documento.

b. O Fornecedor deve registar e manter um inventário dos ativos de tecnologia da informação que façam parte do Serviço.

c. As informações da Ericsson não podem ser armazenadas, impressas, copiadas, divulgadas ou processadas pelo Fornecedor para outros fins que não o cumprimento das respectivas obrigações definidas em contrato.

d. O Fornecedor deve estabelecer processos para a devolução dos ativos da Ericsson em caso de demissão ou mudança de emprego do pessoal do Fornecedor.

e. O Fornecedor deve estabelecer e manter procedimentos para a remoção segura das informações da Ericsson, de acordo com as melhores práticas da indústria (incluindo dispositivos eletrônicos antes de serem disponibilizadas para reutilização).

f. Após a rescisão ou término do Contrato, o Fornecedor deve devolver ou destruir de forma segura, de acordo com as melhores práticas da indústria, todas as cópias das Informações da Ericsson em posse do Fornecedor, incluindo todas as cópias de segurança e de arquivo, em qualquer formato eletrônico ou não eletrônico. Mediante solicitação, o Fornecedor deve fornecer à Ericsson uma confirmação por escrito ou, quando aplicável, um certificado de destruição.

1.5 Controle de acessos

a. O acesso aos ativos da Ericsson a partir de uma rede fora do controle da Ericsson por indivíduos ou entidades que não façam parte da Ericsson só é permitido através de uma solução de acesso remoto aprovada pela Ericsson.

b. O acesso às Informações da Ericsson deve ser limitado a indivíduos específicos e em função da respectiva necessidade de tomar conhecimento(need-to-know).

c. Contas compartilhadas são estritamente proibidas. Todos os indivíduos que acessam as informações da Ericsson devem ter uma conta própria e exclusiva.

d. A autenticação multifator (MFA) deve ser implementada para todos os acessos a sistemas e redes que contenham informações da Ericsson, de acordo com as melhores práticas do setor.

e. O fornecedor deve implementar controles de seleção e gestão de senhas de acordo com as melhores práticas da indústria ao acessar as Informações da Ericsson, tais como, entre outros, a complexidade das senhas, o número máximo permitido de tentativas de início de sessão incorretas e o período de validade dassenhas.

f. O fornecedor deve ter um processo que exija aprovação para adicionar, alterar ou excluir usuários de suas redes e sistemas que processam, transmitem ou armazenam informações da Ericsson.

g. O fornecedor deve ter um processo para revogação/atualização de acesso em caso de rescisão ou mudança de emprego.

h. O fornecedor deve revisar os privilégios de acesso aos sistemas e redes que manipulam as informações da Ericsson, incluindo privilégios de acesso administrativo. As revisões periódicas devem ser realizadas pelo menos a cada doze (12) meses e, para usuários privilegiados, pelo menos a cada três (3) meses.

i. O fornecedor deve ter um processo para administrar e gerenciar contas privilegiadas.

j. Os registros devem ser mantidos de forma auditável, mostrando quais informações da Ericsson foram acessadas, modificadas, divulgadas ou descartadas.

1.6 Criptografia

a. Os controles criptográficos devem ser implementados em conformidade a todos os acordos, legislações e regulamentos relevantes.

b. O fornecedor deve ser capaz de comunicar-se de forma segura com a Ericsson através de correio eletrónico encriptado, utilizando técnicas de encriptação conformes às melhores práticas da indústria.

c. As Informações da Ericsson devem ser protegidas utilizando técnicas de encriptação em trânsito e em repouso, em conformidade com as melhores práticas da indústria.

d. As chaves criptográficas devem ser geridas a nível central, com processos em vigor relativos à geração, renovação, acesso, distribuição, armazenamento, arquivo, revogação e destruição das chaves, em conformidade com as melhores práticas da indústria.

e. Certificados raiz não devem ser usados em um ambiente operacional.

