Política de Seguridad de la Información del INE

SEG 001 11

Versión del documento: 1.2

Fecha: 16/04/2012

El Presidente del Instituto Nacional de Estadística

Gregorio Izquierdo Llanes

Status

Título	Política de Seguridad de la Información del INE
Nomenclatura	SEG-001-11
Versión	1
Fecha elaboración	29/11/2011
Distribución	Personal del INE y colaboradores externos
Elaboración	Área de seguridad TIC
Aprobación	Pendiente de aprobación por el Consejo de Dirección (con la firma del Presidente del INE en la portada)
Fecha de aprobación	18/4/2012
Fecha entrada en vigor	El día de la fecha de aprobación
Fecha de expiración	Sin expiración definida
Resumen	Directrices del INE para la Seguridad de la Información

Historia del documento

Versión	Fecha	Cambios	Autores
0.1	26/04/2011	Borrador interno.	Área de seguridad TIC
0.2	25/05/2011	Modificaciones del CTyS	CTyS
0.3	14/09/2011	Modificaciones del CD	CD
0.4	10/10/2011	Modificaciones de DDPP	DDPP
0.5	01/11/2011	Modificaciones de Subdirec-ciones	Subdirectores
1	29/11/2011	Informe Jurídico	
1.1	23/12/2011	Observaciones de los Sindicatos	
1.2	16/04/2012	Documento final	

INDICE

1 OBJETIVOS Y MISIÓN

1.1 Funciones del Instituto Nacional de Estadística (INE)

a. El Instituto Nacional de Estadística tiene encomendadas las funciones de coordinación general de los servicios estadísticos de la Administración General del Estado, la vigilancia, control y supervisión de las competencias de carácter técnico de los servicios estadísticos estatales, y las demás previstas en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

1.2 Misión y objetivos de la seguridad de la información.

a. El INE se apoya en las Tecnologías de la Información y las Comunicaciones (TIC) para mejorar la eficiencia de su funcionamiento y de los servicios que ofrece, haciendo que sus sistemas de información sean elementos claves para el desarrollo de su misión, por lo que uno de los objetivos del INE es la protección de los mismos. Con la presente Política de Seguridad, el INE reconoce expresamente la importancia de diseñar e implementar controles de seguridad en sus sistemas de información.

b. La misión de la Política de Seguridad del INE es establecer y comunicar las directrices en materia de seguridad en toda la organización para una adecuada protección de su información y sus servicios.

c. La seguridad estará presente en el ciclo de vida de los servicios y sistemas de información del INE, que pondrá los recursos necesarios para mantener los mecanismos de control que garanticen su cumplimiento.

d. Será objetivo de la Política de Seguridad garantizar la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información y los servicios.

e. El cumplimiento de la Política de Seguridad del INE aumentará la confianza de ciudadanos, empresas y administraciones en sus sistemas de información, reforzando y mejorando la imagen del Instituto.

1.3 Alcance

a. La Política de Seguridad se aplicará a todos los activos del INE, considerando como tales la información, los servicios, las personas y la infraestructura que los soporta: aplicativos, hardware, software de base, comunicaciones, todo tipo de soportes (incluido papel), locales, etc.

1.4 Marco legal de seguridad

a. La Política de Seguridad del INE, y toda normativa que de ella emane, cumplirá y será siempre coherente con la legislación vigente.

b. El INE está obligado a mantener el Secreto Estadístico, regulado por el Capítulo III del Título I de la Ley 12/1989 de la Función Estadística Pública. Por este motivo, el INE tendrá procesos continuos de mejora de las medidas de seguridad para proteger y amparar todos los datos de sus informantes.

c. Así mismo, el INE está obligado a implementar las medidas de seguridad para cumplir con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

d. El INE adoptará, en todas sus decisiones en materia de seguridad, los principios básicos enunciados en el artículo 4 del Esquema Nacional de Seguridad.

e. El INE, en función del resultado de un análisis de riesgos, aplicará, en los sistemas de información que así lo requieran, las medidas de seguridad previstas en el Esquema Nacional de Seguridad.

f. Toda la normativa que emane de esta Política de Seguridad será coherente con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y con aquellas directrices de seguridad que pueda dictaminar para el INE la Agencia Española de Protección de Datos (AEPD) de conformidad con el artículo 34.m. de dicha ley.

