Criterios generales de seguridad en los sistemas de información al servicio de la Administración de Justicia

Acuerdo del Pleno, de 13 de septiembre de 2007

El Pleno del Consejo General del Poder Judicial, en su sesión de 13 de septiembre de 2007, ha adoptado el siguiente acuerdo:

«Aprobar el documento denominado "Criterios generales de seguridad en los sistemas de información al servicio de la Administración de Justicia", que se incorporará como Anexo al "Test de Compatibilidad de los Sistemas Informáticos de Gestión Procesal", aprobado por el Pleno en su sesión celebrada el 12 de abril de 2007.»

1. ANTECEDENTES

La sensibilidad de la información jurisdiccional y la creciente importancia de los sistemas de información en la tramitación de los procedimientos judiciales son dos elementos que inciden en la relevancia de la seguridad de la información.

El Consejo General del Poder Judicial es consciente de la importancia de la seguridad en los sistemas de información al servicio de la Administración de Justicia, y en particular en lo relativo a los aspectos relacionados con el cumplimiento de la Ley Orgánica de Protección de Datos y el Reglamento de Medidas de Seguridad.

El Código de Conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia (Instrucción 2/2003, de 26 de febrero, BOE de 10 de marzo de 2003) y la realización de auditorías de seguridad en los sistemas de información al servicio de la Administración de Justicia (aprobada por el Pleno en sesión celebrada el 23 de julio de 2003), son algunas de las iniciativas abordadas y que reflejan esta importancia. Trabajo e iniciativas que han permitido concluir con la creación y declaración de los Ficheros de carácter personal dependientes de los Órganos Judiciales, efectuada por Acuerdo del Pleno del Consejo General del Poder Judicial de 20 de septiembre de 2006 (BOE de 12 de octubre de 2006).

En esa línea, la colaboración de las Administraciones Públicas competentes en la provisión de recursos y medios materiales (a las que se reconoce, en el citado acuerdo de 20 de septiembre de 2006, la cualidad de Encargados del tratamiento, al ser los responsables de los centros de tratamiento, locales, equipos, sistemas, programas, así como del personal técnico que interviene en el tratamiento) y de los usuarios (entendidos como todos los profesionales que prestan sus servicios en los órganos judiciales) es indispensable, dado que constituyen una parte clave en el nivel de seguridad y protección de la información.

El Consejo General del Poder Judicial, al amparo de lo dispuesto en los artículos 230.5 de la Ley Orgánica del Poder Judicial, 97.1 y 102.1 del Reglamento núm. 1/2005, de 15 de septiembre, de los Aspectos Accesorios de las Actuaciones

Judiciales, ha elaborado este documento que incluye un conjunto de medidas que permitan mejorar y/o homogeneizar (cuando proceda) el nivel de seguridad existente sobre los sistemas de gestión procesal. En este sentido, no debe ser interpretado como una lista exhaustiva sino como un marco de referencia (o modelo de seguridad) asociado a los requerimientos fundamentales relativos a la seguridad de estos sistemas, cuyo desarrollo, ejecución e implantación corresponde a las Administraciones Públicas competentes en la dotación de medios materiales, en su respectivo ámbito territorial. En atención a las peculiaridades y necesidades propias del Tribunal Supremo, dichas labores deberán ser llevadas a cabo por el Ministerio de Justicia en coordinación con el Gabinete Técnico de Información y Documentación del citado Alto Tribunal.

2. CRITERIOS BÁSICOS DE SEGURIDAD

MARCO NORMATIVO

Con carácter general, las tareas realizadas por las Administraciones Públicas competentes en la provisión de recursos y medios materiales en lo relativo a la gestión de la infraestructura tecnológica y sistemas de información al servicio de la Administración de Justicia, estarán basadas en un Documento de seguridad, de obligado cumplimiento para el personal con acceso a los datos de carácter personal de los Sistemas de Información de Gestión Procesal, que describirá las medidas de seguridad (organizativas y técnicas) puestas en marcha por las mencionadas Administraciones Públicas. El Documento de seguridad, adecuadamente formalizado e implantado, contendrá los aspectos contemplados en los artículos 8.2 y 15 del Reglamento de Medidas de Seguridad.

Además, las Administraciones Públicas competentes elaborarán (y ejecutarán) un Plan de acción detallado de las medidas a adoptar para dar cumplimiento al expresado Documento de seguridad, así como las que permitan asegurar la ejecución de los criterios técnicos y organizativos que se señalan a continuación.