1.7 Segurança física e ambiental

a. O Fornecedor deverá restringir o acesso físico às instalações e aos centros de dados onde as Informações da Ericsson sejam processadas ou armazenadas a indivíduos específicos e em função da respetiva necessidade de tomar conhecimento.

b. As instalações de processamento de dados onde as informações da Ericsson são processadas devem ser monitoradas e ter acesso controlado o tempo todo (24 horas por dia, 7 dias por semana).

c. O Fornecedor deve proteger as Instalações de Processamento de Dados onde as Informações da Ericsson são processadas contra ameaças e riscos externos e ambientais.

d. Uma política de mesa e tela limpas deve ser aplicada para proteger as informações e os ativos da Ericsson.

e. O acesso físico aos locais onde os Serviços são prestados para a Ericsson deve ser restrito, usando cartões individuais de proximidade ou outro sistema equivalente.

f. O acesso físico aos locais onde os Serviços são realizados para a Ericsson deve registrar continuamente eventos relacionados ao acesso físico, como data, hora, ID do cartão de proximidade/passagem, ID da porta, acesso negado ou acesso concedido.

1.8 Segurança das operações

a. Os sistemas do fornecedor devem ser provisionados com capacidade suficiente para garantir disponibilidade contínua em caso de incidente de segurança ou aumento de demanda.

b. O fornecedor deve garantir que a proteção contra software malicioso seja implantada em seus sistemas e mantida atualizada, de acordo com as Melhores Práticas do Setor.

c. Todas as ações de usuários privilegiados devem ser registradas. Quaisquer alterações a estes registos por parte de um sistema, de um usuário privilegiado ou de um usuário final devem ser identificáveis. Os registros de log também devem ser revisados periodicamente de forma independente.

d. As informações sobre eventos importantes relacionados com a segurança devem ser registadas nos logs, incluindo tipos de eventos como falhas no início de sessão, falhas do sistema, alterações nos direitos de acesso e atributos de eventos como data, hora, ID do usuário, nome do arquivo, tipo de atividade do usuário e endereço IP.

e. Os registros de log devem ser armazenados criptografados por pelo menos seis (6) meses e disponibilizados à Ericsson mediante solicitação.

f. Os backups devem ser realizados e mantidos para garantir a continuidade e as expectativas de entrega conforme o Contrato.

g. Um processo de gerenciamento de vulnerabilidades deve estar em vigor para priorizar e corrigir vulnerabilidades com base na natureza/gravidade da vulnerabilidade.

h. Um processo de gerenciamento de patches deve estar em vigor para garantir que os patches sejam aplicados em tempo hábil.

i. O fornecedor deve realizar testes de penetração de sistemas e infraestrutura usados para suporte à Ericsson pelo menos uma vez por ano, usando as melhores práticas do setor.

j. O fornecedor deve sincronizar os relógios de todos os sistemas de processamento de dados relevantes com uma única fonte de referência de tempo.

k. Para reduzir a vulnerabilidade aos ataques, deve ser aplicado a todos os sistemas uma configuração forte (hardening) que siga as melhores práticas atuais da indústria.

l. O Fornecedor implementará políticas concebidas para impedir o armazenamento de Informações da Ericsson em dispositivos portáteis sem autorização prévia por escrito da Ericsson.

m. O Fornecedor deve garantir que as Informações e aplicações e sistemas da Ericsson são segregados dos sistemas e dados do próprio fornecedor ou de outros clientes, através de meios físicos, técnicos e/ou lógicos adequados.

n. Os ambientes de desenvolvimento, teste e produção que contenham Informações da Ericsson deverão estar lógica e fisicamente separados uns dos outros.

o. O Fornecedor não deve usar as Informações da Ericsson em nenhuma inteligência artificial, a menos que esta possibilidade esteja especificamente prevista no Contrato.

1.9 Segurança das comunicações

a. Os sistemas que contenham Informações da Ericsson devem ser reforçados de acordo com as melhores práticas da indústria, incluindoa remoção ou desativação de software e funcionalidades que não estejam sendo utilizados.

b. O Fornecedor deve implementar uma abordagem de segurança estratificada, utilizando firewalls, sistemas de detecção e prevenção de intrusões, segmentação de rede e outras medidas relevantes, de acordo com as melhores práticas da indústria.

c. O Fornecedor deve implementar uma solução de segurança de e-mail de acordo com as melhores práticas da indústria para proteger o correio eletrônico contra ataques maliciosos, como malware, spoofing, ataques de phishing e spam.

