Medidas técnicas y organizativas (TOM) en seca

Esta traducción se proporciona únicamente para su comodidad y mejor comprensión. No es legalmente vinculante y no sustituye en modo alguno a la versión original legalmente vinculante de este documento en inglés. En caso de discrepancias o inconsistencias entre esta traducción y la versión original, prevalecerá la versión original en inglés.

seca no asume ninguna responsabilidad por la exactitud, integridad o actualidad de esta traducción. El uso de esta traducción es bajo su propia responsabilidad. Se recomienda encarecidamente consultar la versión original de este documento en inglés o buscar asesoramiento legal para cualquier cuestión jurídica o ambigüedad.

Descripción de las medidas técnicas y organizativas de seca de conformidad con el artículo 32 del RGPD.

seca opera un sistema de gestión de la seguridad de la información certificado con
gestión de la protección de datos integrada de conformidad con las normas internacionales
ISO/IEC 27001:2022 e
ISO/IEC 27701:2019.

A. Seudonimización y cifrado (art. 32, apartado 1, letra a), del RGPD)

Criptografía

- Uso de cifrado de correo electrónico (TLS 1.2) y métodos de mensajería segura
- Gestión segura de claves
- Seudonimización en el tratamiento de los datos del estudio
- Seudonimización en los archivos de registro

B. Confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios (art. 32, apartado 1, letra b), del RGPD)

Organización de la seguridad de la información

- Uso de software central para la administración de teléfonos inteligentes
- Posibilidad de borrado remoto de datos en los dispositivos móviles
- Evaluación y revisión periódica de los proveedores de servicios en lo que respecta a la seguridad de la información y la protección de datos
- Especial cuidado en la selección del personal de limpieza y seguridad

Seguridad del personal

- Compromiso de los empleados con las políticas de privacidad de datos y seguridad de la información
- Política de escritorio limpio y política de pantalla limpia
- Formación periódica sobre protección de datos y seguridad de la información, incluyendo el phishing y cómo tratar los dispositivos no utilizados, cómo dar de

baja los servicios que ya no se utilizan y cómo manejar la información de autenticación, las claves y los transpondedores

Gestión del valor

- Registro de equipos informáticos
- Documentación de la emisión y devolución de equipos informáticos
- Política de control de documentos con la definición de niveles de confidencialidad y el marcado adecuado de los documentos
- Puesta en servicio de trituradoras con sello de protección de datos para la destrucción de archivos y soportes de datos electrónicos.
- Registro de la destrucción o eliminación de archivos y soportes electrónicos de datos

Control de acceso

- Funcionamiento de un sistema automatizado de control de acceso (gestión de identidades y accesos, IAM)
- Implementación de una política de asignación de accesos según un modelo de derechos y roles
- Matriz para la asignación de perfiles de usuario a los sistemas informáticos
- Asignación de derechos según el principio de «necesidad de conocer»
- Proceso formalizado para la concesión de derechos con la aprobación del supervisor correspondiente
- Eliminación del usuario o revocación de los derechos de usuario al abandonar la empresa
- Ajuste de los derechos de usuario en caso de cambio de responsabilidad
- Sistema de inicio de sesión único para todas las aplicaciones esenciales
- Conceptos de permisos de lectura/escritura para unidades y archivos, así como para páginas y áreas individuales en la wiki interna
- Conceptos de permisos de lectura/escritura para sistemas de tickets
- Gestión centralizada de derechos a través del servicio Microsoft Active Directory
- Cambio de contraseñas cada 72 días
- Política de contraseñas que incluye la longitud, la complejidad, el historial y la validez de las contraseñas
- Necesidad de cambiar la contraseña inicial en el primer inicio de sesión
- Asignación de cuentas de usuario adicionales para administradores (además de su cuenta de usuario personal)
- Básicamente, sin derechos de administrador de dominio o local para los usuarios (excepción: derechos de administrador local para ordenadores en una red de desarrolladores especialmente particionada)
- Acceso protegido por transpondedor a impresoras y colas de impresión individuales
- Registro de intentos de inicio de sesión incorrectos
- Bloqueo de la cuenta de usuario si se supera el número máximo de intentos fallidos
- Autenticación de dos factores para administradores de TI
- Restricción del uso de aplicaciones mediante la gestión de PC.
- Acceso al código fuente de los programas del departamento de Investigación y Desarrollo solo para los desarrolladores

Seguridad física y ambiental

- Sistema de alarma para áreas especialmente sensibles (incluidas las salas de servidores).
- Videovigilancia del acceso a áreas especialmente sensibles
- Protección mediante detectores de movimiento y barreras luminosas
- Mostrador de recepción atendido durante el horario comercial en la zona de entrada
- Registro de visitas de personas externas (lista de visitantes y tarjetas de identificación)
- Acompañamiento de los visitantes por parte de los empleados en las instalaciones de la planta
- Autorización de acceso específica para cada empleado mediante un sistema de cierre con transpondedor
- Ubicación de las salas de servidores en lugares especialmente seleccionados para protegerlas contra el acceso no autorizado, daños por agua o fuego, rayos, etc.
- Ubicación de salas de servidores redundantes en diferentes edificios
- Conocimiento de la existencia y actividad en áreas especialmente sensibles (incluidas las salas de servidores) según el principio de «necesidad de saber»
- Las áreas especialmente sensibles no son reconocibles como tales y no son directamente accesibles desde el exterior
- Acceso externo a las salas de servidores solo con acompañante
- Aire acondicionado y control de la temperatura y la humedad en las salas de servidores.
- Extintor y sistema de alarma contra incendios
- Tendido de cables protegido físicamente.
- Armarios o salas de distribución cerrados con llave en áreas especiales.
- Eliminación de soportes de datos generalmente a través de un proveedor de servicios especializado