Una copia de dicho Documento de Seguridad y del Plan de acción serán remitidos a la Comisión de Informática Judicial del Consejo General del Poder Judicial.

MEDIDAS TÉCNICAS

2.1.1. Configuración de infraestructura tecnológica

- Los servidores en los que se ubiquen los sistemas de gestión procesal deberán prevenir riesgos asociados a accesos no autorizados derivados de la existencia de aplicaciones y/o sistemas no relacionados con aspectos jurisdiccionales (por ejemplo: sistemas de información soporte a las áreas,

departamentos o consejerías de educación, agricultura,…). Para ello implantarán las medidas y medios tecnológicos necesarios para garantizar la independencia, unicidad y protección de los datos.

- Las plataformas tecnológicas soporte a los sistemas de gestión procesal (lo que también incluye sistemas operativos y bases de datos y, cuando proceda, configuraciones en puestos clientes) estarán configuradas de acuerdo a guías y estándares de securización adecuadamente formalizadas y actualizadas. La posibilidad de realizar cambios sobre esta configuración estará restringida, previa aprobación, a un reducido número de usuarios (personal técnico especializado). Existirá un registro de cambios (que incluye la instalación de parches u otro tipo de soluciones facilitadas por el proveedor).

- Con carácter general, existirá una separación efectiva entre los entornos de desarrollo y producción.

2.1.2. Identificación y autenticación

Los sistemas de información (y software de base) dispondrán de mecanismos de identificación y autenticación que prevengan los accesos no autorizados basados en la existencia de un identificador unívoco de usuario y contraseña, o mediante la utilización de certificado digital o algún otro mecanismo de protección suficientemente probado, dado el estado de la tecnología en cada momento y las características de la información a proteger.

- En el caso de sistemas de identificación basados en usuario y contraseña, la creación de un nuevo usuario se realizará atendiendo al procedimiento establecido y previa autorización del responsable competente. La asignación de contraseña inicial será aleatoria y, en cualquier caso, pre-expirada. Los sistemas permitirán asociar períodos de validez a los identificadores de usuario de forma que fuera de ese rango de fechas el sistema prevenga la autenticación a través de dicho identificador.

- Las contraseñas de los usuarios generales (es decir, sin privilegios especiales asociados a tareas de administración) deberán satisfacer, al menos, los siguientes criterios:

    - Calidad. La contraseña tendrá, al menos, una longitud mínima. Adicionalmente, deberá evaluarse la posibilidad de exigir reglas adicionales de complejidad en base al grado de madurez de los controles de seguridad implantados.

    - Cambio periódico. Los usuarios deberán cambiar periódicamente sus contraseñas (por ejemplo, cada tres meses). Existirá un histórico de contraseñas que prevenga la re-utilización de la contraseña anterior. En cualquier caso, los sistemas permitirán el cambio autónomo de contraseña por parte de los usuarios aún cuando no sea como consecuencia del cambio periódico previsto.

  En cualquier caso, las contraseñas se almacenarán en las aplicaciones y sistemas, de forma encriptada.

  Los usuarios con privilegios de administración considerarán mecanismos adicionales de seguridad y protección, en relación a las claves, para prevenir accesos no autorizados a través de sus identificadores.

- Los sistemas de gestión procesal y la infraestructura tecnológica soporte dispondrán de mecanismos de bloqueo de los usuarios. En particular, considerarán al menos las siguientes casuísticas:

    - Bloqueo automático por intentos reiterados de acceso fallidos (por ejemplo: 6 intentos).

    - Bloqueo automático asociado a intentos de acceso fuera del intervalo de fechas de validez de un identificador de usuario.

    - Bloqueo manual por parte del Administrador.

  Se recomienda el bloqueo automático por no acceso en un determinado período de tiempo (por ejemplo: tres meses) con objeto de regularizar las cuentas activas en el órgano judicial.

El desbloqueo de un determinado identificador se realizará, con carácter general, de forma manual por parte del personal autorizado al efecto.