2 ORGANIZACIÓN Y RESPONSABILIDADES

2.1 El Presidente, El Consejo de Dirección y los órganos del INE

a. El Presidente del INE impulsará esta Política de Seguridad con su firma y con la divulgación a todos los empleados y a terceros implicados.

b. Será el Consejo de Dirección el encargado de aprobar o actualizar la política de seguridad a propuesta del Comité de Tecnología y Seguridad (CTyS).

c. Será el CTyS el encargado de mantener, proponer los cambios al Consejo de Dirección y hacer accesible a cada uno de los implicados la Política de Seguridad, así como toda la normativa que emane de ésta.

d. Será responsabilidad de cada Subdirección General y Delegación Provincial correspondiente, la implantación de las medidas de seguridad derivadas de la Política de Seguridad que le correspondan.

e. Será responsabilidad de cada Subdirección General y Delegación Provincial tener un catálogo actualizado de, como mínimo, todos los activos de los sistemas que formen parte de las funciones, objetivos o misión del INE.

f. Será la Subdirección General de de Tecnologías de la Información y las Comunicaciones (SGTIC) la encargada de facilitar, normalizar y centralizar la gestión de la información de dicho catálogo de activos.

g. Será responsabilidad de la Secretaría General tramitar los expedientes sancionadores que procedan, de acuerdo con la normativa vigente.

2.2 Responsables del Sistema.

a. Los sistemas de información del INE estarán catalogados y como mínimo tendrán asignados uno o varios de los siguientes roles:

- Responsable de la Información: es la persona (u órgano colegiado con responsabilidad unitaria identificable) que tiene la potestad de valorar la información conforme a los niveles de seguridad establecidos, que los activos que tratan dicha información estén debidamente catalogados, de establecer el nivel de riesgo aceptable y de aprobar el plan de seguridad resultante.

- Responsable del servicio: se encarga del buen funcionamiento y cumplimiento de los objetivos en los servicios o procesos de un sistema de información. Valorará el servicio desde el punto de vista de la seguridad, velando especialmente por la disponibilidad del servicio e indicando los acuerdos de nivel de servicio deseables para un adecuado desempeño de este.

- Responsable de sistemas: se encarga del buen funcionamiento de las infraestructuras y aplicativos de base. Se responsabilizará de implantar las medidas de seguridad en dichas infraestructuras y aplicativos de base, en el diseño de la arquitectura de red y comunicaciones, en la gestión de las configuraciones, en la realización de copias de respaldo de la información y de que la infraestructura soporte los acuerdos de nivel de servicio definido por el responsable del servicio.

- Responsable de desarrollo: se encarga de la lógica de funcionamiento y del cumplimiento de los requisitos de seguridad de los aplicativos en todo su ciclo de vida de desarrollo. Será responsable de tener una metodología de desarrollo reconocida y de cumplir los niveles de servicio.

- Responsable de seguridad de la información: se encarga de todos los aspectos que afecten a la seguridad de los sistemas de información. Colaborará con el resto de responsables en la categorización de los sistemas desde el punto de vista de la seguridad. Fomentará la formación, concienciación y comunicación de la seguridad. Coordinará la respuesta ante incidentes de seguridad y se encargará de la mejora continua de la seguridad y del análisis y gestión de los riesgos. Coordina con las Subdirecciones Generales y Delegaciones Provinciales la implantación de las medidas de seguridad así como la formación del catálogo de los activos de los sistemas que les correspondan.