1.10 Relações com subcontratados

a. A divulgação de Informações da Ericsson a um subcontratante só será permitida com o consentimento prévio por escrito da Ericsson e apenas para efeitos de cumprimento das obrigações do Fornecedor estabelecidas em Contrato.

b. O subcontratante deve limitar-se apenas ao acesso, utilização, retenção e à divulgação das Informações da Ericsson necessárias ao cumprimento das obrigações contratuais.

c. O fornecedor é responsável por repassar as mesmas obrigações encontradas aqui por meio de acordo escrito aos seus subcontratados.

d. O Fornecedor deve avaliar o risco associado aos novos subcontratantes antes de os integrar e deve dispor de um processo de gestão do risco associado a terceiros.

e. O fornecedor deve monitorar, revisar e auditar regularmente a conformidade do subcontratado com o ISR.

1.11 Gestão de incidentes

a. O fornecedor deve ter um processo documentado de gerenciamento de incidentes de segurança para detectar e lidar com incidentes.

b. O fornecedor deve notificar a Ericsson imediatamente após tomar conhecimento de um incidente que afete as informações da Ericsson. Tal notificação deverá ser feita, no máximo, no prazo de vinte e quatro (24) horas ou conforme acordado a partir do conhecimento de qualquer incidente ocorrido ou suspeito para:

   i. o contato da Ericsson estabelecido no Contrato; e

   ii. gs.sim.dispatch@ericsson.com

c. Todas as notificações de incidentes relacionados com a segurança devem ser tratadas como informações confidenciais e encriptadas, utilizando os métodos de encriptação recomendados pela indústria.

d. O fornecedor deve cooperar totalmente com a Ericsson ao lidar com esses relatórios. A cooperação pode incluir o fornecimento de acesso a dados de evidências baseados em computador para avaliação forense.

e. O Fornecedor deverá cooperar com a Ericsson para garantir que medidas e procedimentos de segurança apropriados e mutuamente aceitáveis sejam implementados como parte de ações de remediação contra um incidente de segurança ou fraqueza que afete os Serviços ou envolva Informações da Ericsson.

1.12 Gestão de Continuidade de Negócios

a. O fornecedor deve implementar planos de continuidade de negócios e recuperação de desastres que sejam documentados e testados pelo menos uma vez por ano e, mediante solicitação da Ericsson, fornecer cópias.

b. O fornecedor deve garantir que os requisitos de segurança da informação e ICT sejam incorporados aos planos de continuidade de negócios e recuperação de desastres.

c. A pedido da Ericsson, o Fornecedor deve contribuir para as atividades mútuas de manutenção da atividade empresarial e de recuperação de desastres, de acordo com a designação da Ericsson.

1.13 Aquisição, desenvolvimento e manutenção de sistemas

Os seguintes requisitos de segurança das informações são aplicáveis aos Fornecedores que prestem serviços de desenvolvimento ou adaptação de software ou hardware, incluindo o processamento de Informações da Ericsson.

a. O fornecedor deve ter uma metodologia documentada de ciclo de vida de desenvolvimento de software (SDLC).

b. O código-fonte/objeto do sistema deve ser protegido contra acesso não autorizado. Os privilégios de acesso ao repositório de código-fonte devem ser revisados periodicamente e limitados a funcionários autorizados.

c. As informações de um sistema de produção não devem ser usadas em sistemas de teste e desenvolvimento.

d. O fornecedor deve garantir que o software e/ou outros produtos que processam as informações da Ericsson estejam livres de todas as vulnerabilidades de segurança conhecidas ou outros defeitos de segurança.

e. Mediante solicitação da Ericsson, o Fornecedor deve divulgar qualquer software/plug-in de terceiros (proprietário ou de código aberto) usado no desenvolvimento do software que dá suporte ao processamento de Informações da Ericsson.

f. O fornecedor deve seguir procedimentos documentados de gerenciamento de mudanças para solicitar, testar e aprovar mudanças relacionadas a aplicativos e infraestrutura.

