INFORME DISPOSICION TRANSITORIA CUARTA DEL REAL DECRETO 1671/2009, DE 6 DE NOVIEMBRE, POR EL QUE SE DESARROLLA PARCIALMENTE LA LEY 11/2007, DE 22 DE JUNIO, DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS

ÍNDICE

1 INTRODUCCIÓN

La disposición transitoria cuarta del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, sobre la adaptación de sedes electrónicas indica que "*En tanto no se aprueben los Esquemas Nacionales de Interoperabilidad y de Seguridad, la creación de sedes deberá ir acompañada de un informe en el que se acredite el cumplimiento de las condiciones de confidencialidad, disponibilidad e integridad de las informaciones y comunicaciones que se realicen a través de las mismas*".

Dado que ni el Esquema Nacional de Interoperabilidad (ENI) ni el Esquema Nacional de Seguridad (ENS) ha sido publicados, se elabora el presente informe para dar cumplimiento a la mencionada disposición transitoria cuarta mediante la adecuación en el Ministerio de Educación de los tres principios de la seguridad de la información, esto es, confidencialidad, disponibilidad e integridad. Se toma como referencias:

- Las normas ISO 27000
- La Ley Orgánica 15/1999 del 13 de diciembre

2 CONFIDENCIALIDAD

La norma ISO 27001 define la confidencialidad como: “el a*cceso a la información por parte únicamente de quienes estén autorizados*”. En el mismo sentido la norma ISO/IEC 13335-1:2004 la define como "*la característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados*”.

Como consecuencia tanto la información transmitida entre un emisor y uno o más destinatarios o el tratamiento de la misma por el propio usuario ha de ser preservada frente a terceros.

Para proteger la confidencialidad de la información desde el Ministerio de Educación se han definido los siguientes controles:

1. **Confidencialidad en el tratamiento de la información**, la cual se logra a través de las siguientes medidas:

    a. El desarrollo y la aplicación de las normas de funciones y obligaciones del personal en materia de seguridad de la información.

    b. La adecuación de la información a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

    c. El desarrollo y la aplicación de los acuerdos de confidencialidad con terceros implementados tanto en los pliegos de cláusulas de los contratos administrativos como de forma independiente a las empresas suministradoras.

    d. El desarrollo y la aplicación del control de acceso a la información realizado por identificadores únicos de usuarios.

    e. El proceso de gestión de derechos de acceso mediante la utilización de roles y perfiles.

    f. El desarrollo y la aplicación del control del registro de actividad de los usuarios implementado a través de herramientas de IDS/IPS

    g. El desarrollo y la aplicación del borrado seguro de la información a través de herramientas automatizadas y regladas de acuerdo con los estándares de seguridad

2. **Confidencialidad en la comunicaciones** a través del uso de:

    a. Conexiones cifradas por medio del protocolo SSL

    b. Certificado de Sede electrónica (www.sede.educacion.gob.es)

3 DISPONIBILIDAD

La norma ISO 27001, interpreta el principio de disponibilidad como: "*acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran*". En el mismo sentido la norma ISO/IEC 13335-1:2004 indica que la disponibilidad es "*la característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada*".

En el Ministerio de Educación se han definido los siguientes controles:

1. Para poder disponer de la información frente amenazas externas provenientes de la utilización de medios de comunicación se han establecido las siguientes medidas:

    a. Dispositivos de bloqueo/autorizador de comunicaciones (Firewall). Dichos dispositivos previenen de ataques como pueden ser Denegación de Servicio.

    b. Monitorización de la actividad del uso de la red que pudiera afectar a la disponibilidad de la información o los sistemas que la gestionan.

2. La tolerancia a fallos en la disponibilidad del servicio es proporcionada por la mediación de:

    a. Centro alternativo de proceso de información donde se encuentran replicados los datos y los servidores para su utilización en los sistemas críticos del Departamento.

    b. Política de copia de seguridad de la información y su recuperación en caso de corrupción o desastre.

    c. Utilización de sistemas de almacenamientos tipo RAID 1 y 5, que previenen error de pista en discos duros.

    d. Redundancia de los elementos de comunicaciones y servidores web que ofrecen los servicios al usuario

    e. Contratos de acuerdo de nivel de servicio (ANS) con proveedores de material informático.

    f. Sistema de alimentación ininterrumpida (SAI) contra las posibles contingencias y caídas de suministro eléctrico, además de los sistemas contraincendios y mantenimiento climático de la infraestructura informática.

3. Mantenimiento y revisión de los equipos informáticos llevado a cabo por los técnicos encargados de los mismos.

4 INTEGRIDAD

La norma ISO 27001, interpreta el principio de integridad como: "el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso". En el mismo sentido la norma ISO/IEC 13335-1:2004 indica que la integridad es "*la propiedad/característica de salvaguardar la exactitud y completitud de los activos*".

La integridad vela porque no se realicen modificaciones no autorizadas de la información además de que sea consistente entre sí misma y respecto de la situación real externa.

Para satisfacer lo anteriormente descrito en el Ministerio de Educación se han determinado los siguientes controles:

1. Control de modificaciones y solicitud de accesos a la información:

    a. El desarrollo y la aplicación del control de acceso a la información realizado por identificadores únicos de usuarios.

    b. Gestión de las autorizaciones a través de la gestión de incidencias.

    c. Registro de actividad de los usuarios.

2. Seguridad de la identidad del usuario e integridad de la información tratada por el mismo mediante el empleo de certificados digitales y firma electrónica de acuerdo con el artículo 21 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

5 ANEXO I - GLOSARIO

TERMINO	DEFINICIÓN
ANS	Acuerdo de Nivel de Servicios
Borrado	Eliminación de la información de un sistema de información, sus equipos de almacenamiento y demás periféricos. El borrado debe ser sistemático y garantizar que la información no es recuperable por medio alguno. Por si fuera posible recuperar información de equipos teóricamente borrados, los soportes de información no deberían ser reutilizados sino con información del mismo nivel o superior.
Control de acceso	Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
Copia de respaldo	Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo, como ser discos duros, CDs, DVDs o cintas magnéticas (DDS, Travan, AIT, SLR, DLT y VXA).
Cortafuegos	Sistema formado por aplicaciones, dispositivos o combinación de estos, encargados de hacer cumplir una política de control de acceso en las comunicaciones entre dispositivos según una política de seguridad existente.
Datos de carácter personal	Cualquier información numérica, alfabética, gráfica, fotográfica y acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
Firewall	Elemento de seguridad físico (hardware) o lógico (software) que tiene por objetivo regular los servicios que pueden pasar a través de él.
Identificación	Proceso que permite a un sistema reconocer unívocamente a un activo, ya sea éste una persona, una máquina o un proceso. Ese sistema puede ser tanto un servidor físico como una base de datos o una aplicación.
IDS	Sistema de Detección de Intrusiones
IEC	International Electrotechnical Commission
Intrusión	Acción de soslayar o violar los mecanismos de seguridad instalados y los procedimientos de seguridad establecidos con objeto de atacar a un sistema.

IPS	Sistema de Prevención de Intrusiones
ISO	Organización Internacional de la Estandarización
RAID	Redundant Array of Independent Disks o conjunto redundante de discos independientes
SAI	Sistema de Alimentación Ininterrumpida
SLA	Service Level Agreement (véase ANS)
Tratamiento de datos	Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, consulta, utilización, modificación, cancelación, bloqueo o suspensión
Vulnerabilidad	Estimación de la exposición efectiva de un activo a una amenaza.