Requisitos de seguridad para proveedores de Alludo

Contenido

Introducción

Este documento describe las prácticas de seguridad de datos, continuidad empresarial y privacidad de las empresas del grupo Alludo (colectivamente "Alludo"), así como el programa para evaluar las medidas de seguridad y continuidad de los proveedores de Alludo. Los procesos, procedimientos, requisitos y obligaciones mencionados en este documento se denominan colectivamente "Estándares de Alludo".

Este **Documento de requisitos de seguridad para proveedores** informa a aquellos proveedores que ofrezcan bienes y servicios ("Proveedores") acerca de las expectativas de seguridad, continuidad empresarial y privacidad de las que Alludo los hace responsables a la hora de proporcionar servicios. Los proveedores deben implementar estos requisitos siguiendo las mejores prácticas del sector y sus políticas de seguridad corporativas. Alludo no será responsable de ningún problema al que se

enfrenten los proveedores, como la pérdida de datos o los daños del equipo, independientemente de la causa.

Si existiese alguna incoherencia entre este documento y un contrato escrito, prevalecerán las condiciones del contrato escrito. Los proveedores también deberán cumplir los requisitos normativos locales, nacionales y regionales. Si se produjese un conflicto entre este documento y la normativa aplicable, los proveedores deberán notificar a Alludo y sugerir controles alternativos para mantener estándares de seguridad, continuidad y privacidad equivalentes.

Descripción de los requisitos de seguridad para proveedores

Alludo tiene la responsabilidad de proteger su información restringida y confidencial del acceso o la divulgación no autorizados. A este efecto, Alludo aplica los estándares de Alludo: estándares internos de seguridad de datos, continuidad empresarial y privacidad para garantizar la protección de esa información restringida y confidencial y la disponibilidad continua de los servicios proporcionados por Alludo. Para garantizar el cumplimiento por parte de Alludo de los estándares internos y los requisitos normativos en lo que respecta a la seguridad de datos y continuidad empresarial, Alludo requiere que sus proveedores cumplan los estándares de Alludo descritos en este documento.

A su vez, si un proveedor delega o subcontrata cualquier parte de sus obligaciones bajo su contrato con Alludo o si contrata a otro proveedor para que proporcione servicios de manera directa o indirecta a Alludo, el proveedor requerirá que ese segundo proveedor implemente y administre un programa y plan de protección de datos que cumpla con los estándares de Alludo. Alludo se compromete a trabajar de manera razonable con sus proveedores para ayudar al proveedor a cumplir los requisitos normativos relacionados con los estándares de Alludo. El grado de aplicación de tales estándares de Alludo a un proveedor específico variará en función de tipo de servicios y productos que proporcione ese proveedor a Alludo.

Identidad y control de acceso

El proveedor garantizará que:

1. **Control de acceso y gestión de usuarios:**
   - 1.1. Existe una política de control de acceso documentada que se revisa como mínimo una vez al año.
   - 1.2. Están definidos y documentados las funciones, los permisos y los derechos de acceso de los usuarios.
   - 1.3. Existen procesos estándar de iniciación y cese de los usuarios, incluido el registro de las aprobaciones pertinentes.
   - 1.4. Se concede acceso a los componentes de la infraestructura de TI en función del principio del menor privilegio y se gestiona mediante herramientas de administración de identidades (p. ej., Active Directory, OKTA o similar).

1.5. El acceso individual a los sistemas, recursos de red y otros recursos de TI está aprobado y controlado formalmente a través de identificadores de usuario únicos y contraseñas individuales.
1.6. Se mantiene la segregación de las obligaciones al crear o modificar los identificadores de usuario y al asignar privilegios.

2. Políticas de contraseñas y autenticación:

2.1. Los usuarios deben cambiar su contraseña al iniciar sesión por primera vez.
2.2. Las contraseñas cumplen los requisitos estándares del sector, como la longitud, la complejidad, el historial de contraseñas, los intentos fallidos, la duración del bloqueo de la cuenta, la antigüedad de la contraseña y el cambio de contraseña en el primer inicio de sesión.
2.3. Se usan mecanismos seguros para enviar contraseñas de usuario y validar las identidades de usuario antes de iniciar restablecimientos de contraseña.
2.4. Los sistemas que no admiten la autenticación de IdP o que deben crearse para ser independientes están configurados para aplicar autenticación fuerte, no inferior a la configuración definida en las políticas centrales de contraseñas y control de acceso.
2.5. Todos los sistemas y aplicaciones están configurados para usar procedimientos de inicio de sesión seguros a través de mecanismos aprobados de gestión de acceso e identidades.
2.6. Los sistemas y aplicaciones están configurados para tiempo de espera de inactividad de la sesión con el fin de evitar el acceso no autorizado.

