NORMATIVA DE SISTEMES DE CONTROL D'ACCESSOS A LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprovada pel Consell de Govern de 27 de febrer de 2020

1. Objectiu, àmbit d'aplicació i nomenclatura.

Els sistemes de control d'accessos són un element fonamental en la seguretat dels recursos materials de la Universitat Politècnica de València. Aporten comoditat, flexibilitat, control i seguretat, per la qual cosa una gestió adequada pot millorar enormement aquesta seguretat.

Les directrius d'aquesta Normativa tenen com a objectiu establir els criteris per a instal·lació, ús i gestió de qualsevol tipus de sistema de control d'accessos utilitzats a la Universitat.

En el context de la present Normativa considerem la nomenclatura següent:

a. Sistema de control d'accessos: mecanisme físic que limita el control d'accessos (obertura) d'una porta. Pot funcionar amb diverses tecnologies: teclat, panys electrònics, sistemes biomètrics, etc.

b. Mitjà d'obertura: clau en qualsevol suport físic (targeta, mòbil, clauer, etc.).

c. Usuari d'un sistema de control d'accessos: persona que accedeix a espais protegits pel sistema de control d'accessos, per la qual cosa necessita disposar d'un mitjà d'obertura.

d. Gestor d'un sistema de control d'accessos: persona que gestiona permisos i equipament del sistema. I té accés a la informació del sistema.

e. Entitat: agrupació (àrea, departament, centre) que engloba elements del sistema de control i usuaris configurats per un gestor comú. Cada entitat pot funcionar autònomament de la resta.

NORMATIVA DE SISTEMAS DE CONTROL DE ACCESOS EN LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprobada por el Consejo de Gobierno de 27 de febrero de 2020

1. Objetivo, ámbito de aplicación y nomenclatura.

Los sistemas de control de accesos son un elemento fundamental en la seguridad de los recursos materiales de la Universitat Politècnica de València. Aportan comodidad, flexibilidad, control y seguridad, por lo que una gestión adecuada puede mejorar enormemente esta seguridad.

Las directrices de esta Normativa tienen como objetivo establecer los criterios para instalación, uso y gestión de cualquier tipo de sistema de control de accesos utilizados en la Universitat.

En el contexto de la presente Normativa consideramos la siguiente nomenclatura:

a. Sistema de control de accesos: mecanismo físico que limita el control de accesos (apertura) de una puerta. Puede funcionar con diversas tecnologías: teclado, cerraduras electrónicas, sistemas biométricos, etc.

b. Medio de apertura: llave en cualquier soporte físico (tarjeta, móvil, llavero, etc.).

c. Usuario de un sistema de control de accesos: persona que accede a espacios protegidos por el sistema de control de accesos por lo que necesita disponer de un medio de apertura.

d. Gestor de un sistema de control de accesos: persona que gestiona permisos y equipamiento del sistema. Y tiene acceso a la información del sistema.

e. Entidad: agrupación (área, departamento, centro) que engloba elementos del sistema de control y usuarios configurados por un gestor común. Cada entidad puede funcionar autónomamente al resto.

2. Autorització prèvia a la instal·lació.

Qualsevol entitat (centre, departament, institut, servei, etc.) que vulga instal·lar un sistema de control d'accessos a la Universitat Politècnica de València ha de sol·licitar prèviament autorització per escrit al vicerectorat responsable de la gestió dels espais on es desitge dur a terme la instal·lació. Aquesta sol·licitud es cursa per correu electrònic i va dirigida al vicerectorat corresponent.

El vicerectorat avalua la sol·licitud, i aprova o denega motivadament la realització d'aquesta.

En aquells edificis on ja hi ha una instal·lació de control d'accessos, es pot procedir a la seua ampliació sol·licitant la validació de les ubicacions al Servei d'Infraestructures mitjançant un correu electrònic dirigit a infraes@upv.es.

En totes les ubicacions s'ha de tenir en compte que la instal·lació d'un element de control (per exemple un pany electrònic) en una porta d'accés a una zona comuna a diverses entitats, implica que aquesta porta siga de gestió compartida per totes les entitats, independentment que només una o algunes d'aquestes hagen assumit el cost de la instal·lació. Cada entitat l'ha de gestionar com si fora de la mateixa entitat.

La instal·lació de qualsevol sistema de control d'accessos haurà de comptar amb l'autorització corresponent.

3. Subministrament del sistema de control d'accessos.

Cada entitat és responsable a nivell econòmic dels seus sistemes de control d'accessos.

