T-Systems Iberia Security Rules

T-Systems Iberia

Tabla de contenidos

1. Instrucciones de uso 3
2. Soporte 4
2.1. Concienciación 4
2.2. A6 Organización de la Seguridad de la Información 4
2.3. A7 Seguridad para los Recursos Humanos 4
2.4. A8. Gestión de Activos 4
2.5. A8.2 Clasificación de la Información 5
2.6. A.8.3 Manejo de medios 11
2.7. A.9 Control de acceso 12
2.7.1. A.9.2 Gestión de acceso de usuarios 13
2.7.2. A.9.3 Responsabilidad del usuario 13
2.7.3. A.9.4 Control de acceso al sistema y a las aplicaciones (directiva de contraseñas) 13
3. A.10 Criptografía 14
4. A.11 Seguridad física y ambiental 14
4.1. A.11.1 Áreas seguras (Requisitos Identificación) 14
4.2. A.11.2 Equipo (Política de escritorio limpio) 14
5. A.12 Seguridad de la operación 14
6. A.13 Seguridad de las comunica- ciones 14
7. A.14 Adquisición, Desarrollo y Mantenimiento 14
8. A.16 Gestión de incidentes de se- guridad de la información 15
9. A.18 Compliance 15

1. Instrucciones de uso

Este documento contiene un resumen de las reglas de seguridad del manual ISMS Handbook, que aplica a todos los empleados

Todos en el grupo Deutsche Telekom, empleados, externos o subcontratistas, somos responsables que nuestras acciones cumplan con los diez principios generales de seguridad de Deutsche Telekom.

En particular, todas las personas son responsables de la protección de la información en su área de responsabilidad, influencia o control. Cada uno también debe conocer sus tareas de seguridad por iniciativa propia y cuestionará cualquier requisito que considere ambiguo o ininteligible, por ejemplo, oponiéndose a cualquier instrucción que sea manifiestamente ilegal.

Se anima a todos a notificar a la empresa de cualquier riesgo e incidente de seguridad relevante del que tengan conocimiento. La información puede facilitarse a través del superior jerárquico respectivo o a través de canales de comunicación especiales establecidos específicamente para tales fines, a través de los cuales dichas divulgaciones pueden presentarse de forma confidencial, cuando todas las personas que proporcionen la información de buena fe estén protegidas de posibles desventajas y el anonimato de la persona esté garantizado por medios técnicos. Especialmente en tiempos de creciente uso de las redes sociales internas y externas para la comunicación y la colaboración, depende más que nunca del individuo decidir sobre las actividades y el comportamiento adecuados.

Por lo tanto, todos deben ser conscientes de los conceptos básicos de la cultura de seguridad y la conciencia para prevenir los riesgos de seguridad planteados, por ejemplo, por la ingeniería social o el phishing. (Security Policy).

Notas

- Los capítulos se refieren al ISMS Handbook y a la ISO/IEC 27001.
- Los números se refieren a los requerimientos del Security Control Framework.
  El Security Control Framework es el paquete completo de normas de seguridad.
  Ver el capítulo A del ISMS Handbook.
- ISMS: Information Security Management System

2. Soporte

2.1. Concienciación

[1.7.3.1.A b)] La participación en los cursos centrales de concienciación y formación es obligatoria para los empleados de todas las entidades legales dentro de la compañía.

2.2. A6 Organización de la Seguridad de la Información

A6.2.1.0 a) Los discos duros/dispositivos de datos de los dispositivos móviles deben estar completamente encriptados.

2.3. A7 Seguridad para los Recursos Humanos

A7.80.2.0 a) La unidad firmante debe garantizar que se asignen responsabilidades para el tema de la violencia en el lugar de trabajo y que las personas de contacto competentes estén disponibles para los empleados involucrados cuando sea necesario.

2.4. A8. Gestión de Activos

A.8.1 Responsabilidad sobre los activos

Los activos son todo lo que tiene valor para la empresa. Hay muchos tipos de activos:

- Recursos humanos (y sus cualificaciones, competencias, experiencia, etc.),
- Información
- Activos tangibles (infraestructura, hardware/software, etc.),
- Valores intangibles (reputación, imagen, etc.),
- Servicios.