3. Gestión de acceso privilegiado:

3.1. El acceso privilegiado a los recursos está restringido a funciones de usuario definidas y aprobado por personal autorizado.
3.2. Las cuentas de usuario privilegiadas están configuradas para usar autenticación multifactor.
3.3. Los privilegios que ya no son necesarios se revocan de inmediato.
3.4. El uso de credenciales administrativas está restringido a circunstancias limitadas, como la solución de problemas, y los usuarios llevan a cabo operaciones diarias con las credenciales menos privilegiadas.
3.5. El acceso a la infraestructura crítica de TI, los sistemas, los dispositivos de red y las aplicaciones (p. ej., el acceso remoto, los servidores esenciales, los dispositivos de red) está protegida mediante autenticación multifactor.

4. Revisión y supervisión del acceso:

4.1. Se llevan a cabo revisiones periódicas de los derechos de acceso y las excepciones identificadas se tratan rápidamente.
4.2. Se realiza una reconciliación de todos los identificadores de usuario (incluido el dominio, las aplicaciones, los dispositivos de red, los sistemas de TI, el middleware, las bases de datos, etc.) con una frecuencia máxima anual, con acciones correctivas inmediatas aplicadas a cualquier discrepancia identificada.

5. Gestión de terceros y proveedores:

5.1. El acceso de proveedores externos a las redes y sistemas está controlado estrictamente, en función de la necesidad y la aprobación formal.

5.2. Las credenciales predeterminadas suministradas por el proveedor se cambian antes de que se pongan en marca los sistemas, las aplicaciones, los dispositivos de red y otros dispositivos de la infraestructura de TI.

6. **Consideraciones de acceso especiales:**
   6.1. No se usan identificadores genéricos ni compartidos, a menos que estén justificados y aprobados formalmente por la dirección, con mecanismos para realizar el seguimiento del uso y asignar acciones a usuarios individuales.
   6.2. Todo acceso administrativo no realizado a través de la consola está cifrado mediante algoritmos de cifrado aprobados por el sector y se prohíbe el acceso administrativo no realizado a través de la consola a los protocolos no seguros (p. ej., telnet, ftp).

Administración de activos

El proveedor garantizará que:

7. **Administración e inventario de activos:**
   7.1. Se mantienen inventarios completos de activos, que incluyen detalles esenciales como la información, los datos de contacto y la ubicación de los propietarios de activos.
   7.2. Los registros de activos de tecnología de la información, como hardware, sistemas operativos, aplicaciones y bases de datos, se actualizan y revisan con regularidad para garantizar la precisión.
   7.3. Se establecen y mantienen los controles de configuración y los procedimientos de administración de activos para gestionar la disponibilidad de activos esenciales y las configuraciones de sistemas de red e información vitales.

8. **Clasificación y etiquetado de la información:**
   8.1. Se mantiene una política de clasificación de la información con procedimientos y directivas complementarios. Todos los activos se etiquetan siguiendo las instrucciones establecidas y la información se clasifica y protege en función de niveles de clasificación definidos.

9. **Gestión de activos:**
   9.1. Se mantienen y comunican a todos los empleados y contratistas aplicables directivas de administración de activos para su gestión adecuada.
   9.2. Existen procedimientos documentados para proteger activos de información, identificar activos que se deben eliminar y garantizar la eliminación segura de tales activos.
   9.3. Están establecidos procesos para garantizar que los activos asignados se devuelven enseguida al equipo de administración de activos correspondiente tras la finalización o cese de empleo, contrato o acuerdo.

10. **Administración de dispositivos móviles y medios extraíbles:**
    10.1. Están implementados políticas y procedimientos para controlar dispositivos móviles (incluidos aquellos aportados por los empleados) utilizados para almacenar, transmitir o

procesar información empresarial. Son necesarias medidas de protección adecuadas para poder permitir a los dispositivos móviles acceder a información y recursos empresariales.

10.2. El uso de dispositivos de almacenamiento masivo extraíbles debe estar cifrado para garantizar la seguridad de los datos.

11. Cumplimiento de software:

11.1. Está prohibido el uso de software sin licencia o no aprobado. Existen procesos para identificar cualquier infracción y tomar los pasos necesarios para solucionarlas.

