# Arriskuak neurtu, informatika segurtasuna kontrolatu

**Informazio sistemetan segurtasun arazoak zehaztu eta kontrolatzea derrigorrezkoa da. Baita Lanbide Heziketako zentroetan ere.**

# Medir los riesgos, controlar la seguridad informática

**Definir y controlar los problemas de seguridad en los sistemas de información resulta vital. También en los centros de Formación Profesional.**

**Iñigo Balerdi Urrestarazu**

**(Tolosaldea IKTko dinamizatzailea)**
**(dinamizador TIC's en el instituto Tolosaldea)**

**Komunikazio sareak eta informazio sistemak dira gaur egun LHko institutuetako aktibo nagusiak. Informatika eta sareak leku guztietan agertzen dira, bere garaian ura eta elektrizitatearekin gertatu zen moduan. Hori dela eta, informazio sistemen eta komunikazio sareen segurtasuna da gure institutuetan gehien kezkatzen duen arazotariko bat.**

## Segurtasun politika baten beharra

Ordenagailuekin lan egiten dugunean, informatika erabiltzaileok nahi batzuk izaten ditugu. Esate baterako, ordenagailua pizten dugunean guztia bezperan utzitako moduan egotea. Edo mezuak jasotzailearengana zuzen iristea, atxikitako datuak galdu gabe. Edo ikasguneko datu basera jotzerakoan, ikasleen notak eta faltak egiazkoak izatea.

Neurri egokiak hartu ezean, baliteke nahi edo itxaropen horiek ez betetzea. Informazioa (intranet, ikasgune aplikazioa, elkartuz, posta...) zentroetako aktibo nagusia dela kontuan hartuz, hori babestea izango da egin beharreko zeregin nagusia. Baina zein alor ziurtatu behar dira? Nagusienak hemen zehazten dira:

- **Konfidentzialtasuna:** baimendutako erabiltzaileek soilik izango dute informaziorako sarbidea.
- **Segurtasuna:** datuak benetakoak izatea; hau da, asmo txarreko erabiltzaileren batek ez dituela aldatu egiaztatzea.
- **Eskuragarritasuna:** zergatik ziurtatu aurreko alorrak informazioa ez baldin badago eskuragarri? Beraz, informazioak eskuragarri egon beharko du beharrezkoa den guztietan eta denbora guztian.

**Las redes de comunicación y los sistemas de información se han convertido a día de hoy en los principales activos de los institutos de FP. La informática y las redes son recursos que aparecen por todas partes, como en su día ocurrió con el agua y la electricidad. Debido a esto, se ve que la seguridad de los sistemas de información y la de las redes de comunicación es uno de los problemas que mas preocupan en nuestros institutos.**

## Necesidad de una política de seguridad

Los usuarios de la informática depositamos unas expectativas cuando trabajamos con los ordenadores. Por ejemplo, que al encender el ordenador, todo este tal y como se dejo la víspera. O que los mensajes lleguen al receptor correcto, sin perdida de los datos adjuntos. O que al acceder a la base de datos de ikasgune, las notas y faltas de los alumnos sean las verdaderas.

Si no se toman las medidas adecuadas puede que no se cumplan dichas expectativas. Sabiendo que la información (intranet, aplicación ikasgune, elkartuz, correo,...) es uno de los principales activos de los centros, su securizacion y protección será una de las tareas primordiales a llevar a cabo. ¿Pero que aspectos se han de asegurar? Aquí se detallan los principales:

- **Confidencialidad:** A la información solo accederán los usuarios autorizados.
- **Integridad:** Que los datos accedidos sean los auténticos, es decir, tener la certeza de que ningún usuario malintencionado los haya modificado.
- **Disponibilidad:** ¿Para que asegurar los aspectos anteriores si la información no esta disponible? Por lo tanto. la información deberá estar accesible todas las veces que sea necesario y durante todo el tiempo.

## Arriskuen kudeaketa

Gero eta mehatxu zerrenda (birusak, arrak, erabiltzaileen hanka-sartzeak...) gehiago dagoen arren, gertatzeko dauden aukerak edo arriskuak hartu behar dira kontuan. Agian, erabiltzaileen utzikeriagatik edo hornidura elektrikoarengatik arazoak izateko arrisku gehiago dago birusek eraginda baino. Beraz, segurtasuna arriskua kudeatzeko tresna gisa ulertzen da. Segurtasun politika zehaztu baino lehen, arrisku-azterketa egin behar da.

Erasoek ondorio bat baino gehiago izan ditzakete: ekonomikoak (zentroko jarduera ez aurrera eta ez atzera geratzeagatik eta lehengo egoerara itzuli beharrak eraginda), lege ondorioak (gure ekipoetatik erasoak jasan behar izan dituzten enpresen salaketak), zentroaren izen onean eta ospean eragina...

## IssGunea sortzea

Arrisku azterketa egiteko eta segurtasuneko politika zehazteko, institutuko informazio sistemaren segurtasun gunea (issGunea) ezarri da Tolosaldea institutuan. Gune hori zuzendariek, idazkariak, kalitate arduradunak, IKT dinamizatzaileak eta sare administratzaileak osatzen dute. Batzorde horrek ondorengo zereginak ditu:

- Informazioa ondo erabiltzeko errespetatu beharreko arauak zehaztu, gainbegiratu eta zabaltzea; baita erantzukizunak zehaztea ere.
- Business Continuity Plan (BCP) bat zehaztu eta ezartzea.
- Informazioaren segurtasunean gertakariak gainbegiratu eta aztertzea.
- Informazioaren segurtasuna nabarmen hobetzen duten ekintzak zehaztu eta onartzea.
- Institutuko baliabide informatikoak kudeatzea.

