UNIVERSIDAD D SEVILLA

Normas de Seguridad

Normativa de control de acceso físico

Índice

1. Introducción

La presente normativa establece las condiciones y acciones a realizar para el acceso físico a las ubicaciones de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) de acceso restringido de la Universidad de Sevilla (en adelante, US) estableciendo tanto el protocolo de autorización como los procedimientos de acceso específicos para cada caso.

2. Objeto

Esta normativa trata de determinar las medidas de seguridad que se deben aplicar para llevar a cabo un correcto seguimiento y control del acceso físico en relación a la seguridad física y del entorno, como son los controles físicos de entrada y las áreas de acceso restringido.

3. Ámbito de aplicación

Esta normativa será aplicable al control de acceso físico a todas las ubicaciones seguras y las áreas de acceso restringido de la US.

Esta normativa es de aplicación para todo el personal, que de manera permanente o eventual, preste sus servicios en la US, incluyendo el personal de organizaciones externas cuando sean usuarias o posean acceso a los Sistemas de Información de la US.

4. Vigencia

La presente normativa ha sido aprobada por la Comisión de Seguridad de la US con fecha 16 de diciembre de 2016, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la US pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la US. Las versiones anteriores quedan anuladas por la última versión de esta normativa.

5. Revisión y evaluación

La gestión de esta normativa corresponde al Servicio de Informática y Comunicaciones (en adelante, SIC) de la US, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario, para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Cuando las circunstancias así lo aconsejen se revisará la presente normativa, que se someterá, de haber modificaciones, a la aprobación de la Comisión de Seguridad de la US.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica y organización general o cualquier otra cuestión que pueda provocarla.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

6. Referencias

La presente normativa se fundamenta en la legislación vigente en materia de seguridad de las Tecnologías de la Información y las Comunicaciones de ámbito europeo, estatal y autonómico, así como en las normas y procedimientos internos que resulten de aplicación a la Universidad en el marco de la Política de Seguridad de la Información.

7. Desarrollo de la normativa

7.1. Marco de aplicación

La presente normativa regula el acceso físico a las ubicaciones que albergan Tecnologías de la Información y las Comunicaciones en la US que, por sus características especiales, requieren un acceso restringido. Todo el personal de la US y de organizaciones externas que disponga del permiso correspondiente, debe conocer y seguir las directrices de control de acceso que le afecten.

A cada local se le aplican unas medidas de seguridad de control de acceso que dependen de sus características. Con el fin de establecer unas medidas homologables, a cada local se le asigna una de las siguientes categorías:

- Centros de Proceso de Datos (en adelante CPDs): salas de equipamiento TIC en las que se ubican los Sistemas de Información de la US. Requieren unas características técnicas particulares, infraestructura específica, medidas concretas de seguridad y mantenimiento continuo para su correcto funcionamiento.
- Cuartos Técnicos de Telecomunicaciones: locales donde se ubican los racks de telecomunicaciones del edificio y/o la central telefónica del edificio o Campus.
- Salas de operación: salas, normalmente anejas a los CPDs, donde se desarrollan tareas de operación de los CPDs.
- Almacenes: locales donde se guarda material informático y de telecomunicaciones y/o copias de seguridad.
- Otros espacios TIC: el resto de espacios de trabajo que no se encuadran en las categorías anteriores como aulas TIC, laboratorios, salas de videoconferencia, seminarios, salas de servidores, etc.
- Despachos: espacios en los que desarrolla su trabajo el personal de la US y que están dotados de las infraestructuras TIC requeridas por el puesto de trabajo.

El inventario de áreas de acceso restringido, con su clasificación, se relaciona en el Anexo II de esta normativa.

En cada área restringida hay una persona encargada del control y registro de accesos a los que se refiere esta normativa. Estas personas se encargan de la identificación en primera instancia del personal autorizado. Ante cualquier duda sobre la identidad de las personas que soliciten acceso, se requerirá su autenticación a los servicios de seguridad.

7.2. Procedimientos de acceso

7.2.1. Acceso a Centros de Proceso de Datos

Todos los CPDs deben disponer de un sistema informatizado de registro y control de acceso basado en lectores de tarjeta de proximidad. El acceso se realiza utilizando una tarjeta corporativa proporcionada por la US y, dependiendo del CPD, tecleando adicionalmente un PIN. En cada acceso queda registrado de forma automática la tarjeta, la fecha y hora en la que se produce el acceso. Sólo puede acceder a los CPDs el personal autorizado por el responsable de explotación del área restringida.