- Responsable de auditoría: está autorizado a evaluar la implantación de todas las medidas de seguridad para los sistemas de información.

b. Excepto el rol de auditoría, la responsabilidad de todos estos roles siempre recaerá en personal interno del INE. Se podrán transferir ciertos trabajos pero nunca la responsabilidad.

c. Los roles definidos para un sistema de información siempre irán asignados a un cargo que se identificará con la persona que lo ostenta, debiendo estar claramente identificado en el catálogo.

d. Un sistema de información podrá tener cuantos otros roles se estimen necesarios para su adecuada asignación de funciones o responsabilidades.

e. Los sistemas de información tendrán asignados los roles definidos en la Política de Seguridad, siendo obligatorio que el responsable de seguridad y el auditor estén diferenciados.

f. Cuando un sistema de información del INE tenga flujos con otra organización deberá existir el rol de responsable externo para cada organización.

g. Siempre habrá un responsable de la seguridad física por cada instalación u oficina, encargándose de implantar las medidas de seguridad para proteger sus instalaciones

h. Los responsables organizarán la seguridad en entornos homogéneos de información, en los que puedan delimitarse con claridad los niveles de seguridad, con el propósito de facilitar la implantación de las medidas de seguridad.

i. Los responsables mantendrán categorizados, conforme a los niveles de seguridad establecidos, los sistemas de información.

j. Los responsables de la información transferirán, eliminarán, mitigarán o asumirán formalmente los riesgos de seguridad. De acuerdo a este tratamiento del riesgo, el responsable de seguridad estará autorizado para llevar a cabo las medidas de seguridad necesarias con la colaboración del resto de responsables.

k. Los responsables potenciaran la formación y la concienciación en seguridad de la información en el INE.

l. Deberá existir un procedimiento para la designación formal de todos los roles definidos en la presente política. La asignación de estos roles identificará a la persona, al cargo o puesto de trabajo y la fecha de su designación. Los posibles conflictos serán resueltos por un superior jerárquico común a las áreas en conflicto.

2.3 Todo el personal

a. Todo el personal que forme parte o colabore con el INE en el ejercicio de sus funciones tiene la obligación de conocer y cumplir la Política de Seguridad del INE y toda la normativa que emane de la misma y afecte a sus funciones. En particular, a conocer las "Normas de utilización de los equipos informáticos y de los sistemas de información del INE" y firmar la Declaración individual en materia de Secreto Estadístico.

b. Todo el personal del INE fomentará y facilitará la implantación de medidas de seguridad que mejoren la protección de la información, implicándose activamente en el incremento de la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información y los servicios.

c. Será obligación de todo el personal comunicar cualquier incidente de seguridad o el incumplimiento de la normativa de seguridad del INE a la persona o personas encargadas de la seguridad.

d. El incumplimiento por parte del personal de INE de la presente Política de Seguridad y la normativa que de ella emana será una responsabilidad personal. Para facilitar el conocimiento y cumplimiento de la presente política y sus normas derivadas, todo el personal tendrá derecho a formación y concienciación suficiente en materia de seguridad y el INE asume la obligación de impartirla y actualizarla como norma de actuación con carácter estratégico.

3 COORDINACIÓN Y RESOLUCIÓN DE CONFLICTOS DE SEGURIDAD

a. El CTyS se encargará de la resolución de conflictos que pueda haber entre los diferentes responsables, personas, sistemas y normativas, en lo relativo a la seguridad.

b. En aquellos conflictos que surjan entre unidades en las que haya un superior jerárquico común, será este quien decida si resolverlos o llevarlos al CTyS.

c. En caso de que en un sistema de información hubiera varios responsables para un mismo rol, éstos podrán elegir entre ellos un solo responsable, o hacerlo de forma coordinada entre los mismos.