Seguridad de las comunicaciones

- Designación de personas responsables de la red e implicación de un proveedor de servicios seleccionado para la administración de la red
- Normas estrictas para la concesión de derechos de acceso a las redes y los servicios de red
- Uso coherente de cortafuegos con tecnología VPN.
- Registro y supervisión continuos de las actividades de la red
- Limitación de los sistemas integrados en la red
- Red separada para desarrolladores
- Red WLAN para diversos fines (por ejemplo, WLAN independiente para invitados)

Adquisición, desarrollo y mantenimiento de sistemas

- Desarrollo de software para aplicaciones de uso propio según los mismos estándares y procesos que para el software médico
- Proceso de control de cambios establecido también para aplicaciones de uso propio
- Procesos de verificación y validación de aplicaciones desarrolladas externamente y por cuenta propia
- Red especialmente protegida para el desarrollo de productos y aplicaciones de uso propio
- Entorno de pruebas especialmente protegido
- Generación de datos de prueba especiales en lugar de conjuntos de datos reales con datos personales.

Relaciones con proveedores de servicios y suministradores

- Selección cuidadosa del personal de seguridad y limpieza
- Celebración de contratos de procesamiento de pedidos de conformidad con el artículo 28 del RGPD en el caso del procesamiento de datos por cuenta ajena o meras cláusulas de protección de datos y acuerdos de confidencialidad en el caso de otros encargos a proveedores de servicios y proveedores

C. Rápida restauración de la disponibilidad y el acceso (art. 32, apartado 1, letra c), del RGPD)

Seguridad operativa

- Supervisión de recursos
- Eliminación periódica de datos obsoletos para optimizar el espacio de almacenamiento
- Desmantelamiento de aplicaciones, sistemas, bases de datos o entornos cuando deja de existir la finalidad de la aplicación
- Optimización de los procesos por lotes y los calendarios
- Limitación del ancho de banda de los servicios que consumen muchos recursos (por ejemplo, la transmisión de vídeo).
- Separación de los entornos de desarrollo, prueba y operación para servicios en la nube, aplicaciones internas y sistemas
- Filtro web y bloqueo de descargas
- Uso sistemático de software antivirus
- Suscripción a servicios de alerta e información relevantes
- Proceso de copia de seguridad de datos según el principio de generación y pruebas periódicas de las copias de seguridad para comprobar su recuperabilidad.
- Conservación de parte de las copias de seguridad en una ubicación externa
- Registro de auditoría de los sistemas pertinentes utilizados en toda la empresa
- Gestión de cambios y procedimientos de aprobación para la actualización de aplicaciones
- Prueba de las aplicaciones antes de su instalación en un sistema de prueba
- Uso de estrategias de reversión al actualizar aplicaciones

Aspectos de seguridad de la información en la gestión de la continuidad del negocio

- Política de gestión de la continuidad del negocio
- Documentación y revisión de los planes de emergencia
- Acceso a Internet de emergencia a través de un segundo proveedor
- Sistema de alimentación ininterrumpida (SAI)
- Generador diésel de emergencia para dos días de funcionamiento independiente de los sistemas informáticos

D. Revisión, evaluación y valoración periódicas de la eficacia (art. 32, apartado 1, letra d), del RGPD)

- Aplicación de una política de seguridad de la información y su revisión anual como parte de la gestión de la calidad de conformidad con la norma ISO 9001 (ya aplicada) y la norma ISO 27001 (prevista)

- Nombramiento de un responsable de seguridad de la información que depende directamente de la dirección, independientemente de TI y de los demás departamentos especializados

Gestión de incidentes relacionados con la protección de datos y la seguridad de la información

- Creación de un equipo de protección de datos y seguridad de la información con una dirección de correo electrónico específica.
- Evaluación periódica de los incidentes y del statu quo por parte de este equipo.
- Asesoramiento del delegado externo de protección de datos sobre la evaluación de una violación de datos personales de conformidad con los artículos 33 y 34 del RGPD en lo que respecta a las medidas, las obligaciones de notificación y la notificación a los interesados.

Cumplimiento

- Supervisión de la protección de datos y la seguridad de la información por parte del departamento jurídico interno

Control de pedidos (participación de terceros/externalización)

- No se realiza ningún tratamiento de datos por encargo sin el correspondiente contrato
- Normativa sobre el uso de otros subcontratistas
- Celebración de los acuerdos necesarios sobre el tratamiento por encargo de conformidad con el artículo 28 del RGPD o las cláusulas contractuales tipo de la UE para terceros países (artículo 44 y siguientes del RGPD).

E. Medidas en relación con los servicios en la nube

- Dado que seca opera servicios SaaS exclusivamente en la infraestructura del subcontratista Amazon Web Services EMEA SARL (AWS), especializado en alojamiento de servidores externos, en la sede de Fráncfort del Meno, y que no se almacenan ni procesan datos personales de clientes, empleados o datos sanitarios en las propias instalaciones de seca, las medidas técnicas y organizativas mencionadas anteriormente en el caso de SaaS se limitarán a las medidas de seguridad establecidas por el contratista en sus instalaciones.
- Las TOM de AWS están disponibles en https://aws.amazon.com/de/compliance/data-center/controls/.
- seca cifra todos los datos personales en los servicios SaaS para impedir el acceso no autorizado a estos datos.
- Seca comprueba periódicamente los requisitos del art. 44 y siguientes del RGPD en relación con el uso de AWS como proveedor de servicios. Si es necesario, se proporcionan las garantías adecuadas exigidas en el art. 46 del RGPD, en particular en forma de cláusulas tipo de protección de datos.