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

VIRUS INFORMÁTICOS

PARA ELIMINAR, O AL MENOS, MINIMIZAR LA INFECCIÓN POR VIRUS, SE TENDRÁN EN CUENTA LAS SIGUIENTES CONSIDERACIONES:

- Se prohíbe el uso de productos sin licencia, no autorizados por la Fundación, o adquiridos de fuentes sin garantía.
- Cualquier disco o archivo que provenga de otro usuario, se debe verificar con programas antivirus.
- Se debe mantener un producto antivirus residente en memoria de forma permanente.
- Hay que actualizar periódicamente el producto antivirus a versiones más modernas.
- Es conveniente realizar periódicamente copias de seguridad.
- Comunicar al Servicio de Informática cualquier infección de virus que se detecte.
- Está totalmente prohibido propagar conscientemente datos o programas infectados por virus.
- Hay que controlar las transferencias de información recibidas.

SEGURIDAD DEL SISTEMA

- SÓLO LOS USUARIOS AUTORIZADOS PUEDEN AÑADIR, MODIFICAR O ELIMINAR FUNCIONES DE SEGURIDAD O DE ADMINISTRACIÓN DE SEGURIDAD, DEL SISTEMA.
- LOS INTENTOS DE ACCESO NO AUTORIZADOS AL SISTEMA O A LA INFORMACIÓN, PUEDEN SER RECONOCIDOS Y SEGÚN LAS CIRCUNSTANCIAS, SANCIONADOS.

CONEXIONES EXTERNAS

La red externa más comúnmente usada es la de Internet.

¡ATENCIÓN!, cualquier acceso a una conexión externa puede representar un riesgo debido a:

- Pérdida de integridad de la información.
- Interceptación de información clasificada.
- Contaminación por virus por obtención de productos infectados.

Medidas de protección:

- Utilizar sólo los servicios a los que se haya autorizado.
- Utilizar la propia identidad, nunca una ajena.
- No almacenar información clasificada, a no ser cifrada.
- No introducir ni obtener de la red, material ofensivo, amoral o no apropiado.

PLANES DE EMERGENCIA Y EVACUACIÓN

ANTE LA POSIBILIDAD DE OCURRENCIA DE CUALQUIER TIPO DE DESASTRE O CONTINGENCIA, SE DEBERÁ CONOCER Y LLEGADO EL CASO, EJECUTAR EL PLAN DE EMERGENCIA Y EVACUACIÓN, DEBIENDO PARA ELLO:

- Conocer los edificios, ubicación de instalaciones, zonas de posibles riesgos y medios de protección disponibles.
- Evitar, o al menos, minimizar las posibles causas de emergencias.
- Estar informados de las medidas de protección.
- Preparar la posible intervención de recursos externos, (policía, bomberos, ambulancias, etc.)
- Cumplir la normativa vigente de seguridad.

PLANES DE CONTINGENCIA

SON CONJUNTOS DE PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD, QUE DEFINEN LAS ACCIONES A REALIZAR EN CASO DE PRODUCIRSE ACONTECIMIENTOS QUE PUEDAN INUTILIZAR O DEGRADAR AL SISTEMA.

ANTE UN HECHO QUE ACTIVE UN PLAN DE CONTINGENCIA SE DEBEN PROTEGER:

- Datos críticos
- Información
- Equipos físicos
- Comunicaciones
- Documentación
- Suministro de energía eléctrica
- Climatización
- Instalaciones

Y ADEMÁS, EN UN PLAN DE CONTINGENCIA

ES MUY IMPORTANTE

- Asegurar la continuidad de las aplicaciones críticas y la integridad de la información del sistema que la procesa, en caso de desastre, (recuperación de desastres).
- Tratar de salvar la información crítica, es decir, aquella información cuya falta de disponibilidad causaría graves dificultades en la continuidad de las actividades.

Comité de Seguridad Informática

comite.seguridad@ceu.es

COPIAS DE SEGURIDAD (backups)

ES RECOMENDABLE PLANIFICAR LA OBTENCIÓN DE LAS COPIAS DE SEGURIDAD AL TERMINAR TODOS LOS PROCESOS DIARIARIAMENTE, QUEDANDO DE ESTA FORMA ACTUALIZADA Y SALVADA LA INFORMACIÓN.

Se harán copias de seguridad periódicamente, en caso de que no se hagan de forma diaria.

Se podrán hacer:

- Sobre medios de almacenamiento, (discos, cintas, etc.), o bien
- Mediante transferencia electrónica de información a un centro de almacenamiento, si se disponen de medios de transmisión.

FORMACIÓN DE LOS USUARIOS

- LAS AMENAZAS MÁS SERIAS PARA LOS SISTEMAS DE INFORMACIÓN SON LAS PERSONAS, QUE PUEDEN PRODUCIR DAÑOS ACCIDENTALES O INTENCIONADOS.
- LOS ERRORES QUE SE COMETEN DE FORMA NO INTENCIONADA, BIEN POR ACCIDENTE O POR IGNORANCIA, OCURREN MÁS FRECUENTEMENTE. POR ELLO:
- EL REQUISITO MÁS IMPORTANTE PARA EL ÉXITO DE TODO PROGRAMA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN, ES LA FORMACIÓN Y SENSIBILIZACIÓN DE LOS USUARIOS. POR ELLO, SE DEBERÁ PROCURAR:
  - Conocer las buenas prácticas de seguridad.
  - Tomar conciencia sobre la seguridad de los sistemas de información.
  - No considerar obstáculos los controles de seguridad establecidos.