## Informazio sistemen segurtasun kudeaketa

Tolosaldean, ISO 17.799 (egun, ISO 27.001) estandarraren aholkuak ari gara jarraitzen, segurtasun politikaren definizioa aurrera eramateko. Informazioaren segurtasuna modu eragingarrian kudeatzeko tresna da. Informazio sistemen segurtasunaren eta segurtasun beharren kudeaketaren ikuspegi orokorra eskaintzen du.

ISO 17.799 gaian ahalegin, ezagutza eta adituen bizipenei esker lortutako kontrol gida zabala (baina sakona) da. Segurtasun arau auditagarriak izatea da helburua. ISO 17.799 hamar nagusitasunetan egituratzen da, eta horiek, era berean, 36 kontrol helburutan (kontrolak ezartzerakoan lortu nahi diren helburuak) eta 127 kontroletan (praktikak, prozedurak eta arrisku maila murrizten duten mekanismoak) bereizten dira.

Estandar aholkuei jarraituz, gaur egun, institutuak segurtasun formalaren politika du zehaztuta. Erabiltzailearen kontratua ere zehaztu da (erabiltzailearen eskubideak eta betebeharrak). Aktiboen sailkapena egin da (informazioa eta hardwarea). Erabiltzaileak segurtasun digitalean gaitzen dira. Sareko administrazioko eragiketak jarraitzen dira. Informaziorako sarbideak zehaztuta daude. Institutuko zerbitzu kritikoak gelditu egiten baldin badira, zentroa sistema errekuperatzeko prest egongo da, arrisku planaren bitartez. Eta legea bete egiten da. Datuak Babesteko Legea (LOPD), Internet Legea (LSSICE), Jabetza Intelektualeko Legea (LPI). IssGunearen menpe dago guztia.

## Web estekak

http://www.cert.org
http://www.iso-17799.com
http://www.17799.com
http://www.delitosinformaticos.com

## Gestión de riesgos

Aunque la lista de amenazas (virus, gusanos, despistes de los usuarios,..) van aumentando, es la probabilidad o riego de que ocurran lo que se debe de tener en cuenta. Quizás son más peligrosos y hay más riesgo de que se produzcan los problemas ocasionados por la dejadez del usuario o los problemas con el suministro eléctrico, que los producidos por los virus. Por lo tanto, se entiende la seguridad como la gestión de riesgos. Antes de definir la política de seguridad hay que hacer un análisis de riesgos.

Las consecuencias de los ataques pueden ser económicas (las surgidas por la paralización de la actividad del centro y por la vuelta al estadio anterior), legales (denuncias de empresas que han sufrido ataques desde nuestros equipos), repercusión en la fama y buen nombre del centro,...

## Creación de issGunea

Para la realización del análisis de riegos y para la definición de la política de seguridad, se ha creado en el instituto Tolosaldea el espacio para la seguridad de los sistemas de información del instituto, informazio sistemaren segurtasun gunea (issGunea). Este gune o foro es un comité multidisciplinar compuesto por director, secretaria, responsable de la calidad, dinamizador de las TIC's y administrador de red. Los quehaceres de este comité son los siguientes:

- Definir, revisar y difundir las normas que hay que respetar para el manejo correcto de la información; además de definir responsabilidades.
- Definir e implantar un Bussines Continuity Plan (BCP).
- Revisar y supervisar los incidentes en la seguridad de la información.
- Definir y aceptar aquellas acciones que mejoren sustancialmente la seguridad de la información.
- Gestionar los recursos informáticos del instituto.

## Gestionar la seguridad de los sistemas de información

En Tolosaldea estamos siguiendo los consejos del estándar ISO 17.799 (hoy en día ISO 27.001) para llevar a cabo la definición de la política de seguridad. Es una herramienta para gestionar de modo eficiente y eficaz la seguridad de la información. Nos ofrece una visión global de la gestión de la seguridad de los sistemas de información y de las necesidades de seguridad.

La ISO 17.799 es una extensa (pero no profunda) guía de controles, obtenidas gracias al esfuerzo, conocimiento y experiencia de expertos en el tema. El objetivo es tener un conjunto de normas de seguridad auditables. La ISO 17.799 se estructura en diez dominios, y estos a su vez en 36 objetivos de control (objetivos que se quieren lograr al implantar los controles) y 127 controles (practicas, procedimientos y mecanismos que reducen el nivel de riesgo).

Siguiendo los consejos de estándar, hoy en día el instituto tiene definida una política de seguridad formal. También se ha definido un contrato de usuario (derechos y obligaciones del usuario). Se ha hecho la clasificación de activos (información y hardware). Se cualifica a los usuarios en seguridad digital. Se procedimentan las operaciones de administración de red. Los accesos a la información están definidos. Si los servicios críticos del instituto se paran, el centro esta preparado para la recuperación del sistema mediante un plan de contingencia. Y se cumple la ley; Ley de Protección de Datos (LOPD), Ley de Internet (LSSICE), Ley de la Propiedad Intelectual (LPI). Todo esto bajo la batuta de issGunea.

## Enlaces web

http://www.cert.org
http://www.iso-17799.com
http://www.17799.com
http://www.delitosinformaticos.com

**Arazoak gertatzeko arrisku gehiago dago erabiltzailearen utzikeriagatik, birusarengatik baino**

**Hay más riesgo de que se produzcan problemas por dejadez del usuario que por los virus**