Existen tres tipos de perfiles de acceso:

- Acceso permanente: personal que realiza tareas habituales en las salas de operación y en los CPDs, y que dispone de tarjeta de acceso propia, asignada a su nombre, la cual es personal e intransferible. Aunque el acceso sea permanente, si el sistema de control de acceso lo permite, podrían existir limitaciones horarias en función del grupo al que pertenezcan. Los grupos de personas con acceso permanente son los siguientes:
  - Personal de sistemas: explotación, comunicaciones y atención a usuarios.
  - Limpieza: personal de limpieza destinado al edificio.
  - Seguridad: vigilantes de Campus y Responsable de seguridad.
  - Personal responsable de evacuación en caso de emergencia.
  - Personal de Mantenimiento de la US.
- Acceso temporal: personal interno o externo de la US que debe realizar tareas ocasionales durante un periodo de tiempo definido, y a los que se debe proveer de autorización temporal, ya sea asignando el permiso sobre su tarjeta corporativa, o en caso de no disponer de tarjeta, proporcionándole una tarjeta de cortesía a la que se asigna el permiso de acceso correspondiente y cuyo uso debe quedar registrado. Esta tarjeta podrá ser de uso diario, en cuyo caso se recogerá al inicio de la jornada de trabajo y se devolverá al finalizar, o bien permanente si es una tarjeta para un centro que dispone de instalaciones TIC. En este caso el centro será el responsable de registrar los usos de la tarjeta. Una persona con acceso permanente indicará a la persona con acceso temporal la ubicación del rack, equipo o sistema sobre el que ha de actuar.
- Visitas: personal interno o externo de la US que realiza tareas puntuales sin supervisión, visitas supervisadas o visitas guiadas a las instalaciones.
  - Visitas sin supervisión: personal que ha de acceder para realizar tareas puntuales y que no es necesario que estén acompañados mientras realizan sus tareas, por ejemplo, reparación de averías, instalaciones de cableado y de equipos, etc. Una persona con acceso permanente indicará al visitante la ubicación del rack, equipo o sistema sobre el que ha de actuar. Una vez finalizado el trabajo, lo notificará a la

persona que le ha acompañado en el acceso y a la persona para la que ha realizado el trabajo, para registrar el fin de la visita.

- Visitas supervisadas: personal que ha de acceder puntualmente y han de estar acompañados en todo momento. Si se trata de visitas de replanteo de instalaciones, transportistas, etc. el acceso al área restringida se realizará acompañado de una persona que dispone de acceso permanente, quien le acompañará hasta el rack, equipo o sistema sobre el que ha de actuar, y permanecerá acompañado en todo momento hasta la finalización de la visita.
- Visitas guiadas a las instalaciones: se rigen por el protocolo elaborado por el Servicio de Prevención de Riesgos Laborales de la Universidad de Sevilla (en adelante SEPRUS) que recoge el documento “Recepción de Grupos de Visitantes en Instalaciones de la Universidad de Sevilla”. Dada la naturaleza de estas instalaciones cada Centro podrá disponer de consideraciones particulares que deberán ser consultadas al solicitar la visita.

El procedimiento de solicitud y asignación de permisos de acceso, así como el protocolo detallado de acceso al CPD estará descrito en la normativa particular de cada instalación. El SIC dispone de una normativa propia, aprobada y disponible dentro del marco del Proceso de Gestión de la Continuidad.

En todo caso, el personal ajeno a la US que tenga que realizar cualquier tipo de trabajo en sus instalaciones, deberá ajustarse a la normativa publicada por el SEPRUS en cuanto a subcontratación de servicios externos, debiendo estar dado de alta en el Portal GESPREM (coordinación de actividades empresariales en la Universidad de Sevilla) para poder realizar los trabajos en cualquier instalación objeto de este documento.

En general, el trabajo en el interior de los CPDs se regirá por la normativa básica de buenas prácticas que se especifica en el Anexo III.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura de la oportuna incidencia de seguridad.

7.2.2. Acceso a Cuartos Técnicos de Telecomunicaciones

Los cuartos técnicos están siempre cerrados bajo llave o con cerradura electrónica. Sólo puede acceder a los cuartos técnicos el personal autorizado por la persona responsable. En caso de que el cuarto técnico disponga de cerradura electrónica, el procedimiento de acceso será el mismo que para los CPDs.