Operaciones de TI

El proveedor garantizará que:

12. Operaciones críticas del sistema:

12.1. Están establecidos y mantenidos procedimientos para utilizar redes y sistemas de información críticos. Estos incluyen:

12.1.1. Procedimientos de aprobación formales para el acceso a activos de TI.

12.1.2. Mecanismos de autenticación robustos para todas las tecnologías (p. ej., VPN, inicio de sesión de Windows).

12.1.3. Revisión regular de los derechos a privilegios.

12.1.4. Identificación de ubicaciones de red para las tecnologías esenciales en función de los requisitos de continuidad empresarial.

13. Gestión de cambios:

13.1. Está implementado un proceso completo de gestión de cambios para sistemas de TI, aplicaciones, bases de datos y componentes de red, lo que garantiza:

13.1.1. Registro, revisión, prueba y aprobación formal de todos los cambios.

13.1.2. Planes de reversión para modificaciones potencialmente disruptivas.

14. Otros:

14.1. Los sistemas y los componentes de red que manejan información privada y confidencial están sujetos a comprobaciones de supervisión de la integridad de los archivos.

14.2. Todos los sistemas y componentes de red están configurados para usar fuentes autorizadas NTP (Network Time Protocol) para una sincronización de hora precisa.

14.3. Están establecidos procesos de mantenimiento proactivos y preventivos regulares para todos los sistemas, aplicaciones, dispositivos de red y máquinas de usuario final esenciales.

14.4. Los conjuntos de reglas de firewall y de router se revisan periódicamente o siguiendo los estándares del sector, con las reglas innecesarias o no autorizadas eliminadas de inmediato.

14.5. Se implementan controles para mantener la integridad de la información y el software en todo el entorno de TI.

Seguridad de recursos humanos

El proveedor garantizará que:

15. **Comprobaciones de antecedentes:**
    15.1. Se establecen y mantienen políticas y procedimientos para llevar a cabo comprobaciones de antecedentes.
    15.2. Se realizan comprobaciones de antecedentes apropiadas de empleados y contratistas antes de la iniciación, hasta donde lo permita la Ley, en función de sus obligaciones y responsabilidades.
16. **Gestión de cambios de personal:**
    16.1. Se implementa un proceso para gestionar los cambios de personal o de sus funciones y responsabilidades, como la educación y formación de nuevos empleados en las políticas y procedimientos pertinentes.
    16.2. Se revocan derechos de acceso, distintivos, equipo y otros recursos rápidamente tras los cambios de personal cuando ya no son necesarios o no están permitidos.
17. **Aplicación de políticas:**
    17.1. Se implementa y respeta un proceso disciplinario claro para empleados que incumplen las políticas de seguridad.
    17.2. Se garantiza la responsabilidad por infracciones de políticas de seguridad a través de medidas contractuales adecuadas. Esto incluye la incorporación de cláusulas pertinentes en los contratos de trabajo del personal y contratos de servicios para contratistas externos.

Formación en seguridad y privacidad

El proveedor garantizará que:

18. La formación en seguridad y privacidad es obligatoria para todos los empleados y contratistas. Esta formación deberá completarse con la contratación inicial y anualmente o con menos frecuencia a partir de entonces.
19. Los empleados y contratistas con responsabilidades de seguridad de TI importantes se someten a formación anual especializada y adaptada a sus obligaciones y funciones de seguridad específicas.
20. La dirección tiene acceso a herramientas y sistemas que les permiten supervisar y seguir el proceso de formación de sus empleados y contratistas.
21. El programa de formación y concienciación de la organización se somete a revisión y actualizaciones periódicas. Este proceso tiene en cuenta los requisitos empresariales cambiantes, los cambios de la legislación y las lecciones aprendidas de incidentes de seguridad anteriores.

