Comité de Seguridad Informática

comite.seguridad@ceu.es

LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

GUIA DE SEGURIDAD INFORMÁTICA PARA LA FORMACIÓN Y SENSIBILIZACIÓN DE USUARIOS FINALES

¿POR QUÉ LA SEGURIDAD INFORMÁTICA?

- PORQUE SI UN SISTEMA DE INFORMACIÓN DEJA DE FUNCIONAR O FUNCIONA MAL, PUEDE OCASIONAR GRAVES RIESGOS MATERIALES O DE IMAGEN A LA FUNDACIÓN.
- LA SEGURIDAD INFORMÁTICA APORTA NORMAS Y PROCEDIMIENTOS OPERATIVOS PARA QUE ESTOS RIESGOS NO OCURRAN, O AL MENOS SE MINIMICEN.

OBJETIVOS GENERALES DE LA SEGURIDAD INFORMÁTICA

PRESERVAR LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD

- CONFIDENCIALIDAD: proteger la información contra accesos o divulgación no autorizados.
- INTEGRIDAD: garantizar la exactitud de la información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- DISPONIBILIDAD: asegurar que los recursos informáticos y la información puedan ser utilizados en tiempo y forma requeridos. Bajo el punto de vista de seguridad, la disponibilidad se refiere a su posible recuperación en caso de desastre

MARCO LEGAL

- LA SEGURIDAD INFORMÁTICA ESTÁ RESPALDADA POR:
  - LA NORMATIVA LEGAL NACIONAL
  - LA NORMATIVA DE LA UNIÓN EUROPEA

refiriéndose ambas a la protección de la información y de los sistemas informáticos, entre las que cabe señalar:

- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).
- Ley 34/2002 de Servicios de la Sociedad de la Información y del Correo Electrónico (LSSICE)
- Real Decreto 428/1993
- Ley 22/1987 de Propiedad Intelectual
- Ley sobre Protección Jurídica de Programas de Ordenador
- Real Decreto 1332/94
- Directivas europeas 95/46/CE y 97/66/CE
- Real Decreto 994/1999

Comité de Seguridad Informática

comite.seguridad@ceu.es

CLASIFICACIÓN DE LA INFORMACIÓN

- SIN CLASIFICAR: es aquella información que puede ser conocida o utilizada sin ninguna autorización por cualquier persona.
- DE USO INTERNO: es la información que, sin poder ser publicada, puede ser conocida o utilizada por todos los usuarios y cuya divulgación o uso no autorizado podría ocasionar pérdidas leves y asumibles por la Fundación.
- CONFIDENCIAL: es la información que sólo puede ser conocida y utilizada por un grupo de usuarios que la necesiten para realizar su trabajo y cuya divulgación y uso no autorizado podría ocasionar pérdidas significativas, tanto materiales como de imagen
- SECRETA O RESERVADA: es toda aquella información que sólo puede ser conocida y utilizada por un grupo muy reducido de usuarios, generalmente la Dirección y a quien ésta autorice a conocerla y manipularla. Su divulgación o uso no autorizado podría ocasionar graves pérdidas materiales o de imagen.

PROTECCIÓN DE LA INFORMACIÓN

IMPORTANTE:

La principal regla de protección es que la información clasificada sea conocida o utilizada sólo por personas autorizadas y siempre por razones de necesidad debido a tener que trabajar con dicha información.

Y EN GENERAL:

- La información clasificada se guardará con medios físicos y lógicos adecuados.
- Si la información es confidencial se deberá guardar bajo llave permanentemente.
- Si la información es secreta deberá permanecer guardada en una caja fuerte de seguridad.

PROTECCIÓN FÍSICA

OBJETIVO:

Evitar riesgos potenciales de ataque, sabotaje, pérdidas, robo o daño a los sistemas de información, ya sean accidentales o intencionados, que puedan ocasionar la interrupción total o parcial de las actividades.

ACCIONES A TOMAR:

- Se tendrán en cuenta los aspectos de seguridad relacionados con locales, instalaciones, personas y cosas que rodean a los sistemas de información.
- Se cuidarán las acciones que puedan producir daños por fuego, inundación, explosión, disturbios de personas, o cualquier forma de desastre natural o provocado.
- Se respetarán los sistemas de control de accesos, los sistemas de detección y los sistemas de emergencia y evacuación.