A8.1.2.0 a) Para cada activo de valor de la empresa (edificio, equipo de lugar de trabajo, hardware, software) debe nombrarse una persona como responsable del activo y su protección.

A8.1.1.0 a) Es responsabilidad del administrador de activos garantizar el mantenimiento de registros adecuados relacionados con el pedido, la emisión, la transmisión y el desmantelamiento de sus activos.

A8.1.3.0 a) El hardware y el software para uso de la empresa deben ser proporcionados por la empresa para uso de la empresa

A8.1.3.0 b) Por regla general, las herramientas de trabajo proporcionadas por el empleador deben utilizarse en principio para tareas relacionadas con la empresa.

2.5. A8.2 Clasificación de la Información

Definición de los objetivos de protección. Los siguientes objetivos de protección deben observarse a efectos de información y protección de datos:

- **Confidencialidad** - La condición de que la información no puede ser puesta a disposición o divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad** - La condición de que la información sea accesible a petición de una persona, entidad o proceso autorizado.
- **Integridad** - La condición de salvaguardar la exactitud e integridad de la información.
- **Autenticidad** - La condición de proporcionar evidencia de que el remitente / autor y, cuando corresponda, el destinatario de un elemento de in- formación, son claramente verificables.
- **Privacidad** - La condición de que la información personal se maneje de acuerdo con las disposiciones legales

Clases de protección para el objetivo de protección Confidencialidad

Los siguientes criterios de toma de decisiones ayudan en la clasificación con el objetivo de protección de "Confidencialidad".

ABIERTO

Información que puede ser publicada.
Información destinada al público o a la publicación.
Información ya publicada o disponible públicamente (en periódicos o Internet).

INTERNA

Información que puede ser conocida por todos dentro de la empresa.
Información que puede ser conocida por todos dentro del Grupo DT.

CONFIDENCIAL

Información que puede no ser conocida por todos dentro de la empresa.
Información cuyo acceso y tratamiento estarán especialmente protegidos.
Información que, si se obtiene conocimiento de ella, podría poner en peligro la vida o la integridad física de las personas

CONFIDENCIAL DE CLIENTE

Esta información es importante para la estrategia corporativa de nuestros clientes.

La información está destinada exclusivamente a un grupo de individuos muy definido.

Si existen acuerdos contractuales específicos con respecto a la clasificación de datos y su manejo, estos acuerdos deben cumplirse.

En tales casos, el nombre/descripción del cliente debe añadirse a la clasificación CONFIDENCIAL DE CLIENTE (por ejemplo, CONFIDENCIAL DE CLIENTE DEKRA, o abreviado CONFIDENCIAL-DEKRA).

Clases de protección para el objetivo de protección ‘Disponibilidad’.

Los siguientes criterios de decisión ayudan con la clasificación básica para el objetivo de protección ‘disponibilidad’ y corresponden a las clases de disponibilidad ordenables en el sentido de la gestión del portfolio/producto de la unidad firmante.

Disponibilidad limitada

La información puede no estar disponible durante largos períodos de tiempo (por ejemplo, >7 días*) o, en casos extremos, incluso de forma permanente sin que las operaciones comerciales se vean comprometidas como resultado.

Baja disponibilidad

La información debe estar disponible a corto
plazo (por ejemplo, dentro de las 48 a 72 horas*).

Los sistemas y procesos que dependen de la información no tienen requisitos relacionados con las clases de protección "Disponible" o "Altamente disponible" que puedan verse comprometidos.

Disponibilidad normal

La información debe estar disponible inmediatamente (por ejemplo, dentro de las 8 a 24 horas*).

Los sistemas y procesos que dependen de la información tienen requisitos de protección de "disponibilidad normal" para la información que puede verse comprometida.

Alta disponibilidad

La información debe estar disponible permanentemente (por ejemplo, dentro de 1 a 4 horas.

Los sistemas y procesos que dependen de la información tienen requisitos de protección de "alta disponibilidad" para la información que puede verse comprometida.

Clases de protección para el objetivo de protección 'Integridad'

Los siguientes criterios de toma de decisiones ayudan en la clasificación del objetivo de protección de "Integridad".

Sin integridad

No se causará ningún daño al cambiar la información.

Baja integridad

El emisor de la información no es aparente o no está especificado.

Es posible que la información se pueda cambiar sin ser notada.