- No se permitirá, con carácter general, el acceso a los sistemas a través de usuarios genéricos. Esto incluye, sin limitarse a, aquellos que, por defecto, son creados en el proceso de instalación de los sistemas y aplicaciones. En cualquier caso, deberá asignarse un responsable de aquellos usuarios genéricos que se estimen necesarios.
- En el caso de sistemas basados en identificación digital, solo se podrán utilizar certificados digitales autorizados por la Administración competente. Las aplicaciones deberán consultar las listas de certificados revocados correspondientes antes de permitir el acceso.
- Igualmente podrán ser utilizados sistemas biométricos como método de identificación y autentificación.

2.1.3. Control de acceso

- Perfiles y roles. El acceso a los sistemas de información de gestión procesal estará basado, habitualmente, en perfiles y roles. Estos mecanismos determinarán, en base a las necesidades autorizadas de los usuarios, dos aspectos fundamentales:
    - Las funcionalidades (de las previstas por el sistema de información) a las que podrán acceder (con frecuencia basado en puntos de menú)
    - Los datos a los que deberán tener acceso. Para ello permitirá, sin perjuicio de las capacidades de búsqueda y explotación de la información, segmentar los usuarios en base a criterios organizativos como los órganos judiciales, secciones, etc. a las que están adscritos. Será posible aplicar mecanismos adicionales de protección basados en expedientes o asuntos concretos (por ejemplo, a través de listas de control de acceso)

Con relación a las sustituciones, los sistemas de información tenderán a considerar el principio de herencia. En particular, se pretende que sea

posible asociar (y revocar) a un sustituto los asuntos en los que participara el sustituido.

- Bloqueo por inactividad. Tras un período de inactividad (por ejemplo: 30 minutos) se activará un mecanismo de bloqueo que evite la suplantación del usuario en momentos en los que su equipo no esté atendido.
- Con carácter general, los privilegios de administración en los propios equipos de los usuarios estarán restringidos. Es decir, se prevendrá la instalación de software no autorizado en los equipos de los usuarios por parte de los mismos.

2.1.4. Registro de accesos

- Los accesos a los expedientes o asuntos mantendrán un registro que incluya, al menos, la identificación del usuario, la fecha y hora en la que se realizó el acceso, el tipo de acceso y si ha sido autorizado o denegado.
- Se definirán pistas de auditoría y seguimiento de actividad en los sistemas operativos y gestores de bases de datos. El seguimiento estará, especialmente, orientado a las tareas de administración del sistema. La configuración del sistema prevendrá la eliminación y/o desactivación de estos logs.

2.1.5. Redes y comunicaciones

- La red en la que se ubiquen sistemas y a la que accedan los usuarios de los sistemas de información al servicio de la Administración de Justicia estará protegida de accesos no autorizados.
- El acceso a otras redes estará protegido a través de cortafuegos (firewalls) u otro tipo de mecanismos que aseguren en las comunicaciones a través de las redes locales un nivel de protección suficiente frente a las amenazas de terceros. Este apartado también incluye la existencia y actualización periódica de mecanismos de protección frente a virus u otros códigos maliciosos. Los dispositivos de red (como encaminadores – routers -) también estarán adecuadamente securizados y protegidos.

- La conectividad remota (“teletrabajo”) a través de redes públicas de datos estará adecuadamente protegida, en línea con las soluciones tecnológicas de seguridad existentes en cada momento.
- Igualmente, la conectividad a través de redes inalámbricas requerirá la configuración (con los mecanismos actualmente disponibles o los que puedan existir en el futuro) segura de la misma.
- La administración de forma remota de los equipos y servidores, en caso de ser necesaria, se realizará mediante canales seguros.

MEDIDAS ORGANIZATIVAS

2.1.6. Organización de seguridad

- Las funciones y responsabilidades asociadas a la administración y explotación de los sistemas y, en particular, a la gestión de la seguridad de la información estarán formalmente aprobadas y asignadas a personas concretas. Estas funciones pueden incluir, sin limitarse a:
    - Mantenimiento y actualización del marco normativo.
    - Instalación y configuración segura de sistemas.
    - Elaboración de informes asociados al análisis de logs.
    - Monitorización y resolución de incidencias.
    - Formación y concienciación de usuarios
    - Seguimiento de accesos en sistemas operativos y gestores de bases de datos y, en términos generales, accesos en tareas de administración de sistemas.
    - Seguimiento de los servicios contratados en lo que afecte a la administración y explotación de sistemas de gestión procesal.
    - Realización de copias de respaldo

2.1.7. Ubicación física de los servidores y equipos

- La ubicación física de los servidores y dispositivos de comunicaciones (electrónica de red, firewalls,…) prevendrá el acceso no autorizado y se

realizará atendiendo a un análisis de riesgos. En particular, el acceso estará restringido de forma efectiva (por ejemplo, a través de puertas cerradas con llave) a personal autorizado. Existirá, por lo tanto, un registro de estos accesos.