En cas de disposar d'autorització per a instal·lar algun sistema de control d'accessos, l'entitat ha de complir la normativa de compres vigent.

2. Autorización previa a la instalación.

Cualquier entidad (centro, departamento, instituto, servicio, etc.) que quiera instalar un sistema de control de accesos en la Universitat Politècnica de València deberá solicitar previamente autorización por escrito al vicerrectorado responsable de la gestión de los espacios donde se desee llevar a cabo la instalación. Dicha solicitud se cursará por correo electrónico e irá dirigida al vicerrectorado correspondiente.

El vicerrectorado evaluará la solicitud y aprobará o denegará motivadamente la realización de la misma.

En aquellos edificios donde ya exista una instalación de control de accesos se podrá proceder a su ampliación solicitando la validación de las ubicaciones al Servicio de Infraestructuras mediante correo electrónico dirigido a infraes@upv.es

En todas las ubicaciones se deberá tener en cuenta que la instalación de un elemento de control (por ejemplo una cerradura electrónica) en una puerta de acceso a una zona común a varias entidades, implicará que dicha puerta será de gestión compartida por todas las entidades, independientemente de que solo una o varias de ellas hayan asumido el coste de la instalación. Cada entidad la gestionará como si fuera de la propia entidad.

La instalación de cualquier sistema de control de accesos deberá contar con la autorización correspondiente.

3. Suministro del sistema de control de accesos.

Cada entidad es responsable a nivel económico de sus sistemas de control de accesos.

En caso de disponer de autorización para instalar algún sistema de control de accesos, la entidad deberá cumplir la normativa de compras vigente.

4. Política d'instal·lació.

L'entitat assumeix el cost total de la instal·lació del sistema de control d'accessos.

Per a totes les instal·lacions, cal tenir en compte les indicacions següents:

a. Equipament connectat a la xarxa de dades de la Universitat Politècnica de València.

Tots els elements del sistema de control d'accessos que necessiten connectivitat de xarxa han d'instal·lar-se el més a prop possible d'una presa de xarxa de dades o elèctrica, si és necessari. En cas de ser possible, la instal·lació de l'equipament es col·loca en el bastidor *(rack)* de dades més pròxim a la ubicació del lector.

És necessari coordinar la instal·lació amb l'Àrea de Sistemes d'Informació i Comunicacions i amb el Servei d'Infraestructures.

b. Elements de control en una zona comuna a diverses entitats.

En cas d'instal·lar un element de control (per exemple, un pany electrònic) en una porta d'accés a una zona comuna a diverses entitats, aquesta porta s'ha de configurar perquè puguen controlar-la totes les entitats. Cada entitat la gestiona com si fora pròpia. S'ha de compartir la gestió de l'element comú.

c. Configuració

L'usuari gestiona l'alta dels diferents elements instal·lats en els sistemes de control, seguint les instruccions de l'Àrea de Sistemes d'Informació i Comunicacions i del Servei d'Infraestructures. Cada element se situa sempre utilitzant el codi d'espai de localització de la Universitat.

d. Gestors.

El responsable de cada entitat defineix un o diversos

4. Política de instalación.

La entidad asumirá el coste total de la instalación del sistema de control de accesos.

Para todas las instalaciones se atenderán las siguientes indicaciones.

a. Equipamiento conectado a la red de datos de la Universitat Politècnica de València.

Todos los elementos del sistema de control de accesos que necesiten conectividad de red deberán instalarse lo más cerca posible a una toma de red de datos y/o eléctrica si fuese necesario. En caso de ser posible, la instalación del equipamiento se colocará en el rack de datos más cercano a la ubicación del lector.

Será necesario coordinar la instalación con el Área de Sistemas de Información y Comunicaciones y con el Servicio de Infraestructuras.

b. Elementos de control en zona común a varias entidades.

En caso de instalar un elemento de control (por ejemplo una cerradura electrónica) en una puerta de acceso a una zona común a varias entidades, dicha puerta deberá configurarse para poder ser controlada por todas las entidades. Cada entidad la gestionará como si fuera propia. Se deberá compartir la gestión del elemento común.

c. Configuración.

El usuario gestionará el alta de los diferentes elementos instalados en los sistemas de control siguiendo las instrucciones del Área de Sistemas de Información y Comunicaciones y del Servicio de Infraestructuras. Cada elemento se ubicará siempre utilizando el código de espacio de localización de la Universitat.

d. Gestores.