4 ANÁLISIS Y GESTIÓN DE RIESGOS.

a. El Responsable de Seguridad de la Información realizará un análisis de riesgos para obtener un plan de seguridad con las medidas a implantar en los sistemas del INE, teniendo en cuenta las valoraciones en materia de seguridad de los responsables.

b. El INE implementará las medidas de seguridad en sus sistemas de información basándose en un análisis de riesgos.

c. Tanto el análisis como las medidas de seguridad se reevaluarán y actualizarán periódicamente.

d. El resultado del análisis y gestión de riesgos se formalizará en un documento que será firmado por el responsable de la información y conllevará la realización de un plan de implantación de medidas de seguridad.

5 DESARROLLO NORMATIVO DE SEGURIDAD

a. La Política de Seguridad del INE se desarrollará en diferentes normas, que serán aprobadas, actualizadas o derogadas por el CTyS, y posteriormente elevadas al Consejo de Dirección para su aprobación si procede.

b. Será responsabilidad del Área de Seguridad de la SGTIC, en coordinación con el CTyS, desarrollar la Política de Seguridad en diferentes normas.

c. De las normas de seguridad se derivarán procedimientos que las áreas afectadas deberán elaborar. Dichos procedimientos serán aprobados y divulgados por un responsable superior del área al que pertenezcan.

d. Previamente a la aprobación de cualquier procedimiento que emane de una norma de seguridad, el Área de Seguridad de la SGTIC y/o el CTyS hará una revisión y valoración del mismo, teniendo la potestad de rechazar su aprobación justificando los motivos.

e. Toda norma o procedimiento de seguridad llevará como mínimo su título, ámbito, área departamental, versión, responsable de redacción y aprobación, la fecha de aprobación, de entrada en vigor y vigencia, así como del visto bueno del Área de Seguridad de la SGTIC. Las normas contendrán una lista actualizada de todos los procedimientos derivados de las mismas.

f. La Política de Seguridad y todo su desarrollo en normas y procedimientos deberán ser accesibles a todo el personal de la organización, de acuerdo al principio de “la necesidad de conocer”.

g. Las medidas de seguridad que deriven de las normas y los procedimientos se realizarán bajo el principio de proporcionalidad, que relaciona la naturaleza de los datos y de los tratamientos con los riesgos a los que estén expuestos y el estado de la tecnología.

De la Política de Seguridad se derivarán normas que cubrirán al menos las normas básicas del Anexo I. La entrada en vigor de cada norma que se desarrolle, estará supeditada a la realización de los correspondientes planes de implantación.

6 ANEXO I. NORMATIVAS BÁSICAS DE SEGURIDAD

Las siguientes normas de seguridad deberán ser desarrolladas y posteriormente aprobadas por el CTyS y desarrollarse cumpliendo los siguientes mínimos.

6.1 Código de conducta

a. Todo el personal o colaborador del INE:

- Será formado e informado de sus deberes y obligaciones en materia de seguridad.
- Utilizará los recursos del INE exclusivamente para el cumplimiento de sus funciones.
- Cumplirá con el secreto estadístico, protegiendo la información y los sistemas contra cualquier uso indebido o no autorizado.

b. El INE podrá supervisar la actividad en los sistemas para verificar el cumplimiento de la Política de Seguridad y la normativa que derive de ella. Esa supervisión estará normalizada y será informada y avisada a los implicados.

Los representantes del personal, entre otros, serán informados para que puedan constatar que las posibles acciones de supervisión se realizan sin utilizar, en ningún caso, sistemas o programas que pudieran atentar contra los derechos constitucionales de las personas o contra los derechos del trabajador y éstos conocerán exactamente qué datos de su actividad se guardan en los sistema.

6.2 Autorizaciones

a. Todas las personas o procesos que accedan a los sistemas de información estarán debidamente autorizados, restringiéndose el acceso a las funciones permitidas.

b. Deberá existir un procedimiento de alta y baja de usuarios en la organización donde se incluya y se cumpla la normativa de seguridad. Las altas y bajas de personal se trasladarán con premura en los sistemas de información.

c. Todo nuevo sistema seguirá un procedimiento formal, con su debida autorización, asignación de responsable y catalogación de activos, previa a su entrada en producción.

d. Todo elemento físico o lógico requerirá autorización formal previa a su instalación o desinstalación en un sistema que está en producción.

