Los sistemas de gestión de la información. Su implementación no es sencilla, porque abarca a todos los eslabones de la cadena de gestión de la información y requiere un gran conjunto de medidas organizativas y tecnológicas.

El éxito de su implantación depende, además, de que exista en todos los niveles una cultura de la seguridad, es decir, una concienciación sobre la necesidad de que la información se mantenga en secreto, íntegra y disponible.

Uno de los eslabones normalmente más débiles de la cadena de gestión de la información es precisamente el usuario final del sistema (tanto en el uso de la informática como en soporte papel). Por tanto éste necesita ser consciente de las situaciones de riesgo en materia de seguridad de la información y, al mismo tiempo, debe disponer de unas normas respecto al uso correcto de los sistemas informáticos a su alcance, así como de los soportes o documentos en papel y, con especial relevancia, deberá preservar la confidencialidad de la información de carácter personal que esté siendo tratada.

Es importante que todo el personal del Centro Asociado que utilice equipos informáticos y acceda o trate información de carácter personal para la realización de sus funciones conozca este documento.

Esta Política de Seguridad para sistemas informáticos está diseñada para proteger el CA UNED-Les Illes Balears, nuestros empleados, colaboradores y clientes de los daños causados por el mal uso de nuestros sistemas de tecnología de la información y de los datos almacenados. El mal uso incluye tanto acciones deliberadas como accidentales.

Las repercusiones de la mala utilización de nuestros sistemas pueden ser importantes. El daño potencial incluye, pero no se limita a, la infección (por ejemplo, virus informáticos), responsabilidades legales por la fuga de datos, y la pérdida de productividad resultante por el tiempo de inactividad de la red.

Toda persona que trabaja o colabora en el CA UNED-Les Illes Balears es responsable de la seguridad de nuestros sistemas informáticos y de los datos almacenados en ellos. Como tal, debe asegurarse que todos ellos conocen y se comprometen en todo momento a las directrices de esta Política. Si alguna persona tiene dudas sobre cómo afecta la Política de Seguridad en su tarea diaria debe consultar al Coordinador Tecnológico (C.T.) y/o la dirección del centro

Definiciones

"Usuarios" son todas las personas que tienen acceso a cualquiera de los sistemas informáticos de tecnología de la información del Centro. Esto incluye al personal administrativo, colaboradores, profesorado tutor y clientes.

"Sistemas" se refiere a todos los equipos informáticos que se conectan a la red corporativa o de acceso a las aplicaciones corporativas.

Esto incluye, pero no está limitado a, ordenadores de mesa, ordenadores portátiles, impresoras, redes de datos y de voz, red dispositivos, el software, los datos almacenados electrónicamente, dispositivos de almacenamiento de datos portátiles.

Alcance

Esta es una Política universal que se aplica a todos los usuarios y todos los sistemas. Para algunos usuarios y/o algunos sistemas más específicos puede existir una política concreta: en tales casos, esta tiene prioridad en los casos de conflicto.

Este documento es para uso interno de los sistemas en el CA UNED-Les Illes Balears.
Los miembros del personal en el CA UNED-Les Illes Balears deben vigilar y hacer cumplir esta política y son responsables de garantizar que se cumpla la normativa en todo momento.

Uso de sistemas de TI

Todos los datos almacenados en los sistemas del CA UNED-Les Illes Balears son propiedad del CA UNED-Les Illes Balears. Los usuarios deben ser conscientes de que el Centro no puede garantizar la confidencialidad de la información almacenada en cualquier sistema, salvo que así lo requiera la normativa.

La dirección informará a las personas del Centro de lo que constituye un nivel aceptable de uso personal del los sistemas de TI. Cualquier persona que no esté segura debe consultar con el C.T. o dirección del centro.
Cualquier información que sea particularmente sensible o vulnerable debe estar cifrada y/o almacenada de forma segura para que no se produzca un acceso no autorizado (o al menos sea muy difícil). Sin embargo, estas medidas no deben interferir con el legítimo derecho de las personas autorizadas.

El Centro puede controlar el uso de sus sistemas informáticos y los datos de los mismos en cualquier momento. Esto puede incluir (salvo que se opongan a ello leyes de privacidad) el examen local de los contenidos almacenados en los archivos de correo electrónico y datos de cualquier usuario, y el examen del historial de acceso de cualquier usuario.
El Centro se reserva el derecho de auditar regularmente las redes y los sistemas para garantizar el cumplimiento de esta política.

Seguridad de los datos.