Seguridad y gobernanza de la información

El proveedor garantizará que:

22. **Gobernanza y marco de trabajo de seguridad:**

22.1. El proveedor debe implementar un marco de trabajo de seguridad reconocido (p. ej., NIST CSF, RMF, 800-53, ISO 27001, CIS) para la gobernanza de ciberseguridad e información. Este marco de trabajo debería incluir:
  22.1.1. Políticas y procedimientos completos de ciberseguridad e información, sujeto a revisión anual, aprobación formal y comunicación a toda la organización.
  22.1.2. Una estrategia de seguridad de la información bien definida y alineada con los objetivos empresariales.
  22.1.3. Procesos robustos de gobernanza y gestión de riesgos dirigidos específicamente a los riesgos de ciberseguridad e información.
  22.1.4. Mecanismos de cumplimiento para satisfacer requisitos legales y normativos relativos a la información y la ciberseguridad.
22.2. Si no acata un marco de trabajo de seguridad reconocido, el proveedor debe enviar un informe que demuestre que su entorno ha superado una auditoría.
  22.2.1. Deberá acordarse entre el proveedor y Alludo un plan de remedio para problemas identificados, incluidos los plazos de tiempo esperados.

23. Estructura de la directiva y la organización:

23.1. Están definidas e implementadas en toda la organización funciones y responsabilidades apropiadas para la seguridad de la información y la ciberseguridad.

24. Gestión y evaluación de riesgos:

24.1. Existe un marco de trabajo formal de gestión de riesgos aprobado por la dirección para:
  24.1.1. Identificar amenazas tanto internas como externas.
  24.1.2. Evaluar el nivel de confidencialidad de la información/datos aplicables.
  24.1.3. Evaluar los impactos empresariales potenciales.
  24.1.4. Evaluar las amenazas, vulnerabilidades y riesgos correspondientes.
    24.1.4.1. Se priorizan todos los riesgos y amenazas identificados y se toman los pasos necesarios para mitigar los riesgos a tiempo.
    24.1.4.2. Se implementan procesos o herramientas para identificar eventos que ocasionan interrupciones en los objetivos empresariales clave de la organización.
    24.1.4.3. El proveedor debe notificar a Alludo inmediatamente si no puede remediar o reducir cualquier riesgo material que podría afectar al servicio proporcionado.

25. Supervisión de cumplimiento y rendimiento:

25.1. Existen procesos para identificar, registrar y seguir todos los requisitos legales, normativos y contractuales aplicables de la organización.
25.2. Se realizan evaluaciones periódicas para validar el cumplimiento de las obligaciones legales, normativas y contractuales. Se mantienen registros para tales evaluaciones y las lagunas identificadas se mitigan sin retraso injustificado.
25.3. Las políticas, procedimientos y directivas se revisan como mínimo una vez al año y se actualizan siguiendo los requisitos legales, normativos y contractuales.
25.4. Los indicadores clave de rendimiento para funciones esenciales, como TI, seguridad de datos y privacidad de datos, se definen, se documentan formalmente, se evalúan periódicamente y se envían los resultados a la dirección.

Seguridad de red

El proveedor garantizará que:

26. Diseño de red y arquitectura de seguridad:

26.1. La red del proveedor emplea principios de "defensa en profundidad" e incorpora controles apropiados como la segmentación de red para minimizar las filtraciones de ciberseguridad y de datos.

26.2. Está implementado diseño arquitectónico sólido con gestión de identidades eficaz y configuraciones robustas de sistema operativo.

26.3. El diseño y la implementación de red pasan revisiones anuales para garantizar la efectividad y seguridad continuadas.

26.4. La configuración de red cumple todos los requisitos legales y normativos aplicables.

27. Control de acceso y autenticación:

27.1. Las conexiones de red externas deben estar documentadas, enrutadas a través de firewalls y verificadas, y deben haber recibido la aprobación antes de su establecimiento.

27.2. El acceso a redes inalámbricas requiere autenticación, autorización, segmentación y cifrado. Existen sistemas para detectar y responder a puntos de acceso inalámbrico fraudulentos o conexiones no autorizadas.

27.3. El acceso remoto a la red del proveedor debe aprobarse y realizarse a través de medios seguros, con autenticación multifactor.

27.4. Están implementados controles para impedir o minimizar el acceso no autorizado a la red del proveedor.

28. Administración y gestión seguras:

28.1. Todo el tráfico de red relacionado con la administración entre estaciones de trabajo administrativas y dispositivos de red usa cifrado y protocolos de autenticación estándares del sector.

28.2. El acceso de administrador no realizado a través de la consola se produce exclusivamente a través de canales cifrados aprobados por el sector.

28.3. Las cuentas de invitado están deshabilitadas o se eliminan, y todas las contraseñas predeterminadas y suministradas por el proveedor se modifican antes de implementar los dispositivos de red en el entorno de producción.

