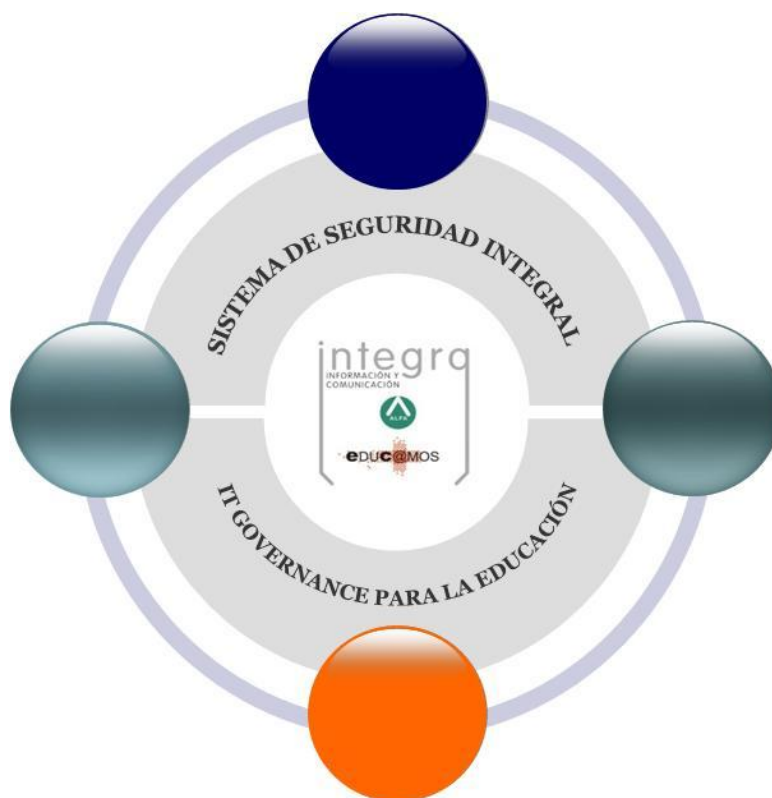


Modelo de IT-Security para la Educación: Soluciones Tecnológicas Avanzadas de Seguridad



Elaborado por: Enrique Laborde Malo de Molina (Integra) y Antoni Bosch i Pujol (IAITG)
Documento: Integra C20111221 V1.1

Fecha: 21 de Diciembre, 2011

1.0 Introducción

Exponíamos en nuestro artículo [Bases del Modelo de IT-Security & IT-Governance para la Educación](#) que una implantación ordenada y organizada de las TIC está relacionada con la mejora en la calidad educativa, y que un futuro ya no muy lejano apunta en esta dirección: educación inseparable de las TIC implica calidad, y a la necesidad de un proceso o un modelo que gobierne, gestione y apoye los objetivos a cumplir.

Resaltábamos a su vez que una educación de calidad a través de las TIC exige asegurar que se lleven a cabo las medidas necesarias para proteger a todos los usuarios – y de manera prioritaria al menor – de los riesgos en Internet y asegurarnos de que disponemos de los medios suficientes para que desde el perímetro del Centro no se cometan delitos informáticos.

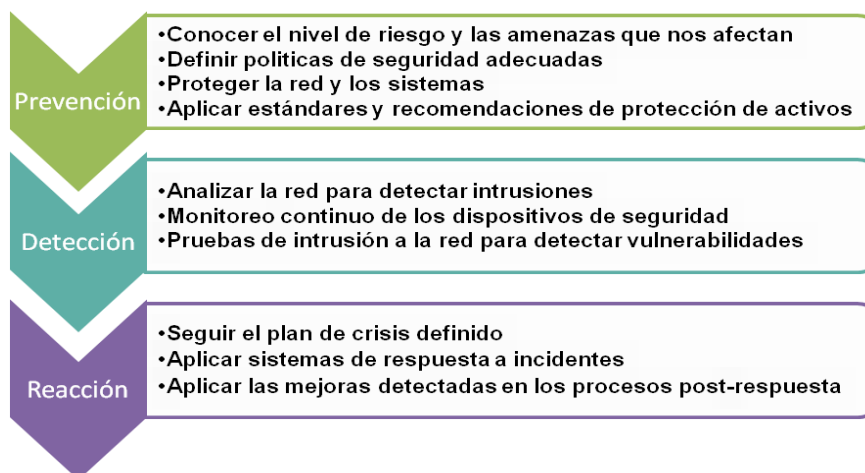
En este artículo presentamos una serie de Soluciones Tecnológicas Avanzadas de Seguridad para complementar nuestro Sistema de Seguridad Integral, ya en marcha en Integra, y para definir un **Modelo de IT-Security para la Educación**.