Cualquier dato de los sistemas del Centro que esté clasificado como confidencial debe estar claramente indicado en los datos y/o en el sistema de acceso a los mismos.
Los usuarios deben tomar todas las medidas necesarias para evitar el acceso no autorizado a información confidencial.
Se espera que los usuarios ejerzan su conocimiento y juicio razonable en el momento de decidir qué información es confidencial.
Los envíos masivos de información así como lo correos que se destinen a gran número de personas serán sólo los estrictamente necesarios.
Los usuarios no deben enviar, cargar, eliminar en medios portátiles o transferir a un sistema externo del Centro cualquier información que sea designada como confidencial, o que deberían considerar

razonablemente como confidencial, salvo que expresamente esté autorizado para ello en el ejercicio de sus funciones regulares.
Los usuarios deben mantener sus contraseñas seguras y no permitir que otros tengan acceso a sus cuentas. Los usuarios deben asegurarse de que todas las contraseñas cumplan con la directiva de contraseñas seguras del Centro.
Los usuarios que acceden con los equipos informáticos del Centro son responsables de la seguridad y del cuidado de esos equipos. Además también son responsables de la seguridad del software y de los datos almacenados en otros sistemas del Centro a los que puedan acceder de forma remota al utilizar un equipo concreto.

Dado que la información sobre los dispositivos portátiles, como tablets, smartphones, etc., es especialmente vulnerable, debe tenerse especial atención con estos dispositivos: la información confidencial se debe almacenar solamente en carpetas cifradas.
Los usuarios serán responsables de las consecuencias del robo o la divulgación de información sobre los sistemas portátiles confiados a su cuidado sino se han tomado las precauciones razonables para asegurarla.
Todas los puestos de trabajo (equipos de escritorio y portátiles) deben estar asegurados con una política de bloqueo en espera activa después de un máximo de 10 minutos de inactividad.
Además, la pantalla y el teclado se deben bloquear manualmente por el usuario responsable siempre que deje la máquina desatendida.

Los usuarios deberán en todo momento protegerse contra el riesgo de malware (por ejemplo, virus, spyware, troyanos, rootkits, gusanos, puertas traseras).
En caso de infección debe comunicarse de inmediato al C.T. y/o dirección del centro y dejar de actuar con el equipo informático infectado a efectos de prevenir la difusión del virus en la red interna del Centro.

Uso Inaceptable
Todos los empleados y colaboradores deben usar su sentido común acerca de lo que es el uso inaceptable de los sistemas del Centro. Las actividades que a continuación se detallan son ejemplos de uso inaceptable, si bien no son las únicas. En caso de que una persona tenga que contravenir estas directrices con el fin de cumplir su función, deben consultar y obtener la aprobación C.T. y/o dirección antes de proceder.

- Todas las actividades ilegales
Estas incluyen el robo, la piratería informática, distribución de malware, derechos de autor y que contravengan patentes y el uso de software o servicios ilegales o sin licencia.
También se incluyen las actividades que contravengan las normas de protección de datos. Todas las actividades perjudiciales para el correcto funcionamiento del Centro. Estas incluyen tanto el intercambio de información sensible fuera del Centro, como información sobre investigación y desarrollo, y las listas de clientes, así como la difamación del Centro.
Todas las actividades para beneficio sólo personal que tienen un impacto negativo en el funcionamiento del día a día del Centro. Estas incluyen actividades que ralentizan la red informática (por ejemplo, reproducción de vídeo en red de juegos,…)

Todas las actividades que no son apropiadas para el Centro y que ponen en entredicho la reputación del mismo. Esto incluye pornografía, juegos de azar, el odio incitación, acoso y hostigamiento.
Sortear los sistemas de seguridad de TI y los protocolos que el Centro ha puesto en marcha.

Aplicación
El Centro no tolerará el mal uso de sus sistemas y deberá corregir con medidas disciplinarias a cualquier persona que se demuestre que ha contravenido la Política de Seguridad, incluyendo no ejercer un juicio adecuado sobre el uso aceptable de los sistemas.

Si bien cada situación será analizada y juzgada caso por caso, los empleados y colaboradores deben ser conscientes de que las consecuencias pueden llegar a incluir la finalización de su relación con el Centro.
El uso de cualquiera de los recursos del Centro para cualquier actividad ilegal suele ser motivo de apercibimiento, amonestación, sanción, de despido o cese de colaboración, y el Centro cooperará con cualquier investigación y procesamiento penal que pueda derivarse de dicha actividad.

Política de cuentas de usuario después de la terminación del contrato o colaboración

Tras la rescisión del contrato de un empleado o colaborador de trabajo, el acceso a todas las cuentas de usuario (correo electrónico, servidor de archivos, sitio web, etc.) y la inclusión en las listas de correo del Centro se cancelará inmediatamente. Si se solicita, el correo electrónico entrante puede ser redirigido de forma automática a una nueva dirección para un período máximo de 30 días.