- Medidas de protección medioambiental. Las salas en las que se ubiquen los servidores tendrán sistemas de detección y extinción de incendios. La temperatura de la sala estará en los rangos de operación definidos por los fabricantes (habitualmente a través de sistemas de aire acondicionado). Por último, en caso de riesgo de daños por agua (tuberías, instalaciones aéreas de aire acondicionado refrigeradas por agua, …) existirán sistemas que mitiguen o prevengan los daños en los equipos y servidores.
- Garantía de suministro eléctrico. Existirán mecanismos que aseguren el suministro eléctrico no sólo a los servidores en los que se ubiquen los sistemas de gestión procesal sino también a los diferentes elementos necesarios para asegurar la conectividad de los usuarios a los servicios críticos.
- Como orientación general y en la medida que resulte posible, los equipos de los usuarios no estarán ubicados en zonas de paso o distribución.

2.1.8. Formación y concienciación de usuarios

- Se desarrollarán mecanismos de formación y concienciación específicamente orientados a la seguridad de la información (complementarios a los que el Consejo General del Poder Judicial pudiera arbitrar). Habitualmente estarán basados en cursos presenciales y/o a través de e-learning, y tendrán carácter periódico. Entre las áreas que pueden incluir figuran:
    - Conocimiento del marco normativo en lo que sea relevante a la operativa de los diferentes usuarios.
    - Funciones y responsabilidades de los usuarios.
    - Confidencialidad y privacidad de las contraseñas (u otros mecanismos de autenticación)

- Criterios de conservación y almacenamiento de los ficheros generados por los usuarios (incluyendo la eliminación de los ficheros temporales)
- Políticas de bloqueo de pantalla y puesto de trabajo despejado de papeles y soportes con información sensible.
- Condiciones de trabajo fuera de las oficinas habituales.

2.1.9. Seguimiento de accesos

- Revisiones periódicas de usuarios autorizados. Periódicamente (por ejemplo, cada tres meses) se realizará, por parte de los usuarios competentes, una revisión de los usuarios autorizados para identificar usuarios con acceso indebido potencial a los sistemas. A tal efecto, los sistemas permitirán obtener los usuarios activos en los sistemas para poder contrastar dicha lista con los usuarios autorizados e identificar excepciones.
- Registro de usuarios con privilegios de administración. Existirá un registro de usuarios con privilegios de administración (asociados a tareas habituales de mantenimiento y explotación de sistemas o como consecuencia de accesos de emergencia de usuarios de desarrollo a producción). Este registro incluirá el identificador autorizado, el período de validez, el responsable de la autorización y las tareas a realizar por el mismo. Este registro podrá servir como fuente de contraste con el log de los sistemas.

  El Consejo General del Poder Judicial considera este apartado especialmente relevante por los riesgos de seguridad inherentes a la función de administración de sistemas y por la constatación que, en ocasiones, estas tareas son realizadas por personal externo (por ejemplo, adscrito a empresas privadas con las que la Administración Pública tiene suscrito un contrato) en el que el índice de rotación puede ser elevado.

  El mantenimiento actualizado de este registro (conjuntamente con la trazabilidad de las acciones realizadas por estos usuarios) debería permitir un seguimiento más efectivo de las tareas que se realizan.

  El registro de usuarios con privilegios de administración estará a disposición de la Comisión de Informática Judicial.

2.1.10. Copias de respaldo

- Se realizarán copias de respaldo, en base a los procedimientos formalizados y de acuerdo a un calendario previsto, que aseguren, en caso de ser necesario, la recuperación de la información anterior a producirse la incidencia. El calendario determinará el período de retención y los controles asociados a la rotación de los soportes.
- Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en el que se encuentren los equipos y servidores (con medidas de restricción de acceso suficientes). El traslado se realizará preservando la confidencialidad de la información.