2.0 Marco de Seguridad por fases: Prevención, Detección, Reacción

Antes de abordar cualquier fase de seguridad en un Centro, es necesario tener una visión clara de la organización e identificar su actividad habitual, de su infraestructura y el estado en que se encuentran los equipos informáticos, y hacer un estudio inicial de vulnerabilidades tecnológicas y jurídicas. Esto nos permitirá detectar el nivel de riesgo y la tipología de amenazas que pueden afectar a los equipos y a toda la infraestructura tecnológica.

También es necesario ver la actividad habitual del Centro en cuanto a hábitos del tráfico de la información y los usos de toda la red, para ver qué políticas hay que configurar en los equipos para mejorar la seguridad de forma preventiva. En este punto, sin duda alguna, es necesaria la colaboración con el personal del Centro, ya que los ajustes a aplicar pueden afectar al Centro.

Entonces, y basándonos en estándares de seguridad, podremos definir una serie de recomendaciones específicas para incrementar la protección de los activos del Centro. Adicionalmente, conociendo el estado normal y de actividad del centro, nos permitirá identificar patrones anómalos de tráfico.



Las actividades preventivas definidas en la figura de arriba son necesarias para llevar a cabo tareas de detección y posibilitar un análisis de la infraestructura de la red que permita detectar

vulnerabilidades e intrusiones. Esta actividad se desarrolla de manera continua; no es posible analizar la red una vez para confiar en su seguridad. Por tanto, para garantizar la seguridad, es necesario añadir una capa de valor adicional a los equipamientos de detección con un servicio de monitorización continua de la red. A partir de este punto, es posible detectar incidencias de seguridad e intrusiones no autorizadas en tiempo real.

El siguiente paso es subsanar la situación. Para ello, es necesario disponer de un equipo altamente especializado y tener una metodología ya implantada. Esto permitirá, de forma eficaz y eficiente, aplicar los mecanismos de respuesta ante incidencias y reaccionar con el mínimo impacto al servicio, recuperando la normalidad del servicio en el menor tiempo posible.

Una vez conseguida la recuperación, se desarrollará un proceso de análisis para intentar deducir que ha ocurrido, y obtener pruebas de ello si es posible. Una vez finalizado este proceso, analizar qué aprendizaje se obtiene del incidente y revisar los procesos que sea necesarios mejorar. En las siguientes secciones enmarcaremos este proceso de prevención, detección y reacción en un **Modelo de IT-Security para la Educación**.

3.0 Modelo de IT-Security para la Educación: Seguridad Técnico-Jurídica

Antes de concluir un estudio de implantación de las TIC en cualquier ámbito y sobre todo aquellas iniciativas basadas en el uso de Internet, y en particular si se trata de un centro donde hay menores, es necesario considerar una serie de políticas de seguridad tanto en el ámbito jurídico como tecnológico. Esto implica dotar al centro de los protocolos, formación y herramientas para mantener la seguridad y el conocimiento para gestionar correctamente la información.

Es por estos motivos que **Integra Información y Comunicación** ha estado desarrollando una iniciativa global de seguridad, desde la primavera de 2010, que a día de hoy consta de las siguientes fases:

- Asesoría en el Correcto Tratamiento de la Información
- Asesoría Tecnológica
- Formación en los riesgos de uso de Internet
- Infraestructuras de control y seguridad

La evolución de estas iniciativas se enmarcan en el **Modelo de IT-Security para la Educación de Integra**, que como se ha indicado en [documentos anteriores](#), es un proceso de calidad en la implantación de las TIC, con las siguientes características:

- Es incremental "Bottom-Up"
- La base es el cumplimiento de las normativas y leyes vigentes que afectan al entorno educativo
- La creciente implantación aumenta la seguridad y la calidad
- Culmina con una fase de Certificación que así lo verifica

La presentación gráfica del **Modelo de IT-Security para la Educación de Integra** se aprecia en la siguiente figura.