6.3 Control de accesos

a. Todas las personas y procesos que accedan a los sistemas de información del INE deberán estar identificados de forma singular.

b. Las personas serán los responsables de custodiar cualquier medio que se les facilite para su identificación y autorización, ya que será personal e intransferible.

c. Las personas y las aplicaciones podrán únicamente acceder a los recursos estrictamente necesarios y autorizados para el cumplimiento de sus funciones.

d. Serán los responsables de la información y/o de los servicios los encargados de gestionar las autorizaciones (otorgar, eliminar y revisar) necesarias a los recursos de los que son responsables.

e. El control de accesos a los sistemas de información debe permitir, en función de la categorización de la información que maneja desde el punto de vista de la seguridad (confidencialidad, integridad...), registrar y auditar quién ha accedido y qué acciones ha realizado sobre dicha información.

6.4 Seguridad física

a. La infraestructura que sustenta los sistemas de información estará ubicada en áreas separadas, delimitadas por un perímetro de seguridad definido y adecuadamente protegido de amenazas físicas o ambientales.

b. Siempre habrá un responsable de la seguridad física por cada instalación u oficina, encargándose de implantar las medidas de seguridad para proteger sus instalaciones.

6.5 Operaciones y comunicaciones

a. Los entornos de producción estarán separados del resto de entornos (desarrollo, pruebas, etc.).

b. Los sistemas en producción garantizarán una seguridad por defecto, proporcionando la mínima funcionalidad necesaria, los controles de acceso adecuados, y un uso sencillo que evite realizar acciones peligrosas por desconocimiento.

c. Los sistemas en producción serán monitorizados en todo momento, analizadas sus vulnerabilidades y las actualizaciones aplicables, reaccionando con diligencia para gestionar sus riesgos.

d. Todo sistema de información del INE solo podrá usar activos autorizados por el INE y para la realización de las funciones que expresamente tiene encomendadas.

e. El tránsito de la información fuera de la organización se protegerá adecuadamente para garantizar su seguridad, de tal forma que cualquier flujo de información saliente o entrante de los sistemas de información del INE tendrá que cumplir la Política de Seguridad del INE.

f. Se asegurará el respaldo de la información perteneciente al INE, incluyendo la conservación a largo plazo en los casos que sea necesario. Se establecerán procedimientos para la recuperación de la información en los plazos mínimos que sean exigibles por los responsables de la información.

6.6 Adquisiciones, desarrollo y mantenimiento de sistemas

a. Se elaborarán normas de seguridad para el desarrollo de software en todo el ciclo de vida, de acuerdo a una metodología.

b. Todos los desarrollos pasarán por un ciclo de pruebas previo a la puesta en producción, para garantizar que cumplen los requisitos de seguridad y de integración con el resto de sistemas.

c. Las pruebas de aceptación de los sistemas no se harán con información real, a menos que se garantice que dicha información tiene el mismo nivel de protección que en explotación.

d. Las nuevas adquisiciones o cambios de versiones de los sistemas deben verificarse para garantizar que cumplen con los criterios de aceptación y las normas de seguridad del INE.

6.7 Gestión de incidencias y continuidad

a. El INE pondrá a disposición del personal un sistema para la comunicación y gestión de incidencias que afecten a la seguridad. Para ello el INE realizará una formación continua para que el personal se mantenga debidamente formado y concienciado en la detección, comunicación y gestión de posibles incidencias de seguridad. Todos los trabajadores serán responsables de la comunicación de cualquier incidencia que pueda afectar a la seguridad.

b. Todas las incidencias y medidas tomadas serán registradas.

c. Este registro y las evaluaciones que se hagan de los sistemas de información serán la base para la elaboración de los planes de mejora continua, en cuanto a la seguridad.

d. Se establecerán procedimientos que garanticen la continuidad de las operaciones de la organización frente a interrupciones del servicio.