REGLAS DE USO (I)

- EL USUARIO FINAL ES EL ÚLTIMO ESLABÓN DE LA CADENA DE SEGURIDAD.
- EL USUARIO FINAL ES EL MÁS PRÓXIMO A LOS DATOS EN LA PROTECCIÓN DE LAS FUENTES DE INFORMACIÓN.
- NO DAR POR HECHO QUE EXISTE UNA SEGURIDAD DE LA INFORMACIÓN. HAY QUE FORMAR PARTE DE ELLA.
- LA SEGURIDAD EN UN SISTEMA DE INFORMACIÓN CONSISTE EN PRESERVAR LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD.

Estos factores pueden ponerse en peligro por actos voluntarios o involuntarios, de origen interno o externo, por errores o por accidentes, accidentales o intencionados.

REGLAS DE USO (II)

UTILIZAR DEBIDAMENTE EL ORDENADOR CON:

- No juegos (entretenimiento, diversión, etc.).
- No trabajos particulares o para otra entidad.
- No introducir virus.
- No extraer o introducir material amoral, ofensivo o no autorizado.
- No provecho personal, (modificaciones provechosas).
- No desafío al sistema.
- No vandalismo.
- No accidente, (negligencia).
- No sacar copias piratas de programas o software utilizado.
- No dejar comida ni bebida cerca del ordenador.
- No enchufar otros dispositivos no informáticos, (calefactores, calculadoras, etc.), en la toma de corriente del ordenador.
- No mezclar cables de corriente con cables de datos, (interferencias).

REGLAS DE USO (III)

AL UTILIZAR EL ORDENADOR SE DEBERÁ OBSERVAR SIEMPRE:

- Buen uso del identificador.
- Buen uso de la contraseña, (observación de las reglas para su uso).
- Salvado periódico de datos y programas, (backups).
- Almacenamiento correcto de las copias de seguridad.
- Detección y anulación de virus.
- Accesos autorizados a informaciones confidenciales.
- Bloqueo del terminal ante descansos o interrupciones.
- Cuidado con el tabaco y los teclados.
- Seguir fielmente los planes de contingencia.
- Cumplir lo practicado en los planes de formación.

REGLAS DE USO (IV)

¡ATENCIÓN, NOTA IMPORTANTE!

TODOS LOS USUARIOS FINALES DE SISTEMAS DE INFORMACIÓN, DEBEN SABER QUE LA COPIA DE PROGRAMAS Y/O USO DE DATOS DE CARÁCTER PERSONAL EN TAREAS NO DECLARADAS O NO AUTORIZADAS, SON OPERACIONES ILEGALES QUE PUEDEN DAR LUGAR A RESPONSABILIDADES, NO SOLO DISCIPLINARIAS, SINO TAMBIÉN JUDICIALES.

¡EL DESCONOCIMIENTO DE LA LEY NO EXIME DE SU CUMPLIMIENTO!

REGLAS DE USO (V)

¡NO CONOCER LA LEY NO EXIME DE SU CUMPLIMIENTO!

- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).
- Ley Orgánica 10/1995 del Código Penal.
- Real Decreto 428/1993 del Estatuto de la Agencia de Protección de Datos.
- Directiva europea 95/46/CE
- Directiva europea 97/66/CE
- Real Decreto 99/1999

REGLAS DE USO (VI)

¡NO CONOCER LA LEY NO EXIME DE SU CUMPLIMIENTO!

- Ley 34/2002 de Servicios de la Sociedad de la Información y del Correo Electrónico (LSSICE).

Objeto

LIMITAR EL USO DE LA INFORMÁTICA Y OTRAS TÉCNICAS Y MEDIOS DE TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL PARA GARANTIZAR EL HONOR, LA INTIMIDAD PERSONAL Y FAMILIAR DE LAS PERSONAS Y EL PLENO EJERCICO DE SUS DERECHOS.

REGLAS DE USO (VII)

NO CONOCER LA LEY NO EXIME DE SU CUMPLIMIENTO!

- Ley 22/1987 de Protección Intelectual.
- Ley 16/1993 sobre Protección Jurídica de programas de ordenador.

Objeto

PROTEGER PROGRAMAS DE ORDENADOR INCREMENTANDO LAS MEDIDAS LEGALES PARA EVITAR LA PIRATERÍA INFORMÁTICA, YA QUE LOS PROGRAMAS DE ORDENADOR Y SU DOCUMENTACIÓN, ESTÁN CONSIDERADOS COMO OBRAS LITERARIAS, POR TANTO, COMO CREACIONES INTELECTUALES DE SU AUTOR.

SI HAS SIDO CAPAZ DE LLEGAR HASTA AQUÍ.

LA FUNDACIÓN UNIVERSITARIA SAN PABLO CEU Y EN SU NOMBRE EL COMITÉ DE SEGURIDAD INFORMÁTICA TE AGRADECE LA ATENCIÓN PRESTADA Y ESPERA QUE TE HAYA SIDO ÚTIL.

MUCHAS GRACIAS