El responsable de cada entidad definirá uno o varios

gestors del sistema de control d'accessos, que han de quedar clarament identificats per als usuaris del sistema.

Els gestors seran els encarregats de configurar els permisos d'accés i gestionar els suports per a obertures (claus, etc.).

Els gestors tenen accés a la informació del sistema.

5. Normativa d'ús.

Les directrius d'aquesta Normativa tenen per objectiu establir un estàndard que permeta l'ús de claus i permisos amb la seguretat suficient per a salvaguardar els espais físics de la Universitat Politècnica de València.

Un mitjà d'obertura és potencialment una "clau mestra" que obri tots els panys per als quals es programe i, per tant, cal tractar aquesta "clau mestra" amb la cura que mereix si volem preservar la seguretat de la Universitat.

Tot usuari d'un sistema de control d'accés a la Universitat Politècnica de València ha de disposar d'un mitjà d'obertura que ha de ser sempre nominatiu.

Només excepcionalment es pot disposar de mitjans d'obertura anònims, que atendran la regulació especial que corresponga, i sempre ha d'haver-hi una persona responsable.

Pot haver-hi col·lectius especials, com ara Seguretat (i d'altres), amb permisos d'accés a tots els punts de control.

6. Consulta de registres.

Els sistemes de control d'accés emmagatzemen tant els registres de pas (obertura de portes) com altres esdeveniments del sistema (actualització de permisos, bateries baixes, etc.).

La finalitat principal d'aquests registres és garantir la

gestores del sistema de control de accesos, quedando claramente identificados para los usuarios del sistema.

Los gestores serán los encargados de configurar los permisos de acceso y gestionar los soportes para aperturas (llaves, etc).

Los gestores tendrán acceso a información del sistema.

5. Normativa de uso.

Las directrices de esta Normativa tienen por objetivo establecer un estándar que permita el uso de llaves y permisos con la seguridad suficiente para salvaguardar los espacios físicos de la Universitat Politècnica de València.

Un medio de apertura es potencialmente una "llave maestra" que abre todas las cerraduras que se le programe, y por lo tanto hay que tratar esta "llave maestra" con el cuidado que merece si queremos preservar la seguridad de la Universitat.

Todo usuario de un sistema de control de acceso en la Universitat Politècnica de València debe disponer de un medio de apertura que será siempre nominativo.

Solo excepcionalmente se podrá disponer de medios de apertura anónimos, los cuales atenderán a la regulación especial que corresponda y siempre deberá existir una persona responsable.

Puede haber colectivos especiales como Seguridad (y otros) con permisos de acceso en todos los puntos de control.

6. Consulta de registros.

Los sistemas de control de acceso almacenan tanto los registros de paso (apertura de puertas) como otros eventos del sistema (actualización de permisos, baterías bajas, etc).

La finalidad principal de estos registros es garantizar

seguretat de les instal·lacions de la Universitat Politècnica de València. Es tractaran d'acord amb l'activitat de tractament de control d'accés als edificis.

El responsable de cada entitat és la que nomena els gestors del sistema.

Per a cada sistema, només els usaris gestors tenen accés als registres d'informació. En cas que una porta registre els accessos d'usuaris de diverses entitats, els gestors de cada entitat només poden consultar els registres dels seus usuaris.

7. Manteniment del sistema.

Cada entitat és responsable del manteniment del sistema de control d'accessos instal·lat als seus espais, seguint les directrius de l'Àrea de Sistemes d'Informació i Comunicacions i del Servei d'Infraestructures.

8. Entrada en vigor.

Aquesta Normativa de Sistemes de Control d'Accessos a la Universitat Politècnica de València entra en vigor l'endemà de la publicació en el *Butlletí Oficial de la Universitat Politècnica de València*.

ANNEX I: SISTEMA DE CONTROL D'ACCESSOS SALTO

El present annex refereix detalls de la instal·lació del sistema de control d'accessos Salto.

1. Política d'instal·lació d'unitats de control i obertures en línia.

Les unitats de control es col·loquen en el bastidor de dades més pròxim a la ubicació del lector. Al bastidor hi ha alimentació elèctrica i també hi ha l'electrònica, a la qual cal connectar la unitat.

És necessari coordinar la instal·lació amb l'Àrea de Sistemes d'Informació i Comunicacions o el Servei d'Infraestructures, amb la finalitat de configurar el

la seguridad de las instalaciones de la Universitat Politècnica de València y se tratarán conforme a la actividad de tratamiento Control de acceso a edificios.

El responsable de cada entidad será la persona que nombrará a los gestores del sistema.