1.14 Segurança da cadeia de suprimentos de software

O Fornecedor deve especificar e documentar os componentes de software de terceiros utilizados e os respectivos números de versão, tanto os componentes de código aberto como os exclusivos, e fornecer à Ericsson uma nomenclatura do software (SBOM) que esteja em conformidade com a Especificação SPDX°V2.2.1/ISO 5962:2021 e com a especificação SBOM destinada aos fornecedores (consulte *Condições e Diretrizes – Fornecedores e Parceiros – Ericsson)* relativamente a todo o software (fornecido de forma autônoma ou integrado no hardware) entregue ou disponibilizado à Ericsson.

2 Conformidade

a. Auditorias e/ou avaliações internas do fornecedor relativas à segurança da informação devem ser realizadas regularmente por pessoal treinado do fornecedor ou por um terceiro designado pelo fornecedor, e quaisquer descobertas devem ser corrigidas imediatamente.

b. Mediante solicitação da Ericsson, o Fornecedor deverá, no prazo de dez (10) dias, demonstrar conformidade com o ISRS e quaisquer outros requisitos de segurança da informação acordados com a Ericsson. Qualquer não conformidade identificada deve ser corrigida imediatamente, sem custo adicional para a Ericsson.

c. O Fornecedor deverá, a pedido da Ericsson, fornecer à Ericsson evidências sobre a conformidade do subcontratado com estes requisitos.

d. Mediante solicitação da Ericsson, o Fornecedor deve fornecer à Ericsson todos e quaisquer resultados de testes de penetração e/ou vulnerabilidade ou permitir que a Ericsson realize testes de penetração e/ou vulnerabilidade em sistemas ou ambientes gerenciados ou hospedados pelo Fornecedor onde as Informações da Ericsson são processadas ou armazenadas.

e. O Fornecedor deve reter e proteger todos os registros necessários para demonstrar conformidade com os requisitos.

3 Definições

Para os propósitos deste documento, as seguintes palavras e expressões devem ter o significado atribuído a elas abaixo, a menos que o contexto obviamente exija o contrário.

Contrato	O acordo entre o Fornecedor e a Ericsson, nos termos do qual a Ericsson irá adquirir, licenciar ou alugar produtos (incluindo software e outros produtos protegidos por IPR), serviços ou outros produtos do Fornecedor, aos quais os presentes Requisitos se aplicam.
Verificação de Antecedentes	As verificações de antecedentes terão o mesmo significado estabelecido na ISO/IEC 27001/27002.
Informações da Ericsson	Informações de propriedade da Ericsson, dos clientes da Ericsson, de outros terceiros que tenham relações comerciais com a Ericsson e outras informações que fazem parte do Serviço. As informações da Ericsson incluem Informações Pessoais.
Melhores práticas da indústria	Significa o grau de habilidade, cuidado, previsão e prática operacional que seria razoável e normalmente esperado de um fornecedor de serviços qualificado e competente envolvido no mesmo tipo de empreendimento que o do destinatário ou de quaisquer contratantes (conforme aplicável) nas mesmas circunstâncias ou circunstâncias semelhantes.
Instalações de Processamento de Dados	Qualquer localização física que abrigue sistemas que tratem ou armazenem Informações da Ericsson.
Informações pessoais	Por Informações Pessoais entende-se qualquer informação que possa ser associada a uma pessoa singular identificada ou identificável (“titular dos dados”), ou definida de outra forma por lei, regulamento ou acordo contratual. Uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador on-line ou a um ou mais fatores específicos de sua identidade física, fisiológica, mental, econômica, cultural ou social.
Serviço	Quaisquer serviços, produtos ou outros bens fornecidos pelo Fornecedor à Ericsson definidos em Contrato.

Fonte de tempo de referência única	Fonte do servidor de tempo que está diretamente vinculada a uma fonte confiável de UTC (Tempo Universal Coordenado), que é o principal padrão de tempo usado globalmente para regular relógios e tempo, ou seja, Stratum1.
Fornecedor	A empresa que celebrou o Contrato com a Ericsson e fornecerá os Serviços. Sempre que o termo "Fornecedor" imponha uma obrigação ou requisito ao Fornecedor de acordo com o presente documento, o termo incluirá também as filiais, subcontratantes e Pessoal do Fornecedor.