Cambiar la información puede causar un daño mínimo.

Integridad normal

El emisor de la información es aparente o puede determinarse con un esfuerzo razonable.

Los cambios en la información se evitan en gran medida; Cualquier cambio posterior siempre se puede detectar/determinar durante una revisión.

Cambiar la información puede causar un daño medio.

Alta integridad

El emisor de la información es inmediatamente aparente y su identidad "verificable".

No es posible cambiar la información sin que esto se note, o todos los cambios en la información pueden ser detectados inmediatamente.

Cambiar la información puede causar daño alto a muy alto.

Clases de protección para el objetivo de protección 'Autenticidad'

No se estipulan clases de protección específicas para el objetivo de protección "Autenticidad", ya que el logro de los objetivos de protección "Integridad" y "Autenticidad" para un elemento específico de información es fuertemente interdependiente.

Por lo tanto, el conocimiento del nivel de integridad de un elemento de información es de poca utilidad si no se conoce la autenticidad, y viceversa. Por esta razón, y también para reducir la complejidad, el objetivo de protección "Autenticidad" se analiza en contexto con el objetivo de protección "Integridad" en esta directiva de grupo, es decir, "Autenticidad" se incluye en "Integridad".
Las medidas de protección utilizadas para lograr los objetivos de protección de "Integridad" y "Autenticidad" ciertamente pueden variar y siempre deben aplicarse de acuerdo con los requisitos actuales en materia de protección

Clases de protección para el objetivo de protección Privacidad

Los siguientes criterios de toma de decisiones ayudan en la clasificación para el objetivo de protección "Privacidad".

Clase de protección 0 - Corresponde a la clase de confidencialidad **ABIERTA**
Datos que no incluyen ninguna referencia a un individuo.
Los datos tienen una referencia a un individuo, pero han sido anonimizados.
Datos personales publicados por el interesado o con su consentimiento, con autorización ilimitada para utilizarlos (periódico, entrevista, libro).

Clase de protección 1 - Corresponde a la clase de confidencialidad **INTERNA**
Datos personales publicados por el interesado o con su consentimiento, con autorización ilimitada para su uso (guía telefónica, redes sociales).
Datos de contacto comerciales de un empleado.
Datos personales seudonimizados.

Clase de protección 2 - Corresponde clase de confidencialidad **CONFIDENCIAL**
De clientes: Datos del contrato, número de teléfono.
De empleados: Dirección privada, datos personales que no pueden asignarse a otra clase de protección de datos.

Clase de protección 3 - Corresponde clase de confidencialidad **CONFIDENCIAL**
Datos personales que pueden implicar una amenaza sustancial para el derecho de auto- determinación con respecto a los datos personales, como con los clientes: metadatos de comunicación electrónica, datos de tráfico/ubicación, contenido de mensajes, datos bancarios; con empleados: Datos de salario/evaluación.

Requirimientos

A8.2.1.0 a) El autor de la información es responsable de su clasificación.

A8.2.1.0 b) La información clasificada como "ABIERTA" debe tener un proceso de divulgación de documentación por escrito. Esta información puede, pero no tiene que ser, identificada con la redacción OPEN (por ejemplo, folleto de feria, contenido de Internet, publicidad).

A8.2.1.0 c) Toda la información de la empresa se considera INTERNA a menos que se especifique lo contrario

Debe etiquetarse como INTERNA. En caso de duda, la in- formación no marcada de ninguna manera se considera INTERNA.

A8.2.1.0 d) La clasificación por clase de protección es vinculante en todas las fases posteriores del tratamiento.

A8.2.1.0 e) Debe garantizarse que, cuando se combinen elementos individuales de información, la clasificación de la información en su conjunto se base en la clase de protección más alta de los elementos individuales de información.

A la hora de clasificar hay que atenerse al límite de valor que la Dirección Financiera estipula para su gestión de riesgos.

A8.2.1.0 f) La clasificación de la información global en función de la clase de protección más alta aplicada a los distintos elementos de información también se aplica a la información ya clasificada obtenida de los clientes u otras unidades de la empresa.

Todas y cada una de las informaciones deben asignarse en función de su necesidad de protección a una clase de protección para el objetivo de protección CONFIDEN- CIALIDAD, es decir, ABIERTA, INTERNA o CONFIDENCIAL.