29. Protección de red y contra amenazas:

29.1. Están deshabilitados los servicios, aplicaciones y puertos no usados para reducir la superficie de ataque.

29.2. Se implementan medidas de detección o prevención de intrusiones para segmentos esenciales de la red.

29.3. Los sistemas esenciales están protegidos de los ataques de denegación de servicio (DoS) y de denegación de servicio distribuida (DDoS).

Criptografía

El proveedor garantizará que:

30. Está implementada una política criptográfica completa, junto con los procedimientos auxiliares, para garantizar el cumplimiento de todos los requisitos empresariales, normativos y legales pertinentes Esta directiva sigue las mejores prácticas del sector para garantizar que el cifrado seguro cumpla las leyes y estándares.

31. **Estándares e implementación de cifrado**:
    - 31.1. Solo se permiten algoritmos y fuerzas de clave seguros aprobados por el sector, lo que garantiza la protección de datos adecuada en todos los sistemas y procesos.
    - 31.2. Se implementan soluciones criptográficas para proteger información confidencial y restringir el acceso a datos confidenciales, incluido el cifrado de datos tanto en tránsito como en reposo.
    - 31.3. El almacenamiento y transmisión de las contraseñas están cifrados, lo que mantiene la confidencialidad de las credenciales de usuario en todo momento.
    - 31.4. Los datos de Alludo en tránsito deben estar cifrados (TLS 1.2 como mínimo o un estándar posterior).
    - 31.5. Los datos de Alludo en reposo deben estar cifrados (AES de 256 bits como mínimo o un estándar posterior).

Seguridad de los datos

El proveedor garantizará que:

32. **Recuperación:**
    - 32.1. **Copia de seguridad y recuperación:**
        - 32.1.1. Las copias de seguridad de los datos de Alludo deben realizarse periódicamente.
        - 32.1.2. Las copias de seguridad de los datos de Alludo deben conservarse durante 1 año.
        - 32.1.3. Las copias de seguridad de los datos de Alludo deben estar cifradas.
    - 32.2. **Recuperación ante desastres:**
        - 32.2.1. El plan de recuperación ante desastres debe probarse de manera anual.

33. **Política y procedimientos de copia de seguridad:**
    - 33.1. La política de copia de seguridad y los procedimientos auxiliares deben estar claramente documentados.
    - 33.2. Los procesos de restauración de copia de seguridad deben estar documentados y probarse a intervalos definidos.
    - 33.3. Deben conservarse pruebas de las pruebas de restauración de copia de seguridad
    - 33.4. Debe conservarse en lugar seguro una copia de los archivos de copia de seguridad de datos esenciales.

34. **Supervisión de copias de seguridad:**

34.1. Los registros de copias de seguridad con error (si existiesen) deben estar supervisados por el administrador de copias de seguridad.
34.2. Las acciones correctivas para copias de seguridad con error deben aplicarse y documentarse.

35. Ubicación de datos:
35.1. El proveedor es responsable de garantizar el cumplimiento de todas las leyes de protección de datos y de privacidad aplicables en los países en que se van a almacenar los datos.
35.2. Debe respetar las restricciones de transferencia de datos entre fronteras (RGPD, etc.).
35.3. El proveedor debe implementar medidas de seguridad técnicas y organizativas apropiadas para proteger los datos, siguiendo las leyes y estándares de los países en que están almacenados los datos.
35.4. Alludo se reserva el derecho de auditar las prácticas de gestión de datos del proveedor para garantizar el cumplimiento de las medidas de seguridad y normativas legales acordadas.

36. Borrado de datos:
36.1. Deben existir procedimientos para el borrado seguro de datos tras la finalización del contrato, garantizando el cumplimiento de las leyes locales de retención de datos.

37. Cifrado de discos completo:
37.1. Debe estar configurado el cifrado de discos completo para las estaciones de trabajo y los servidores.

38. Clasificación de datos:
38.1. Debe existir una política de clasificación de datos documentada.
38.2. Los datos deben clasificarse en función de su criticidad y confidencialidad.
38.3. Deben identificarse e implementarse controles de seguridad correspondientes a la confidencialidad de los datos.

Comunicación de información

El proveedor garantizará que:

39. Seguridad web:
39.1. Está implementado software de filtrado de contenido web para bloquear el acceso a los sitios web que alojan contenido malicioso.
39.2. El acceso a todos los sistemas y aplicaciones basados en web debe llevarse a cabo a través de mecanismos seguros y autenticados.
39.3. La comunicación cliente-servidor para aplicaciones y portales web debe realizarse a través de canales cifrados.