6.8 Relaciones externas

a. Los servicios externalizados garantizarán el cumplimiento de las medidas de seguridad establecidas en la presente Política y las normas que emanen de ella. Para ello será obligatorio informar al responsable de la información, del servicio y de la seguridad de la información del INE que se coordinarán para establecer las medidas de seguridad adecuadas.El INE dispondrá de las medidas necesarias para poder ejercer su responsabilidad y mantener el control en todo momento. Deberá supervisar el cumplimiento de todos los requisitos de

seguridad que se deriven del análisis de riesgos o estén establecidos por convenio o contrato.

b. Cualquier cesión de información deberá estar sujeta, como mínimo, a los requisitos de seguridad establecidos en el INE. Para ello, se crearán acuerdos o contratos que garanticen el cumplimiento de los mismos. El incumplimiento de los acuerdos llevará asociado penalizaciones.

c. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

d. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable externo que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

6.9 Concienciación y formación

a. La normativa de concienciación y formación en seguridad incluirá a todo el personal del INE. Se formará al personal del INE de acuerdo a sus roles y funciones.

6.10 Otras normas

a. Conforme al principio de que la seguridad es labor de toda la organización, cualquier Subdirección General o Delegación Provincial del INE podrá proponer al CTyS la aprobación de una nueva norma de desarrollo o la modificación de una norma de seguridad existente.

7 ANEXO II. DEFINICIONES

a. Confidencialidad: requisito básico de seguridad que garantiza que solo las personas, entidades o procesos autorizados pueden conocer la información.

b. Integridad: requisito básico de seguridad que garantiza que la información no pueda ser modificada o alterada por personas, entidades o procesos no autorizados.

c. Disponibilidad: requisito básico de seguridad que garantiza que se puede acceder a la información y a los recursos o servicios que la manejan, conforme a las valoraciones o necesidades establecidas.

d. Autenticidad: requisito básico de seguridad que garantiza que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

e. Trazabilidad: requisito básico de seguridad que garantiza que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

f. Información del INE: Cualquier dato numérico, alfabético, gráfico, acústico o de cualquier otro tipo concerniente al INE. Dicha información puede estar en cualquier soporte (discos, memorias, papel, etc..) o en instalaciones fuera del INE y no por ello dejará de ser información del INE. Las medidas de protección de la información del INE dependerán de las valoraciones y de los riesgos aceptables definidos por los responsables.

g. Sistema de Información: es un conjunto de componentes interrelacionados que recogen, procesan, almacenan y distribuyen la información. Un sistema de información tiene la misma valoración para toda la información que procesa, dando como resultado la categoría de seguridad del mismo.

h. Servicio: conjunto de actividades con una finalidad concreta, que implica unos recursos y da unos resultados. La información que maneja un servicio será valorada por el responsable del mismo, teniéndose en cuenta la valoración del sistema de información al que pertenece la misma.

i. Ciclo de vida de la información: define las fases por los que pasa la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción). La Política de Seguridad de la Información del INE velará por la seguridad de la información en todas las fases.

j. Responsable externo: persona de contacto de entidad ajena al INE que se responsabiliza de las medidas de seguridad aplicables a información o servicios del INE. Este responsable, su cargo y la entidad a la que representa deberán aparecer en los acuerdos de nivel de servicio, contratos y catálogos del INE.

k. Usuario de los sistemas de información: cualquier persona o entidad externa al sistema que está autorizado para acceder al mismo y es responsable de custodiar las credenciales que le dan acceso.

8 ANEXO III. ACRÓNIMOS

a. INE: Instituto Nacional de Estadística

b. TIC: Tecnologías de la Información y las Comunicaciones

c. CTyS: Comité de Tecnología y Seguridad del INE

d. SGTIC: Subdirección General Tecnologías de la Información y las Comunicaciones del INE

e. AEPD: Agencia Española de Protección de Datos