La necesidad de protección de una información generalmente cambia durante su ciclo de vida. Por lo tanto, deben corregirse las clasificaciones que aparentemente se han asignado erróneamente.

Al generar nueva información (información de destino) a partir de un gran número de elementos individuales de información clasificados de manera idéntica (información de origen), debe comprobarse si esto no da lugar a que la información de destino tenga una clase de protección más alta.

A8.2.1.0 g) Los sistemas de TI / NT deben clasificarse como "críticos" si tienen un requisito de protección alto para al menos un objetivo de protección.

Etiquetado de información

A8.2.2.0 a) La información y los soportes de información clasificados como CONFIDENCIALES y CONFIDENTIAL-CLIENTE deben etiquetarse o darse a conocer como tales.

A8.2.2.0 b) La etiqueta de clasificación de confidencialidad, sin abreviar, debe aplicarse a los documentos de manera que sea claramente visible.

A8.2.2.0 c) Para el tratamiento automático, la clasificación de los datos debe documentarse en el marco del modelo de datos

A8.2.2.0 d) Los documentos con las clases de protección CONFIDENCIAL y CONFIDENCIAL-CLIENTE deben etiquetarse como tales en cada página

A8.2.2.0 e) La etiqueta debe estar en inglés, independientemente del idioma de los datos o documentos. Se recomienda la traducción de la etiqueta de clasificación al idioma del documento o de los datos.

Los correos electrónicos clasificados como CONFIDENCIALES deben etiquetarse como tales. Si es evidente para el destinatario que la transmisión de un correo electrónico está encriptada (por ejemplo, a través del símbolo de candado), esto es suficiente para etiquetar la clase de protección CONFIDENCIAL.

A8.2.2.0 f) En el caso de los sistemas de TI/NT con contacto directo con los empleados (por ejemplo, aplicaciones de TI/NT o teléfono), el usuario DEBE ser convenientemente informado mediante el etiquetado de las restricciones de uso de la información clasificada como "CONFIDENCIAL", o bien las medidas organizativas de- ben garantizar que los empleados son conscientes de las restricciones de uso.

Manejo de la información

A8.2.3.0 a) La información clasificada solo debe almacenarse en plataformas proporcionadas por la empresa que hayan sido aprobadas para su uso con información que tenga al menos esta clase de protección.

A8.2.3.0 b) Las copias, extractos, duplicaciones, microfilms y traducciones de información clasificada y soportes informativos sólo deben crearse cuando sea necesario. Deben clasificarse y manejarse como sus respectivos originales.

A8.2.3.0 c) La duplicación de la información del CLIENTE CONFIDENCIAL solo se permite con el consentimiento del autor. Este consentimiento debe documentarse.

A8.2.3.0 d) Los datos CONFIDENCIALES y CONFIDENCIALES DE CLIENTE solo deben transmitirse con él consentimiento del autor. El autor determina qué personas tendrán acceso a esta información.

A8.2.3.0 e) Los destinatarios de la información CONFIDENCIAL DE CLIENTE deben ser documentados

A8.2.3.0 f) Los terceros externos al Grupo (como los socios contractuales) solo deben recibir la información que necesitan para llevar a cabo actividades comerciales.

A8.2.3.0 g) La configuración del envío automático de información de la empresa a terceros externos del Grupo (por ejemplo, buzones externos, buzones de voz) no está, por regla general, permitida. Cualquier excepción debe ser aprobada por el autor de la información.

A8.2.3.0 h) El envío o reenvío de mensajes electrónicos a cuentas privadas (por ejemplo, correo electrónico, buzones de voz, SMS) de empleados o terceros no está, en principio, permitido.

A8.2.3.0 i) Al transmitir datos CONFIDENCIALES y CONFIDENCIALES DE CLIENTE electrónicamente (es decir, por correo electrónico) siempre deben estar encriptados.

2.6. A.8.3 Manejo de medios

A8.3.1.0 c) Los soportes de información cuando no esté claro o no sea conocido por los empleados si ya se han utilizado o no en algún momento para archivar información deben clasificarse al menos como internos.

A8.3.2.0 a) Los soportes de información (tales como soportes de datos móviles, discos duros, impresiones, impresoras, portátiles, dispositivos de almacenamiento, servidores, etc.) que contengan información asignada a la clase de protección INTERNA deben eliminarse de tal manera que se garantice la prevención del acceso no autorizado.