40. Seguridad de correo electrónico:
40.1. Existen controles de seguridad para impedir el uso incorrecto del sistema de correo electrónico.

40.2. Todas las comunicaciones de correo electrónico deben transmitirse a través de canales cifrados.
40.3. La puerta de enlace de correo electrónico está equipada con:
40.3.1. Filtros anti-phishing.
40.3.2. Protocolos de seguridad para correo electrónico (p. ej., DMARC, DKIM y SPF).
40.3.3. Otras configuraciones necesarias para evitar la amenazas por correo electrónico.

Desarrollo de software

El proveedor garantizará que:

41. Ciclo de vida de desarrollo de software:
41.1. Debe existir un marco de trabajo establecido de desarrollo de software y de sistemas.
41.2. Los sistemas y las aplicaciones deben desarrollarse siguiendo las mejores prácticas de desarrollo de software seguro (p. ej., OWASP).
41.3. El código de software debe estar:
41.3.1. Protegido de modificaciones no autorizadas
41.3.2. Almacenado de manera segura
41.3.3. Sujeto a procesos de control de calidad
41.4. Deben realizarse revisiones del código.

42. Pruebas e implementación:
42.1. Las aplicaciones deben someterse a pruebas exhaustivas de seguridad y funcionalidad antes de su implementación en el entorno de producción.
42.2. Los entornos de producción y los que no sean de producción deben estar correctamente segregados.
42.3. Debe mantenerse la segregación de obligaciones entre el desarrollo para producción y el que no sea para producción.
42.4. Los datos para producción no deben existir en entornos de prueba.

Seguridad de aplicaciones

El proveedor garantizará que:

43. Seguridad de aplicaciones:
43.1. Se realizan evaluaciones de la seguridad de aplicaciones para todas las aplicaciones de nuevo desarrollo y todas las aplicaciones existentes que experimenten cambios considerables para identificar vulnerabilidades de seguridad conocidas.
43.2. Se mitigan todas las vulnerabilidades de seguridad identificadas con una puntuación CVSS superior a 4 antes de implementar la aplicación en el entorno de producción.

43.3. Se implementan procesos de revisión del código para identificar y remediar código que podría introducir vulnerabilidades de seguridad.

44. Protección de aplicaciones web:

44.1. Las aplicaciones web públicas están protegidas por un firewall de aplicaciones web sólido para evitar las amenazas externas.

Gestión de revisiones

El proveedor garantizará que:

45. Se apliquen las revisiones de seguridad más recientes a los sistemas, redes, aplicaciones y bases de datos a su debido tiempo y en función de la criticidad de la vulnerabilidad solucionada por la revisión. Las revisiones se obtienen de los OEM respectivos directamente para sistemas propietarios.

46. Todas las revisiones se prueban antes de la implementación de las revisiones en los sistemas de producción y se comprueba el funcionamiento correcto del servicio revisado tras cualquier actividad de revisión.

47. Existen mitigaciones si no se puede revisar un sistema y la eficacia de esas mitigaciones se evalúa periódicamente y se mantienen las pruebas correspondientes.

Protección contra malware

El proveedor garantizará que:

48. Todos los sistemas de TI están protegidos constantemente por una solución de protección contra malware que inspecciona los datos entrantes en tiempo real para evitar las interrupciones del servicio y las infracciones de seguridad. Además, se aplican procedimientos adecuados de concienciación de los usuarios. El sistema anti-malware detecta varias amenazas, como por ejemplo, virus, spyware, gusanos, código móvil no autorizado, registradores de pulsaciones de teclas, botnets y troyanos.

49. Las firmas de malware se actualizan con regularidad para garantizar que los sistemas estén siempre equipados con las definiciones de amenazas más recientes.

50. El software de protección contra malware está configurado para realizar análisis tanto programados como bajo demanda, y para aislar o eliminar cualquier software o archivo malicioso identificado.

51. Los usuarios finales no tienen los derechos ni la capacidad de deshabilitar la protección contra malware.

Gestión de vulnerabilidades

El proveedor garantizará que:

52. Proceso de gestión de vulnerabilidades:

52.1. Están establecidas políticas, procesos y procedimientos para la gestión completa de vulnerabilidades.

52.2. Están establecidos procesos para recibir, analizar y responder a vulnerabilidades tanto de fuentes internas como externas.