2.1.11. Contratos de prestación de servicios.

- Las Administraciones Públicas competentes en la provisión de recursos y medios materiales mantendrán un registro actualizado de las organizaciones prestadoras de servicios que pudieran tener acceso a información de gestión procesal. En este sentido, estarán identificados para cada organización las funciones asociadas, las personas con acceso, …

- Las Administraciones Públicas arbitrarán mecanismos de seguimiento y control de las empresas o entidades que prestan asistencias técnicas de forma que sea posible conseguir un nivel asimilable de control a la realización interna de las funciones. Los sistemas de seguimiento y control pueden estar basados en estándares, como por ejemplo ITIL. En cualquier caso, las cláusulas contractuales considerarán acuerdos de confidencialidad que prevalecerán aún cuando haya finalizado el contrato.

2.1.12. Procesamiento paralelo por parte del usuario final

- Las Administraciones Públicas arbitrarán mecanismos que permitan el mantenimiento y actualización de las aplicaciones asociadas a la gestión procesal. Asimismo, existirán registros de incidencias o de solicitudes de

mantenimientos evolutivos y se realizará un seguimiento de la resolución y/o cierre de las mismas.

- Por otra parte, se restringirán los privilegios de instalación de programas diferentes a los previstos en las maquetas de equipos ofimáticos definidas. Estas aplicaciones podrán ser instaladas exclusivamente por los administradores autorizados, que en todo momento seguirán las normas señaladas en el Documento de seguridad. Eventualmente, se realizará un seguimiento para identificar software no corporativo instalado en los equipos de usuario. Las excepciones que se identifiquen y el análisis de las mismas permitirán arbitrar las medidas de sensibilización y concienciación aplicables. En todo momento los datos gestionados con las herramientas ofimáticas o aplicaciones distintas a las previstas, seguirán los mismos criterios de seguridad, que los establecidos para las aplicaciones corporativas. En ningún caso se crearán ficheros de carácter personal distintos a los declarados atendiendo a los requerimientos de la Ley Orgánica de Protección de Datos.

- Los sistemas de gestión procesal dispondrán de mecanismos de seguimiento de la frecuencia de acceso de los diferentes identificadores de usuario al sistema. Es decir, permitirán identificar usuarios que no han accedido durante un determinado período de tiempo al sistema de gestión procesal.

2.1.13. Revisiones periódicas

- Al menos cada dos años se revisará el grado de implantación del modelo de seguridad sobre los sistemas de información e infraestructura tecnológica al servicio de la Administración de Justicia y el nivel de madurez de los controles. El análisis tendrá un alcance completo y, como consecuencia del mismo, se derivará además del diagnóstico, un seguimiento de las acciones previstas asociadas a la mejora continua en el nivel de seguridad y control. Además, cuando proceda, incluirá propuestas asociadas a la resolución de los aspectos susceptibles de mejora.

SECRETARIO JUDICIAL

El Secretario Judicial, en el marco de las competencias contempladas en el artículo 454 de la Ley Orgánica del Poder Judicial, velará por la observancia en las oficinas judiciales de los criterios generales de seguridad establecidos en el presente documento.

RESPONSABLES DE SEGURIDAD

Las Administración Pública competente, en su respectivo ámbito territorial, designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el correspondiente Documento de seguridad.

Dicha designación será comunicada a la Comisión de Informática Judicial del Consejo General del Poder Judicial,

AUDITORÍA

Los Sistemas de Información al servicio de la Administración de Justiciase someterán a una auditoría que verifique el cumplimiento del presente documento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años.

Corresponde al Consejo General del Poder Judicial o a la Administración Pública competente, cuando así lo haya manifestado, la práctica y ejecución de la citada auditoría.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente documento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará sus conclusiones a la Comisión de Informática Judicial, así como a la Administración Pública competente, a fin de que se adopten las medidas correctoras adecuadas

Los informes de auditoría quedarán a disposición de la Agencia de Protección de Datos.

PLAZOS DE EJECUCIÓN

Las Administraciones Públicas competentes deberán adoptar las medidas que a continuación se relacionan en los plazos especificados:

Comunicar a la Comisión de Informática Judicial la designación del Responsable de Seguridad, así como de la confección del registro de organizaciones prestadoras de servicios, en Diciembre de 2007.

Enviar a la Comisión de informática Judicial el Documento de Seguridad así como el denominado Plan de acción, en Enero de 2008.

Llevar a cabo la Auditoria de seguridad reseñada en el presente documento, durante el primer trimestre de 2009.