Comité de Seguridad Informática

comite.seguridad@ceu.es

PROTECCIÓN LÓGICA

OBJETIVO:

Proteger la información que se procesa, almacena y transmite para que sea siempre utilizada de forma autorizada, sólo por razones de trabajo y evitar las acciones que puedan provocar su alteración, borrado o divulgación no autorizada, ya sea de forma accidental o intencionada. En base a ello, los usuarios estarán sujetos a:

- Los sistemas de información sólo pueden ser usados para llevar a cabo actividades relacionadas con el trabajo.
- El uso de dichos sistemas para otro fin que no sea éste, debe ser aprobado previamente por la Dirección.
- El uso no autorizado de los sistemas de información, es una violación que atenta contra la seguridad y puede ser sancionado

IDENTIFICACIÓN DE USUARIO

ES LA CLAVE QUE PERMITE A UN USUARIO ACCEDER DE FORMA INDIVIDUAL A UN SISTEMA DE INFORMACIÓN. CADA IDENTIFICADOR DE USUARIO ESTÁ ASIGNADO A UNA SOLA PERSONA, QUE SERÁ RESPONSABLE DE LAS ACTIVIDADES REALIZADAS POR ÉL.

OBJETIVO

Establecer y aprobar la utilización de cada sistema por los distintos usuarios, asegurando que cada identificador de usuario es único y sólo puede ser asociado a una sola persona, de forma que el usuario sea identificado por el sistema cuando acceda a él.

AUTENTICACIÓN DE USUARIOS

OBJETIVO:

Asegurar que un usuario es quien dice ser cuando accede al sistema.

La autenticación se hace mediante la CONTRASEÑA (password)

que verifica inequívocamente la identidad del usuario, constituyendo de esta forma el principal sistema de protección.

¡Cuidado¡ la contraseña es información clasificada.

Comité de Seguridad Informática

comite.seguridad@ceu.es

USO DE LA CONTRASEÑA (password)

- Tiene que ser secreta y no compartida con nadie.
- No puede ser visualizada en la pantalla mientras se teclea.
- No puede ser escrita o almacenada en claro.
- No debe ser trivial o predecible.
- Tendrá una longitud mínima de 6 caracteres.
- Tendrá al menos un carácter numérico y otro alfabético.
- No empezará ni terminará por un número.
- No tendrá más de dos caracteres iguales consecutivos.
- Será cambiada, al menos, cada 60 días, o 30 días en caso de usuarios con privilegios o autoridad.
- No se volverá a utilizar hasta después de, al menos, 12 cambios.
- No contendrá el identificador de usuario como parte de la misma.
- Se guardará en un lugar muy seguro, o mejor aún, se sabrá de memoria.

PROTECCIÓN DE LA INFORMACIÓN DEL SISTEMA

CONSTITUYE UN OBJETIVO PRIMORDIAL DE LA SEGURIDAD INFORMÁTICA , ASEGURAR LA INTEGRIDAD DE LA INFORMACIÓN DEL PROPIO SISTEMA

PROTECCIÓN DE LA INFORMACIÓN DE USUARIO

CADA INFORMACIÓN DE USUARIO ESTARÁ PROTEGIDA CONFORME A LO ESTABLECIDO POR EL PROPIETARIO Y SÓLO TENDRÁN ACCESO LOS USUARIOS AUTORIZADOS POR ÉL.

PROTECCIÓN DE TERMINALES

TODO USUARIO ES RESPONSABLE DE LA PROTECCIÓN DE SU TERMINAL Y EVITARÁ QUE SEA MANIPULADO O USADA LA INFORMACIÓN QUE CONTIENE. PARA ELLO:

- En ausencias, se bloqueará el terminal, bien con un dispositivo físico, (llave o similar), o dispositivo lógico, (software de bloqueo con arranque mediante contraseña).
- Al finalizar la jornada laboral, se utilizarán los mecanismos físicos o lógicos mencionados anteriormente.

CIFRADO DE LA INFORMACIÓN

LA INFORMACIÓN CON ESPECIAL SENSIBILIDAD O CONFIDENCIALIDAD SE CIFRARÁ PARA QUE NO PUEDA SER CONOCIDA O PROCESADA POR NINGÚN USUARIO O PERSONA NO AUTORIZADA.

CLAVES DE CIFRADO:

- Su uso, gestión o distribución tiene que estar restringido a determinadas personas o usuarios.
- La autorización de uso de claves debe ser aprobada por el propietario de la información.
- El método usado para la distribución de claves debe asegurar que son recibidas por el destinatario y sólo por él.
- La clave de cifrado tiene que ser transmitida por conducto distinto al de la información.