53. Evaluación y remedio de vulnerabilidades:

53.1. Evaluaciones trimestrales de vulnerabilidades de la infraestructura de TI y aplicaciones del proveedor, incluidos los sitios de recuperación ante desastres.
53.2. Remedio de las vulnerabilidades identificadas con puntuación CVSS superior a 4 dentro de líneas de tiempo definidas.

54. Pruebas de penetración:

54.1. Pruebas anuales independientes de penetración de la infraestructura de TI y aplicaciones del proveedor utilizadas para los servicios de Alludo.
54.2. Las pruebas tienen como objetivo identificar vulnerabilidades explotables y evitar las infracciones de seguridad mediante ciberataques.
54.3. Acceso concedido por Alludo a los informes de pruebas de penetración/vulnerabilidad pertinentes bajo demanda razonable.

Registro y supervisión

El proveedor garantizará que:

55. Los servicios esenciales, como las aplicaciones, están configurados para registrar eventos clave (incluidos aquellos de acceso privilegiado y actividad de usuario) y conservarlos durante un período mínimo de 1 año o según los requisitos normativos aplicables.
56. Como mínimo, los registros de eventos clave (según corresponda) contienen lo siguiente:

56.1. Inicio y apagado del sistema.
56.2. Estado de inicio y parada de servicios y procesos esenciales.
56.3. Cambios en los parámetros de configuración (p. ej. cambios en la configuración de arranque de sistema).
56.4. Inicios de sesión correctos e intentos de inicio de sesión con error.
56.5. Creación, modificación y eliminación de cuentas de usuario.
56.6. Acceso a sistema/recursos.
56.7. Identificación y ubicación de quién accedió a los recursos y desde dónde.
56.8. Fecha y marca de hora.

57. Se recopilan y correlacionan los registros de auditoría de varios orígenes y sensores y se almacenan de manera segura para permitir la reconstrucción de tales eventos.
58. Están establecidos procesos para supervisar eventos del registro (preferiblemente en tiempo real) para detectar cualquier actividad no autorizada, blancos de ataques, y garantizar que se revisen los registros de eventos clave.

Gestión de incidentes

El proveedor garantizará que:

59. Las funciones y procesos están claramente definidos para garantizar una respuesta rápida, eficaz y organizada a los incidentes de privacidad y seguridad de la información.
60. Los empleados y contratistas están formados para reconocer lo que constituye un incidente de seguridad, así como cómo y dónde informar de cualquier incidente potencial o confirmado.
61. El personal responsable de analizar y responder a incidentes está cualificado en el tema y asiste a formación con regularidad acerca de las prácticas eficaces de respuesta a incidentes.

62. Se mantiene un repositorio para todos los incidentes notificados, que detalla las acciones tomadas para mitigar el impacto del incidente y las lecciones aprendidas del evento.
63. Se notifica a Alludo tan pronto como la organización conozca cualquier incidente que les afecte, pero no más tarde de 24 horas tras la detección.

Seguridad física y ambiental

El proveedor garantizará que:

64. Se implementan as políticas y procedimientos para seguridad física y controles ambientales, siguiendo los estándares del sector.
65. Las instalaciones esenciales que alojan sistemas, aplicaciones y personal de TI (p. ej., centros de datos, sitios operativos) están protegidas de accidentes, ataques y acceso no autorizado.
66. Existen medidas de seguridad, como controles de acceso electrónicos, verificación de identidad, guardas de seguridad, gestión de visitantes y videovigilancia 24/7, para evitar la entrada no autorizada.
67. Las grabaciones de videovigilancia se conservan un mínimo de 30 días, o más si la normativa legal así lo requiere.
68. El acceso a las instalaciones está restringido al personal autorizado para fines específicos y bajo constante revisión.
69. Se escolta a los visitantes, se registran sus horas de entrada y salida y deben llevar identificadores de visitante en todo momento. Se recogen las tarjetas o llaves de acceso a la salida.
70. Las instalaciones esenciales están protegidas de los apagones mediante sistemas de alimentación ininterrumpida (UPS) o generadores para garantizar la continuidad de las operaciones.
71. Se lleva a cabo mantenimiento periódico en equipo esencial, como UPS, generadores, detectores de humo, sistemas de supresión de incendios y sistemas de control de acceso, con registros guardados.
72. Las instalaciones se construyen con materiales ignífugos y están equipadas con alarmas de incendio, detectores de humo, sensores de temperatura e inundación y extintores para protegerlas de los riesgos naturales.
73. Están definidos mecanismos seguros de eliminación de datos tanto en formatos físicos como de software, utilizando trituradoras de papel y métodos como el saneamiento, el desimantado y la destrucción para medios electrónicos.
74. La política de escritorio limpio garantiza la manipulación segura de las notas post-it, documentos escritos y medios extraíbles.
75. Los controles físicos y ambientales se evalúan al menos anualmente para comprobar su efectividad.

