sepian

Seguridad Digital
de Andalucía

Guía JDA-GSTIC-2019-H001

Normativa de Seguridad TIC de la Junta de Andalucía: aspectos generales e índice.

Tipo de documento: Guía
Autor del documento: Unidad de Seguridad TIC Corporativa
Código del documento: JDA-GSTIC-2019-H001
Edición: 1
Categoría: Público
Fecha de elaboración: 12/2/2019

JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO EMPRESA Y COMERCIO

sedian Seguridad Digital de Andalucía

1 Introducción

La Política de Seguridad TIC de la Junta de Andalucía se materializa en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y su modificación por el Decreto 70/2017, de 6 de junio. El desarrollo de dicha Política se realiza, en virtud de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, en forma de resoluciones de la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía, así como mediante documentos técnicos, que se agruparán en las categorías de procedimientos y guías técnicas.

Los procedimientos describirán la secuencia concreta de actividades que permiten satisfacer las obligaciones contenidas en las normas. Las guías técnicas ofrecerán información sobre cómo actuar ante situaciones y tecnologías específicas. Ambos tendrán carácter de recomendaciones y serán desarrollados, por cada organismo o entidad, con arreglo a los ámbitos en materia de seguridad de la información que se establezcan.

2 Objeto y alcance

Esta guía repasa los ámbitos de desarrollo de la normativa de seguridad, describe la nomenclatura de los procedimientos y guías y recoge el catálogo actualizado de resoluciones, procedimientos y guías publicados hasta la fecha.

3 Ámbitos de Desarrollo

1. Acceso y uso de aplicaciones corporativas, servicios de Internet y otros recursos de uso colectivo o individual. Criterios de uso aceptable y seguro de los medios y recursos TIC.
2. Tratamiento seguro de la información y sus soportes. Aspectos relacionados con el almacenamiento, acceso, transmisión, distribución y destrucción de la información manejada, así como de sus soportes. Clasificación de la información, marcado y tratamiento.
3. Seguridad ligada al personal. Concienciación y formación sobre obligaciones y responsabilidades.
4. Gestión de incidentes de seguridad, registro de eventos y continuidad del servicio. Mecanismos para que los eventos relacionados con la seguridad sean detectados, notificados y tratados. Procedimientos de registro y análisis de la actividad. Mecanismos para contrarrestar el impacto sobre los procesos críticos de la organización derivado de catástrofes o fallos importantes relacionados con los sistemas de información y para garantizar la reanudación de la actividad.
5. Contratación y relaciones con terceros. Mantenimiento de la seguridad de los datos, las aplicaciones y los sistemas que sean objeto de tratamiento, desarrollo, suministro o administración por parte de terceros, en el marco de una contratación o cualquier otro tipo de vinculación o acuerdo entre partes.
6. Protección lógica de equipos, electrónica de red, comunicaciones y servicios. Mecanismos para disponer de una configuración segura en los dispositivos, prevenir y detectar ataques y reaccionar ante ellos.

7. Seguridad de las aplicaciones software. Criterios para incrementar la seguridad en en el software a lo largo de todo su ciclo de vida.
8. Protección física de equipos y acondicionamiento y protección de instalaciones. Operativa para evitar accesos físicos no autorizados a las instalaciones con equipamiento TIC y para prevenir circunstancias accidentales que puedan afectar a la actividad normal de la organización.
9. Caracterización y planificación de los sistemas. Caracterización de los sistemas a lo largo del tiempo, para adecuar las medidas de seguridad. Planificación de la evolución de dichos sistemas para mantener parámetros de seguridad adecuados.
10. Auditoría. Procesos para sustentar la confianza y las decisiones en materia de seguridad en análisis independientes, objetivos y basados en evidencias formales.

4 Nomenclatura de las Guías y Procedimientos

Los nombres de las guías de seguridad serán de la forma

JDA-GSTIC-AAAA-XYYY – Descripción

y los de los procedimientos de seguridad de la forma

JDA-PSTIC-AAAA-XYYY – Descripción

donde “AAAA” reflejará el año de publicación del documento, “X” será un dígito entre cero y nueve que codificará el ámbito normativo que desarrolla el documento (o la letra “H” para documentos de ámbito horizontal o genérico) e “YYY” será un identificador numérico secuencial dentro de cada ámbito, que se incrementará con cada documento.

La codificación de los ámbitos normativos (dígito “X”) será la siguiente:

0: Acceso y uso de recursos

1: Tratamiento seguro de la información y sus soportes

2: Seguridad ligada al personal

3: Gestión de incidentes de seguridad, registro de eventos y continuidad del servicio

4: Contratación y relaciones con terceros

5: Protección lógica de equipos, electrónica de red, comunicaciones y servicios

6: Seguridad de las aplicaciones software

7: Protección física de equipos y acondicionamiento y protección de instalaciones

8: Caracterización y planificación de los sistemas

9: Auditoría.

H: Documentación general u horizontal.

5 Índice de normativa

A fecha de publicación de esta guía, la normativa en vigor es la siguiente:

5.1 Resoluciones

- Resolución de 30 de septiembre de 2017, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se asignan las funciones de la Unidad de Seguridad TIC Corporativa (BOJA 193, de 6 de octubre).

- Resolución de 26 de enero de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre integración en el Centro de Seguridad TIC AndalucíaCERT (BOJA 26, de 6 de febrero).

- Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC (BOJA 141, de 23 de julio).

5.2 Procedimientos

Ninguno en este momento.

5.3 Guías

- Guía JDA-GSTIC-2019-H001 – Normativa de Seguridad TIC de la Junta de Andalucía: aspectos generales e índice.
- Guía JDA-GSTIC-2019-H002 – Ciberseguridad en el cambio organizativo.
- Guía JDA-GSTIC-2020-3001 – Denuncia de incidentes de seguridad TIC que puedan ser constitutivos de delito.