Los armarios de comunicaciones que estén ubicados en pasillos o en espacios de uso compartido (no exclusivos de comunicaciones) permanecerán siempre cerrados con llave.

En general, el trabajo en el interior de los cuartos técnicos de telecomunicaciones se regirá por la normativa básica de buenas prácticas que se especifica en el Anexo III.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura de la oportuna incidencia de seguridad.

7.2.3. Acceso a Salas de Operación

El acceso a las salas de operación se realizará en las mismas condiciones que a los CPDs, a excepción del personal externo que no dispone de tarjeta de la US y debe acceder a esta sala con DNI + PIN. Se podrán disponer video-porteros para facilitar el acceso a personal ajeno, por ejemplo, para entrega de material, para solicitud de tarjeta de cortesía, etc. La entrega de paquetes no quedará registrada.

Las visitas guiadas a las salas de operación se rigen por el mismo protocolo que los CPDs.

Cuando una persona con acceso autorizado a un CPD acceda por una sala de operación, se entiende autorizada a esta última con los permisos de acceso al CPD.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura de la oportuna incidencia de seguridad.

7.2.4. Acceso a otros espacios TIC

Los espacios TIC de trabajo que no se encuadran en las categorías anteriores como aulas TIC, laboratorios, seminarios, salas de servidores, salas de videoconferencia, etc. deben considerarse sensibles desde el punto de vista de la seguridad porque disponen de equipos con software y, en muchos casos, acceso a los Sistemas de Información de la US.

Deben seguirse los siguientes principios mínimos de seguridad:

- Permanecerán cerrados cuando no haya nadie trabajando en ellos.
- Fuera del horario de trabajo sólo accederán a ellos personal autorizado de limpieza y seguridad.

El procedimiento de solicitud y asignación de permisos de acceso, así como el protocolo detallado de acceso a los espacios TIC estará descrito en la normativa particular de cada instalación.

En general, el trabajo en el interior de los espacios TIC se regirá por la normativa básica de buenas prácticas que se especifica en el Anexo III.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura de la oportuna incidencia de seguridad. Cualquier presencia sospechosa se pondrá en conocimiento de los servicios de seguridad de la US.

7.2.5. Acceso a despachos

En general, los despachos del personal de la US están dotados de las infraestructuras TIC requeridas por el puesto de trabajo. Cada miembro de la Comunidad Universitaria será responsable del acceso restringido a su despacho y velará por la seguridad de los equipos e información del mismo. Tiene autorización de acceso a los despachos el personal de servicios de limpieza y de seguridad.

En particular, los despachos del personal que trabaja directamente con las TIC deben considerarse especialmente sensibles desde el punto de vista de la seguridad por diversas razones:

- Guardan información sobre estructura y funcionalidad de distintos sistemas de información.
- Pueden disponer de equipos con software y permisos de acceso privilegiado a sistemas de información críticos.
- En algunos casos son lugares que dan acceso a otros de idéntica o similar naturaleza.

En todos los casos deben seguirse los siguientes principios mínimos de seguridad:

- Permanecerán cerrados cuando no haya nadie trabajando en ellos.
- Fuera del horario de trabajo sólo accederán a ellos personal autorizado de limpieza y seguridad.
- En caso de ausencia, el puesto de trabajo estará bloqueado y el monitor presentará la pantalla de bloqueo.

- Se seguirá una política de escritorios limpios cuando deba abandonarse el lugar de trabajo, aunque sea de manera temporal. Se guardará bajo llave en cajones y armarios toda información que pueda considerarse sensible.

Cualquier presencia sospechosa en los despachos se pondrá en conocimiento de los servicios de seguridad de la US.

8. Responsabilidades

Cada persona responsable del acceso restringido a ubicaciones TIC velará, dentro de su ámbito, por el cumplimiento de la normativa y revisará su correcta implantación o cumplimiento.

Apéndice: Lenguaje de género

Esta normativa ha sido redactada con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.

Anexo I: Acrónimos y glosario de términos

CPD

Centro de Proceso de Datos. Espacio equipado para albergar Sistemas de Información de la US que ofrecen Servicios TIC.

SI

Sistema de Información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

SIC

Servicio de Informática y Comunicaciones. Servicio cuyo objetivo es atender las necesidades de apoyo informático a las tareas de estudio, docencia, investigación y gestión en la Universidad de Sevilla.