Privacidad y protección de datos

Si el proveedor o sus subprocesadores procesan datos personales en nombre de Alludo o de los clientes de Alludo, el proveedor garantizará lo siguiente:

76. Cumplimiento y gobernanza de la privacidad de datos:

76.1. Cumplimiento de todas las leyes de protección de datos aplicables.
76.2. Establecimiento de un marco de trabajo de gestión de la privacidad, como:
76.3. Políticas de privacidad, declaraciones, avisos y procedimientos (con revisión anual).
76.4. Gobernanza de la privacidad y procesos de gestión de riesgos.
76.5. Observancia de los requisitos legales y normativos.
76.6. Mantenimiento de registros actualizados de actividades de procesamiento para los datos personales de Alludo.
76.7. Definición e implementación de funciones y responsabilidades apropiadas para la privacidad de datos:
76.8. Nombramiento de un director jefe de privacidad de datos (o equivalente).
76.9. Establecimiento de una función de privacidad de datos especializada.
76.10. Formación de un comité para coordinar las actividades de cumplimiento de la privacidad de datos.

77. Medidas de seguridad y protección de datos

77.1. Implementación de protecciones estándares del sector (p. ej., ISO/IEC 27001:2013, SOC2, etc.) para
proteger la información de Alludo.
77.2. Aplicación de protecciones adicionales para datos personales confidenciales (p. ej, cifrado, pseudonimización).
77.3. Aplicación de controles de acceso:
77.4. Restricción de acceso en función de la necesidad y el principio del menor privilegio.
77.5. Elimina los derechos de acceso rápidamente por finalización de cambios de función.
77.6. Realización de reseñas de acceso periódicas.
77.7. Aplicación de compromisos de confidencialidad por parte de todo el personal que procesa datos personales.

78. Gestión de derechos de los interesados:

78.1. Ayuda a Alludo a satisfacer las obligaciones de derechos de los interesados para datos.
78.2. Notifica a Alludo en los dos días siguientes a recibir solicitudes de los interesados.
78.3. Responde solamente a las solicitudes, tal y como indique Alludo, a menos que la Ley requiera algo distinto.

79. Respuesta a incidentes:

79.1. Notifica a Alludo en 24 horas de las infracciones de datos personales que implican a datos de Alludo.

Medidas de subcontratación

El proveedor garantizará que:

80. Está realizando evaluaciones anuales de riesgos externos a todos los subprocesadores que participan en la manipulación, procesamiento o almacenamiento de datos de Alludo. Estas evaluaciones deberían aplicarse a los controles de seguridad de los subprocesadores, las medidas de protección de datos, el cumplimiento con la normativa pertinente y la posición general ante riesgos. Los proveedores deben proporcionar documentación de estas evaluaciones bajo solicitud, solucionar rápidamente cualquier riesgo identificado y comunicar cualquier cambio a los subprocesadores o hallazgos importantes a su debido tiempo. Nos reservamos el derecho de revisar los resultados de las evaluaciones y solicitar medidas de seguridad adicionales en caso necesario.

Gestión de la continuidad empresarial

El proveedor garantizará que:

81. Esté establecida una política de gestión de la continuidad empresarial (BCM), acompañada de planes y procedimientos detallados. Estos documentos describen los objetivos de continuidad empresarial de la organización y se someten a revisión y aprobación anuales.

82. Se desarrolla e implementa un marco de trabajo de pruebas BCM para evaluar la efectividad de las estrategias existentes de continuidad empresarial.

83. Se llevan a cabo análisis de impacto empresarial (BIA) al menos de manera anual o tras cambios importantes en la organización.

84. Se establece un plan de gestión de crisis, incluidas estipulaciones específicas para la preparación ante pandemias. Este plan garantiza una respuesta adecuada a las emergencias y se concentra en la protección de los empleados, los visitantes, el medioambiente y los activos, y el mantenimiento de las operaciones empresariales esenciales.

85. El sistema de gestión de la continuidad empresarial (BCMS) se somete a pruebas anuales de eficacia, y se conservan registros detallados de cada prueba.

<Fin del documento>