RELATIVAS A ASPECTOS FÍSICOS DE LA POLÍTICA DE SEGURIDAD

- Control de acceso físico a las instalaciones.
El acceso físico a las instalaciones está limitado por las mañanas en la entrada principal del Centro. Por las tardes, al desarrollarse las clases tutorías y aumentar significativamente el número de personas en el Centro, se puede acceder por las puertas que dan acceso al aparcamiento de estudiantes. El personal del centro PAS, personas colaboradoras, así como las personas de dirección están a disposición de quien lo necesite ante cualquier incidencia. Todas las dependencias se encuentran cerradas, bajo llave, en la ausencia de uso (especialmente por las mañanas). Por las tardes se abren al menos media hora antes de su empleo habitual. Por las noches se comprueba el contenido y estado del material de cada aula/dependencia y se procede a su cierre bajo llave.
En el caso que el centro esté abierto al medio día, deberá cuidarse que las distintas dependencias que no estén en uso se mantengan cerradas y con la alarma activada.
Cuando se cierra el centro se activan las alarmas de seguridad que están conectadas a una empresa de seguridad (Trablisa) que dispone de duplicados de llaves para cualquier urgencia. Aquellos edificios que no se utilizan durante el día también tienen activada la alarma de seguridad.

- Control de acceso físico a routers, switches, etc.
El acceso a routers, switches, etc, está limitado a dependencias de acceso restringido del personal del centro. Así mismo cuando procede se encuentran de un armario RACC cerrado. El personal autorizado para el acceso y manipulación se limita al coordinador tecnológico, a la dirección del

centro y aquel personal del centro que por necesidad y/o urgencia deba acceder para reestablecer el funcionamiento adecuado. Están autorizados responsables de empresas (telefónica) a su acceso para reparación/sustitución.

- **Control de acceso físico al CPD, servidores, cortafuegos, etc.**

El centro dispone de servidor que se encuentra cerrado bajo llave de un armario RACC metálico, de 2 m de altura, de material metálico inoxidable. La dependencia en la que está ubicado el servidor es de acceso restringido. Además dispone de climatización, sistema contrainciendios, detector de humos y sensor de movilidad.

- **Control de acceso físico a documentos sensibles**

Los documentos sensibles se encuentran en dependencias de acceso restringido al personal del centro, en el interior de armarios cerrados bajo llave. El acceso a la llave se restringe a la/s persona/s autorizadas de acuerdo con el documento de seguridad (protección de datos).

RELATIVAS A ASPECTOS LÓGICOS DE LA POLÍTICA DE SEGURIDAD

- **Definición de usuarios y autenticación. Política de contraseñas.**

El Centro dispone de un documento donde se incluyen las características/perfil de cada tipo de usuario de los sistemas informáticos. Así mismo, se incluye la política de contraseñas de los usuarios de cada puesto de trabajo que debe renovarse anualmente. La política de contraseñas de cada usuario Uned, correo Uned, está establecida por la Uned sede central, atendiendo a la LOPD.

- **Definición de permisos de cada usuario**

El centro dispone de un documento que incluye los permisos de cada usuario específico tanto en el acceso al sistema operativo de cada sistema, como a los programas específicos de la Uned.

- **Política de acceso remoto**

El centro no tiene establecido el acceso remoto a sistemas por parte de sus empleados y colaboradores. El acceso remoto a determinados sistemas es factible tan sólo por el C.T. y los servicios informáticos debidamente autorizados. Para que tenga lugar el acceso remoto se precisa de VB del director del Centro y debe estar motivado por una acción necesaria de sistema dado (por ejemplo, videoconferencia y clases AVIP).

- **Política de redes inalámbricas, métodos de cifrado y seguridad**

La red inalámbrica del Centro usa en estos momentos una línea de fibra óptica de telefónica y una segunda red inalámbrica se dispone a través de la intranet de la Uned.
La red inalámbrica es parte de la red de datos del Centro, y como en esta, el uso que se hace de ella debe ser acorde con los fines y el buen nombre de la institución.
El acceso a la red inalámbrica se realiza previa autenticación del usuario mediante el par "nombre de usuario - contraseña". Todas las conexiones quedan registradas.
Todos los usuarios tienen los mismos derechos de acceso (esencialmente estudiantes) que los alumnos del Centro. Podrán acceder a todos los recursos que el Centro pone a su disposición tales como Campus Virtual, bases de datos de biblioteca, correo electrónico, web, etc. Podrán además

conectarse a Internet para navegar, acceder a cuentas de correo de fuera de la Uned, y usar otros servicios como ftp o ssh. No podrán conectarse a servidores internos del Centro.
Al detectarse un uso inadecuado de la red inalámbrica por parte de un usuario, se le podrá expulsar de la red y se le apercibirá del comportamiento inadecuado.