TIC

Tecnologías de la Información y las Comunicaciones. Dispositivos que permiten trabajar el ciclo de vida completo de la información, es decir, crear, almacenar, tratar, enviar o borrar información

Anexo II: Áreas de acceso restringido

Denominación	Responsable del acceso	Tipo
CPD Edificio Rojo y sala de operación	SIC	CPD/Sala de operación
Centro de Cálculo Edificio Blanco y sala de operación	ETSI Informática	CPD/Sala de operación
Centro de Cálculo de Cartuja y sala de operación	ETS Ingeniería	CPD/Sala de operación
Cuartos de telecomunicaciones	SIC	Cuarto Técnico
Aulas TIC, laboratorios, seminarios,…	SIC/Centros/ Departamentos	Otros espacios TIC
Sala de Servidores	SIC/Centros/ Dptos/Unidades	Otros espacios TIC
Despachos del personal de la US	Personal de la US	Despachos

Anexo III: Buenas prácticas

Normativa de trabajos en CPDs, Cuartos Técnicos de Telecomunicaciones y espacios TIC

Normativa básica

Los CPDs, Cuartos Técnicos de Telecomunicaciones y Espacios TIC son áreas de acceso restringido donde se ubica equipamiento TI muy sensible, a las que solamente deben entrar personas previamente autorizadas y únicamente a hacer la labor encomendada.

Disponen de una infraestructura eléctrica particular, por lo que se debe consultar al operador antes de conectar móviles, portátiles, taladros, en cualquiera de las tomas eléctricas.

Son espacios climatizados para mantener la óptima refrigeración de los equipos TI y no con criterios de confort. Para su eficiente funcionamiento se debe evitar tener la puerta abierta. En el CPD no se deben retirar simultáneamente más de 6 losetas del suelo técnico.

El CPD tiene un sistema de detección y extinción automática de incendios. Los detectores son muy sensibles por lo que está prohibido hacer trabajos con llama, chispa o que generen polvo o humo. Todas estas operaciones: soldaduras, cortes, taladros,... se deben realizar fuera del CPD. En el caso que no pueda realizarse en el exterior se debe solicitar autorización para hacerlo dentro, poniendo todas las medidas necesarias para minimizar la emisión de polvo y suciedad.

Tanto en el CPD como en los Cuartos Técnicos de Telecomunicaciones y otros espacios TIC se debe tener especial sensibilidad con el orden y la limpieza:

- Ensuciar y desordenar lo mínimo al realizar los trabajos.
- Dar un acabado pulcro y de calidad a los trabajos.
- Recoger y limpiar todo cuando se finalizan los trabajos.
- Los embalajes y las basuras se retiraran como mínimo al finalizar cada jornada.
- NO se podrá dejar NADA (documentación, CD-s, cables, conectores,...) en las mesas o en los racks.
- Las conexiones eléctricas y de red se harán con cables y/o fibras de longitud adecuada.

Es responsabilidad del trabajador traer las herramientas necesarias para hacer su trabajo, guardar las medidas de seguridad y atender los consejos del Servicio de Prevención de Riesgos Laborales.

Acceso a salas de servidores y/o sala de explotación

La tarjeta de acceso al CPD y a los Cuartos Técnicos de Telecomunicaciones es personal e intransferible. No se puede acceder acompañado de otras personas que no dispongan a su vez de tarjeta de acceso con los permisos de acceso a dichas salas.

Una vez dentro del CPD, se deben seguir las siguientes directrices:

- Queda PROHIBIDO abrir las ventanas y/o levantar las persianas.
- Queda PROHIBIDO manipular los sistemas de climatización, de incendios y cuadros eléctricos.
- Queda PROHIBIDO levantar las losetas, salvo permiso concedido expresamente para dicha visita o acceso
- Así mismo queda PROHIBIDO enchufar o desenchufar equipos en los enchufes dispuestos bajo las losetas, salvo que se disponga de permiso expreso.
- Queda PROHIBIDO manipular cualquier otro equipo del que no sea titular.
- Queda PROHIBIDO beber y comer en las instalaciones.

Cualquier duda sobre estas normas o sobre cualquier necesidad que surja mientras se trabaja en el CPD deberá ser consultada con los operadores.

Se debe avisar de cualquier anormalidad observada a los técnicos de las salas de explotación, o bien al servicio de seguridad, sobre todo si se encuentra en la instalación fuera de las horas habituales de trabajo del personal de la US.