sedian

Seguridad Digital
de Andalucía

Guía JDA-GSTIC-2019-H002

Seguridad en el cambio organizativo

Tipo de documento: Guía
Autor del documento: Unidad de Seguridad TIC Corporativa
Oficina de Apoyo a la Seguridad TIC
AndalucíaCERT
Código del documento: JDA-GSTIC-2019-H002
Edición: 1
Categoría: Público
Fecha de elaboración: 12/02/2019

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

ÍNDICE

1 Introducción....3

2 Objeto y alcance....3

3 Desarrollo....4

3.1Sistemas de información....4

3.2Equipos....5

3.3Redes....5

3.4Personal....6

3.5Terceros....6

3.6Ubicaciones....7

3.7Cumplimiento....7

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, de carácter horizontal y no ligada a un ámbito concreto, agrupa consideraciones y buenas prácticas en materia de ciberseguridad a tener en cuenta ante cambios organizativos que impliquen divisiones o fusiones de organismos, migración de sistemas de información o traslados de personal.

No trata de ser exhaustiva, sino de resaltar aspectos que cobran particular importancia ante reorganizaciones y cambios grandes en los organismos.

3 Desarrollo

3.1 Sistemas de información

- Se debe evitar que queden sistemas huérfanos: todos los sistemas de información deben tener personas responsables asignadas.
- Puede aprovecharse para eliminar sistemas no usados ni mantenidos: la falta de actualización o mantenimiento de un sistema de información suele conducir a la exposición de vulnerabilidades.
- Sería conveniente plantearse, a medio plazo, la reconstrucción de sistemas obsoletos o su integración como módulos en otros.
- Se debe prestar atención a las integraciones y la interconexión entre sistemas. La Guía CCN-STIC 811 (Interconexión en el ENS) es una buena referencia. Las conexiones entre sistemas de información deben estar definidas, protegidas y monitorizadas.
- La migración de sistemas puede requerir accesos temporales para mantenimiento o corrección de errores desde el organismo original. Estos accesos deben ser aprobados, los mínimos necesarios, con el privilegio indispensable, y debe establecerse e implementarse un plazo de caducidad.
- Deben mantenerse actualizados los inventarios de sistemas de información (CMDB del organismo, inventario de sistemas de información ENS de la Unidad de Seguridad TIC Corporativa, CRIJA, inventario OCS…).

3.2 Equipos

- Puede producirse un cambio, llegada o salida de un número considerable de equipos de usuario. Sería conveniente:
  a) Controlar y registrar la salida de equipos y asegurarse, si procede, de que se limpian de los mimos los datos que no deban salir del organismo.
  b) Evaluar la necesidad de cifrado de discos en nuevos equipos.
  c) Registrar la distribución de equipos nuevos, con documentos de entrega firmados por los usuarios, que contengan las normas de uso aceptable.
  d) Asegurar el plataformado seguro de nuevos sistemas.
- La migración de servidores, probablemente en formato virtual, debe ser supervisada para que
  a) los sistemas dispongan de una configuración segura y con la funcionalidad mínima necesaria,
  a) se cambien las credenciales de acceso originales y se den de baja usuarios obsoletos o no necesarios,
  b) se apliquen las actualizaciones necesarias del sistema operativo y de los servidores de aplicaciones y
  c) se dispongan medidas de protección perimetral y contra código malicioso.

3.3 Redes

- Los accesos temporales para mantenimiento o corrección de errores ya mencionados anteriormente pueden requerir aperturas temporales en los cortafuegos y otros sistemas de protección del

perímetro. Se deben aplicar los mismos controles ya indicados: aprobación formal, acceso mínimo con privilegio indispensable y caducidad.

- Deben darse de baja las reglas de cortafuegos, entradas DNS, entradas en proxy inverso y redirector corporativos, accesos VPN y RADIUS y otras configuraciones relacionadas con sistemas de información, equipos o personal que salgan del organismo.
- Ante los cambios en redes y direccionamiento, deben actualizarse las herramientas corporativas de gestión de direccionamiento (actualmente GDIP). Esto, entre otras ventajas, facilita la gestión de incidentes por parte de AndalucíaCERT.

3.4 Personal

- Deben establecerse sobre los sistemas nuevos las responsabilidades en seguridad que determina el ENS.
- Es fundamental coordinarse con el servicio de personal (o equivalente) del organismo para que se notifiquen las entradas y salidas de personal, de modo que se puedan aprovisionar y desaprovisionar los recursos.
- Deben contemplarse los aspectos de concienciación en materia de ciberseguridad del personal que llegue al organismo.

3.5 Terceros

- Ante la revisión o modificación de contratos o encargos:

  a) conviene la revisión de las cláusulas en materia de ciberseguridad.

b) debe actualizarse la definición de responsabilidades en ciberseguridad, estableciendo los puntos de contacto en el organismo y el tercero.

c) debe revisarse la condición de encargados de tratamiento según el RGPD, si es de aplicación.

d) convendría hacer una evaluación de riesgo de terceros, como mínimo distribuyendo un cuestionario básico para evaluar la postura en ciberseguridad del tercero en los aspectos que sean de aplicación al contrato o encargo.

- Debe supervisarse la configuración segura de equipos del personal externo, y su correcta integración con los sistemas de seguridad del organismo.

3.6 Ubicaciones

- Los cambios de ubicación de equipos (nuevos edificios o centros de proceso de datos) deben ser revisados para garantizar que la nueva ubicación cumple los requisitos básicos en cuanto a control de acceso a las áreas, acondicionamiento y suministro y protección frente a incendios o inundaciones.

3.7 Cumplimiento

- En el marco del ENS se actualizarán, en lo que proceda, los inventarios, las asignaciones de responsabilidad, los análisis de riesgos y las declaraciones de aplicabilidad de los sistemas de información entrantes. Se revisarán, a la luz de la declaración de aplicabilidad, las medidas implantadas y las carencias que puedan existir. Se planificará la corrección de estas carencias.

- En lo tocante al RGPD y a la LOPD-GDD, se determinarán los tratamientos de datos personales nuevos y los salientes. Se actualizará en consecuencia el Registro de Actividades de Tratamiento. Se establecerán las asignaciones de responsabilidades necesarias. Se evaluará la necesidad de Evaluación de Impacto en Protección de Datos (o su existencia previa, en cuyo caso se revisará). Se actualizarán los análisis de riesgos y se determinarán las medidas a implantar para garantizar la protección de los datos.
- En virtud de la disposición adicional primera de la LOPD-GDD, las medidas a aplicar para garantizar la protección de los datos serán las del anexo II del ENS.
- Es recomendable que, en lo posible, el análisis de riesgos sobre los tratamientos de datos personales se realice en conjunción con el análisis de riesgos del sistema ENS que de soporte a dicho tratamiento.

Unidad de Seguridad TIC Corporativa

Oficina de Apoyo a la Seguridad TIC

AndalucíaCERT