- **Seguridad perimetral: Instalación de firewalls, IDSs, configuración de routers, etc.**

El Centro gestiona y sopesa la incorporación del servicio, EasyAudit, de detección de fallos de seguridad (Vulnerability Assessment and Management) que no necesita ningún tipo de instalación ni configuración. A través de este sistema se obtendría de forma continuada el estado de seguridad de los equipos conectados a internet. En cada momento, el servicio indicaría: todos los fallos detectados, la posible ausencia de parches, errores de configuración, servicios por defecto..., en definitiva, todas las vías que pueden ser aprovechadas para realizar un ataque y poner en peligro la red del Centro. Hasta la fecha no se ha sido objeto de ataques informáticos externos.

- **Protección contra software malicioso (antivirus)**

Todos los equipos informáticos del centro tienen instalado el antivirus suministrado gratuitamente por la Uned en la Web. El antivirus Karspesky es actualizado periódicamente por parte del C.T. y colabora personal del Centro en este proceso que abarca el 100% de los sistemas informáticos del centro. Se comprueba en las revisiones de los sistemas que la instalación y funcionamiento es correcto.
No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia.

- **Planes de contingencia: copias de seguridad, recuperación ante desastres**

Se realizarán copias semanales de seguridad frente al servidor del centro tanto de los datos de trabajo sensible habitual como en las áreas del ámbito económico y protección de datos, si procede. Así mismo documentación electrónica gestionada por la dirección del centro es sujeta a copia de seguridad.

- **Procedimientos de respuesta frente a incidencias de seguridad**

Cualquier incidencia detectada en cuanto a seguridad informática es comunicada al C.T. que ha de actuar de manera diligente, para que se minimicen los efectos de la incidencia detectada.
El C.T. ha de evaluar de forma regular las vulnerabilidades del entorno. Comprobar con regularidad todos los sistemas y dispositivos de red para garantizar que tienen instaladas las revisiones más recientes. Comprobar que se cumple la política de seguridad de contraseñas seguras. Supervisar y analizar el tráfico de red y el rendimiento del sistema cuando se detecten anomalías.

RELATIVAS A ASPECTOS HUMANOS DE LA POLÍTICA DE SEGURIDAD

- El personal del centro y personas colaboradoras han recibido curso una formación relacionada con la seguridad informática y protección de datos. La actividad es obligatoria para el personal implicado en la seguridad. Anualmente se debe realizar, al menos, una actividad de formación con el personal del Centro para actualizar conocimientos y procedimientos de actuación, en relación con la seguridad informática y la protección de datos.

- Protección y ubicación de los equipos

- Los usuarios no deben mover o reubicar los sistemas, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del coordinador tecnológico (C.T.) y dirección del centro, debiéndose solicitar a la misma en caso de requerir este servicio.
- El C.T. será el encargado de velar por el funcionamiento correcto del material suministrado al usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la dirección.
- El sistema asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario del Centro Asociado UNED-Les Illes Balears.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.
- Mientras se opera el sistema, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.
- Se debe evitar colocar objetos encima del sistema o cubrir los orificios de ventilación del monitor o del gabinete.
- Se debe mantener el sistema en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.
- Cuando se requiera realizar cambios múltiples del sistema derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con anticipación a la dirección del centro a través de un plan detallado de movimientos debidamente autorizados por el C.T.
- Queda prohibido que el usuario, por cuenta propia o por encargo externo, abra o desarme los sistemas.

- Mantenimiento de equipo

- Únicamente el personal autorizado de la dirección podrá llevar a cabo los servicios y reparaciones al sistema, por lo que los usuarios deberán sólo han de permitir el acceso a sus equipos a la persona autorizada.
- Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal del C.T.

- Pérdida o transferencia de equipo

- El usuario que tenga bajo su resguardo algún sistema será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- El usuario deberá dar aviso de inmediato a la dirección de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

- Uso de dispositivos especiales

- El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen. Estos dispositivos podrán ser utilizados para realizar copias de seguridad por la dirección y personas autorizadas.
- El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

- Daños en los equipos

El equipo de cómputo o cualquier recurso de tecnología de la información que sufra algún desperfecto por maltrato, descuido o negligencia por parte del usuario, deberá ver cubierto su valor de reparación o reposición del equipo o accesorio afectado por dicho usuario. Para tal caso el C.T. y la dirección del centro determinará la causa y alcance económico de dicho desperfecto.

RELATIVAS A ASPECTOS LEGALES (LOPD)

- El Centro dispone del documento de Seguridad de acuerdo con LOPD. Este documento se actualiza periódicamente (anualmente o cada seis meses), es conocido por todas las personas implicadas en el acceso y/o tratamiento de datos sensible. El personal del centro y personas que colaboran habitualmente reciben formación periódicamente.