A8.3.2.0 b) Para los soportes de información de la clase de protección CONFIDENCIAL, la recuperación no debe ser posible utilizando la tecnología más avanzada.

A8.3.2.0 c) Los medios de almacenamiento no cifrados deben eliminarse o destruirse de forma segura (es decir, de modo que no se puedan recuperar) antes de entregarlos a terceros externos al Grupo.

A8.3.2.0 d) Si se requieren reparaciones por parte de personal ajeno a la empresa y no fue posible la eliminación segura de los datos guardados de antemano, estas reparaciones solo deben llevarse a cabo mediante acuerdo específico o teniendo en cuenta el principio de doble control.

A8.3.2.0 e) Por lo general, se requiere la eliminación segura de datos cuando los medios o los ordenadores cambian de usuarios principales.

A8.3.2.0 f) Si los soportes informativos deben ser destruidos por terceras empresas, los acuerdos contractuales con estos proveedores deben describir detalladamente el procedimiento y también referirse a las consecuencias legales en caso de que no se cumplan.

A8.3.2.0 g) La clasificación de un soporte de información debe verificarse y modificarse cuando proceda tras la su- presión segura de la información almacenada en el so- porte. La eliminación segura debe implementarse utilizando un producto o proceso de eliminación aprobado por los responsables de la gestión de la seguridad.

2.7. A.9 Control de acceso

Los siguientes principios consolidan los requisitos al manejar información y datos:

Necesidad de proteger - La clasificación de la información debe basarse siempre en los requisitos específicos de protección existentes. No sirve para subrayar la importancia de las personas o los departamentos relacionados con ella. El etiquetado general de toda la información/documentos de un departamento como "CONFIDENCIAL" no suele tener sentido.

Necesidad de saber- El acceso a la información y los datos está restringido a un grupo de personas claramente definido y al alcance que se requiere para llevar a cabo sus tareas.

Necesidad de ver - El entorno de trabajo y el equipo deben organizarse de tal manera que las personas no autorizadas no puedan ver u obtener acceso a la información y los datos.

Necesidad de tener - La información puede recopilarse y almacenarse solo en la medida en que sea absolutamente necesario o permitido en interés de la unidad firmante o debido a requisitos legales o contratos con clientes.

Separación de funciones- La acumulación de funciones no debe restringir la eficacia de los conceptos de autorización. Las funciones deben estar suficientemente separadas al planificar los procedimientos operativos. Cuando esto no pueda aplicarse, se determinarán alternativas adecuadas, como la vigilancia de las actividades o los registros de actividades.

2.7.1. A.9.2 Gestión de acceso de usuarios

A9.2.3.0 b) La puesta a disposición, administración y responsabilidad de la infraestructura de red será responsabilidad exclusiva de ICT Management o de un agente en- cargado por ellos.

A9.2.4.0 a) Los medios de autenticación (contraseñas, certificados …etc.) deben mantenerse confidenciales, almacenarse de forma segura y cambiarse regularmente.

A9.2.4.0 b) Los medios de autenticación deben cambiarse inmediatamente si hay alguna sospecha de corrupción.

A9.2.4.0 c) El período de validez de los medios de autenticación debe ser limitado.

2.7.2. A.9.3 Responsabilidad del usuario

A9.3.1.0 a) Los medios de autenticación no deben, ser revelados a terceros y deben ser cambiados inmediatamente si la divulgación es necesaria por cualquier motivo.

A9.3.1.0 c) Cada nuevo usuario recibe su propia contraseña inicial que debe cambiarse al iniciar sesión por primera vez. El usuario debe iniciar sesión por primera vez dentro de las 24 horas posteriores a la recepción de la contraseña inicial.

2.7.3. A.9.4 Control de acceso al sistema y a las aplicaciones (directiva de contraseñas)

A9.4.3.0 a) La contraseña debe tener un mínimo de 12 caracteres e incluir caracteres en al menos tres de las siguientes categorías: letras minúsculas, letras mayúsculas, números o caracteres especiales.