Implantación de IT-Security & Evolución del Modelo de IT-Governance para Centros Docentes



Para definir el modelo de manera global, quedaba pendiente de concretar las fases de las Soluciones Tecnológicas Avanzadas de Seguridad, que son:

- Asesoría Tecnológica
- Formación en el correcto tratamiento de la Información
- Monitorización
- Auditoría de Seguridad

3.1 Modelo de IT-Security: Seguridad Tecnológica – Asesoría Tecnológica

La parte tecnológica es la clave del éxito o del fracaso en el ámbito de la Seguridad del Centro y requiere:

- Un Análisis metódico de las infraestructuras del Centro
- El Conocimiento, el alcance y los límites de dichas infraestructuras, sus vulnerabilidades y sus defectos, conforme a los usos previstos por el centro, es indispensable para establecer las medidas de control y gestión necesarias para el funcionamiento óptimo y seguro de los recursos del centro.
 - Hacer un estudio técnico y el despliegue de las medidas de control necesarias para conocer el estado de uso y vulnerabilidad de sus infraestructuras
 - Poner de manifiesto los verdaderos agujeros de seguridad que tiene el centro,

Las medidas técnicas correctoras a implantar que, unidas con las recomendaciones de carácter legal, los procedimientos y demás medidas jurídicas, nos permiten “blindar” al centro de cualquier riesgo técnico-jurídico, objetivo último del RIS.

3.2 Modelo de IT-Security: Traspase de Conocimiento con Formación ad hoc

Uno de los retos principales que conlleva la introducción de las TIC en el ámbito educativo es ser capaces de dar respuesta a las necesidades de formación de los usuarios. El motivo siendo que la complejidad tecnológica de las mismas infraestructuras que soportan el uso de las TIC que utilizamos requiere muchas veces de medidas suplementarias, revisiones constantes de su

estado y, sobretodo, del conocimiento de todos los usuarios para utilizar la tecnología que ponemos en sus manos – y que por cierto – afecta al centro por la responsabilidad “in vigilando” con respecto a la actividad de todos los involucrados en el tratamiento de la información: padres, profesores, alumnos, administradores...

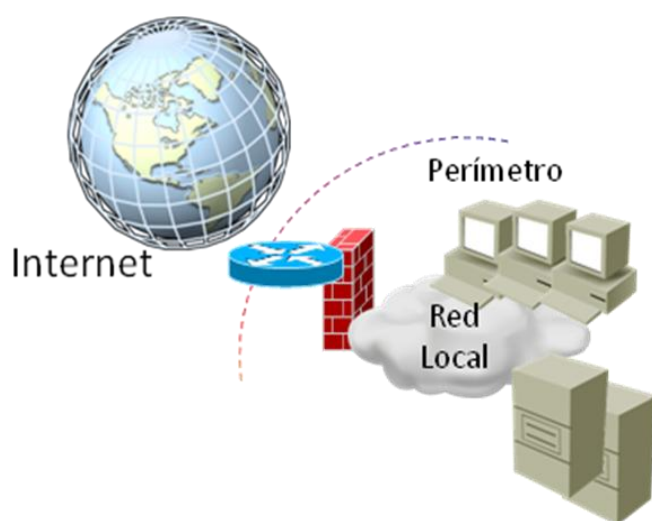
Es por ello imprescindible potenciar los avances tecnológicos junto con aquellos procesos que garanticen la seguridad integral de las TIC, tanto en la implantación como en el uso (y el mal uso). Para hacer esto es necesario formar a todo el personal que tenga acceso al tratamiento de la información en la plataforma, tanto en el centro como en la familia:

1. **Formación incluida en el RIS:** Documento esencial y básico que protocoliza todos los procedimientos que profesores y responsables deben conocer para cumplir la Ley y proteger a los menores.
2. **Mix de Formación:** Un programa exclusivo de formación que combina:
 - a. Talleres presenciales y formación on-line para el personal del centro (administradores, profesores y tutores).
 - b. Charlas y formación on-line especialmente diseñado para las familias que usan el módulo de comunicación de EDUC@MOS de nuestros colegios.

3.3 Modelo de IT-Security: Seguridad Avanzada con Monitorización

La monitorización se realiza a modo Outsourcing, basándonos en la solución de **IAITG**, y con la instalación de equipos en el centro, previa realización de una auditoría de seguridad inicial. Esto nos permitirá entender las condiciones de contorno de Seguridad del centro.

Los equipos instalados nos protegerán del exterior y son el punto de acceso de nuestra red a Internet. Es de suma importancia, desde el punto de vista de la continuidad del servicio, evitar incidencias en estos equipos, ya que si sufren algún problema importante, pueden dejar a la red sin servicio.



También son importantes desde un punto de vista de la seguridad, ya que un ataque puede causar la interrupción del servicio, sobre todo en caso de que se logre acceder a los routers o cortafuegos de la red (Ataque de denegación de servicio, DOS).