A9.3.1.0 b) Para las estaciones de trabajo, la contraseña debe cambiarse después de al menos 365 días (por ejemplo, Directorio Activo). Para aplicaciones y otros sistemas, la palabra de contraseña también debe cambiarse después de al menos 365 días. Además, debe producirse un reconocimiento del abuso de contraseñas.

A9.4.3.0 b) La nueva contraseña debe diferir de las 5 contraseñas anteriores y no debe haberse utilizado en los últimos 2 meses. El usuario debe poder cambiar su propia contraseña en cualquier momento (no debe haber un período mínimo de validez).

A9.4.3.0 c) Después de no más de 5 intentos incorrectos de ingresar una contraseña, el acceso al sistema debe ser bloqueado.

A9.4.3.0 d) La contraseña no debe aparecer en texto sin formato cuando se introduce

3. A.10 Criptografía

A10.1.1.0 a) Como regla general, solo los procedimientos de cifrado aprobados por la unidad firmante están permitidos (algoritmo de cifrado, tamaño de clave, administración de claves...).

4. A.11 Seguridad física y ambiental

4.1. A.11.1 Áreas seguras (Requisitos Identificación)

A11.1.2.0 g) Dentro de las instalaciones de la empresa, las identificaciones de la empresa deben ser usadas obligatoriamente en todo momento, por el personal interno, el personal externo y los visitantes.

A11.1.2.0 i) El personal no perteneciente a la empresa solo puede tener derecho de acceso o entrada a las instalaciones sensibles de la empresa mediante un acuerdo especial de confidencialidad o de conformidad con el principio de doble control, y ser siempre acompañados por el anfitrión.

4.2. A.11.2 Equipo (Política de escritorio limpio)

A11.2.9.0 a) Durante las ausencias de los lugares de trabajo, los documentos que contengan información CONFIDENCIAL o CONFIDENCIAL DE CLIENTE deben estar protegidos por una puerta de oficina cerrada y, además, deben estar bajo llave en espacios de almacenamiento o cajones. Esto también se aplica a los dispositivos de datos móviles.

A11.2.9.0 b) La protección de acceso al equipo debe activarse automáticamente al salir de la estación de trabajo.

5. A.12 Seguridad de la operación

A12.1.2.0 a) La configuración de los ajustes de configuración relevantes para la seguridad para los sistemas de TIC en particular solo puede ser cambiada por la Gestión de TIC responsable dentro de la Gestión de Cambios / Versiones e Incidencias.

6. A.13 Seguridad de las comunicaciones

A13.1.1.0 a) Las personas que no son empleados no deben operar sus propios sistemas dentro de la red corporativa.

A13.1.1.0 b) Los sistemas privados de los empleados no pueden, por regla general, ser operados dentro de la red corporativa.

A13.2.2.0 a) La información puede ser transmitida a terceros, si se ha llegado a un acuerdo de seguridad.

7. A.14 Adquisición, Desarrollo y Mantenimiento

Métodos vinculantes de T-Systems son:

- **PSA** (Privacy & Security Assements)
- **ESARIS** (Enterprise Security Architecture for Reliable Services)
- (**SE-, SM- and PM-Book**) System Engineering, System Management and Project Management Book

A14.1.1.0 a) Como regla general, los datos de la empresa deben almacenarse en sistemas TIC centralizados corporativos.

8. A.16 Gestión de incidentes de seguridad de la información

Los siguientes incidentes son incidentes de seguridad (esto también se aplica a casos sospechosos o tentativas de estos incidentes):

- Acceso o reenvío no autorizado de información
- Robo, pérdida o manipulación no autorizada de datos
- Robo, pérdida o manipulación no autorizada de hardware, sistemas o infraestructura
- Daño o destrucción de hardware, sistemas o infraestructura
- Infecciones virales extensas

A16.1.2.0 a) Los incidentes relevantes para la seguridad deben ser reportados inmediatamente al superior, al Group Situation Center y/o a Security Management.

9. A.18 Compliance

A18.1.4.0 a) Los empleados deberán restringir el manejo de datos personales (recopilación, tratamiento y uso) a la finalidad confirmada y permitida.

Gestión de la seguridad:

Comunicación de incidentes de seguridad a nivel internacional:

Group-Situation-Center@telekom.de

+8000 99 000 77

Buzón de Seguridad en T-Systems Iberia:

fmb.ts-ib-security-management@t-systems.com

+34 93 341 95 15