Existen otro tipo de ataques que se pueden cometer, tales como la redirección del tráfico de la red. En este caso el atacante accede a todo el tráfico que estamos recibiendo en la red sin que el centro tenga constancia de ello. Incluso existe el riesgo de que se hagan cambios en la configuración interna de la red con la que se obtendría información confidencial y de forma inadvertida por el centro.

Seguridad Integral



Por tanto, el equipamiento perimetral es el componente de la arquitectura de seguridad esencial y que nos proporciona servicios de:

- Cortafuegos (bloquea las comunicaciones no autorizadas y permite las autorizadas).
- Antivirus Perimetral. Se encarga de revisar todos los contenidos de navegación web, e-mail y el tráfico entrante y saliente de la red. Elimina también Spam y malware.
- Filtrado y control de acceso a contenidos.
- VPN (comunicaciones seguras en, conexión con terceros, entre centros, ...).
- IPS/IDS (sistemas de prevención y detección de intrusiones)

En la prestación del servicio, es importante destacar la monitorización continua de los equipos en gestión. Esto incluye el seguimiento de las alarmas generadas y la posibilidad de actuar de forma proactiva ante un posible incidente.

Algunas características de la monitorización y de las posibles actuaciones resultantes se describen a continuación:

- Monitorización 12 x 5 (12 horas x 5 días a la semana) de los dispositivos en gestión
- Actualizaciones y cambios en las políticas de los dispositivos
- Escalado a soportes técnicos internos especializados y de fabricantes
- Soporte por correo-e y refuerzo del cumplimiento de la política de seguridad de los Centros
- Servicio de análisis de 'logs' (ficheros históricos) en caso de malfuncionamiento o detección de problemas
- Informes gráficos mensuales sobre el estado de los dispositivos monitorizados
- Mantenimiento en caso de avería

3.4 Modelo de IT-Security: Seguridad Avanzada con Auditoría de Seguridad

La auditoria de seguridad propuesta por **IAITG** consta de una revisión del estado de los equipos visibles desde Internet, así como un informe detallado sobre los hallazgos. Incluye además una auditoria técnica y recomendaciones de securización de todos los dispositivos de seguridad al Centro. Entre estos, se destacan:

- Análisis de la configuración
- Identificación de las medidas correctoras necesarias
- Presentación de dichas medidas al administrador de red, si procede
- Implementación de las medidas técnicas
- Prueba del correcto funcionamiento

De forma periódica también se llevaran a cabo auditorias de seguridad interna, con el posterior informe detallado. El objetivo de esta auditoría es verificar el estado de la seguridad de los diferentes sistemas de información del Centro, tales como:

- Servidores (ordenadores que formen parte de una red y proveen servicios a otros ordenadores llamados clientes) que prestan servicios de DNS, DHCP, Directorio Activo, Servidor FTP, Servidor Correo-e, Proxy, Routers y Switches, Maquinas Linux, Servidor web (Apache, IIS, genérico), Servidores Windows 20XX, Bases de Datos, etc.
- Análisis de la configuración de los equipos
- Identificación de las medidas correctoras necesarias
- Presentación de las medidas al administrador de red, si procede
- Implementación de las medidas técnicas
- Prueba del correcto funcionamiento

Tal como se ha comentado anteriormente, también son necesarios los análisis de forma periódica para garantizar la correcta gestión de la seguridad. Gracias a estos análisis podremos reforzar la seguridad de la organización o centro en:

1. Detección de potenciales intrusiones (vulnerabilidad de los sistemas)
2. Aseguramiento del correcto funcionamiento de los dispositivos clave de la seguridad
3. Refuerzo de la política corporativa de seguridad y garantía de cumplimiento
4. Garantiza el correcto mantenimiento de los equipos de seguridad

4.0 Conclusiones del Modelo de IT-Security

Una implantación de las TIC de calidad requiere que los usuarios conozcan el uso de la tecnología y que también obtengan el conocimiento necesario para el correcto tratamiento de la información y que dispongan, además, de un conjunto con soluciones de protección global que asegure un entorno de seguridad.

Por lo tanto, con la puesta en marcha de las TIC en los centros e instituciones, es una necesidad fundamental disponer de un modelo de integración de las TI, *con el concepto de seguridad como base*, que nos permita maximizar la calidad y operar correctamente. En este documento, y para dar una respuesta global a este reto, hemos definido las Soluciones Tecnológicas Avanzadas de Seguridad del **Modelo de IT Security para la Educación de Integra**.