Para cada sistema, solo los usuarios gestores tendrán acceso a los registros de información. En caso de que una puerta registre los accesos de usuarios de varias entidades, los gestores de cada entidad solo podrán consultar los registros de sus usuarios.

7. Mantenimiento del sistema.

Cada entidad es responsable del mantenimiento del sistema de control de accesos instalado en sus espacios siguiendo las directrices del Área de Sistemas de Información y Comunicaciones y del Servicio de Infraestructuras.

8. Entrada en vigor.

Esta Normativa de Sistemas de Control de Accesos en la Universitat Politècnica de València entrará en vigor al día siguiente de su publicación en el Butlletí Oficial de la Universitat Politècnica de València.

ANEXO I: SISTEMA DE CONTROL DE ACCESOS SALTO

El presente Anexo refiere detalles de la instalación del sistema de control de accesos Salto.

1. Política de instalación unidades de control y aperturas on-line.

Las unidades de control se colocarán en el rack de datos más cercano a la ubicación del lector. En el rack existe alimentación eléctrica y está la electrónica a la que hay que conectar la unidad.

Será necesario coordinar la instalación con el Área de Sistemas de Información y Comunicaciones o Servicio de Infraestructuras con el fin de configurar

port de l'electrònica i encaminar la unitat perquè funcione correctament.

Si la unitat de control actua sobre alguna porta, també es coordina la manera de fer-ho amb l'Àrea de Sistemes d'Informació i Comunicacions o el Servei d'Infraestructures.

2. Normativa d'ús del sistema Salto.

L'àmbit d'aquesta Normativa inclou a tots aquells usuaris i gestors del sistema de panys electrònics amb el Salto, el més implantat a la universitat.

Mitjà d'obertura:

Tot usuari de Salto disposa d'un mitjà d'obertura nominatiu:

• Un usuari només pot tenir una clau, que és sempre la pròpia acreditació facilitada per la Universitat Politècnica de València.
• Si l'usuari perd o li furten l'acreditació, ha d'avisar com més prompte millor a la gestora o gestor de la seua entitat/departament per a cancel·lar els seus permisos.
• Quan l'acreditació s'ompli de registres *(logs)* d'accés, no permet obrir cap porta. És necessari passar per un actualitzador per a descarregar els registres i que torne a funcionar.
• No es pot usar com a clau una acreditació caducada.

Només excepcionalment es permeten mitjans d'obertura anònims, no nominals, seguint els criteris següents:

• No pot coincidir el nom complet, DNI o NIP (ExtID) amb un usuari de la Universitat Politècnica de València.
• Ha de tenir data d'expiració, com a màxim d'un any.
• Ha de tenir període d'actualització, com a màxim de set dies.
• No pot obrir portes d'altres entitats.
• Ha d'haver-hi una persona responsable.

el puerto de la electrónica y direccionar la unidad para que funcione correctamente.

Si la unidad de control va a actuar sobre alguna puerta también se coordinará la forma de hacerlo con el Área de Sistemas de Información y Comunicaciones o Servicio de Infraestructuras.

2. Normativa de uso sistema Salto.

El ámbito de esta Normativa incluye a todos aquellos usuarios y gestores del sistema de cerraduras electrónicas Salto mayormente implantado en la universidad.

Medio de apertura:

Todo usuario de salto dispondrá de un medio de apertura nominativo:

• Un usuario sólo podrá tener una llave que será siempre su propia acreditación facilitada por la Universitat Politècnica de València.
• Si el usuario pierde o le roban la acreditación deberá avisar cuanto antes al gestor de su entidad/departamento para cancelar sus permisos.

• Cuando la acrditación se llena de logs (registros) de acceso, no le permitirá abrir ninguna puerta. Será necesario pasar por un actualizador para descargar los logs y que vuelva a funcionar.
• No se podrá usar como llave una acreditación caducada.

Solo excepcionalmente se permitirán medios de apertura anónimos, no nominales, siguiendo los siguientes criterios:

• No podrá coincidir el nombre completo, DNI o NIP (ExtID) con un usuario de la Universitat Politècnica de València.
• Tendrá fecha de expiración, como máximo de un año.
• Tendrá periodo de actualización, como máximo de siete días.
• No podrá abrir puertas de otras entidades.
• Deberá existir una persona responsable.

Usuaris:

• Es creen des de l'aplicació de gestió accessible als gestors del sistema de panys electrònics. D'aquesta manera, automàticament es carreguen en el sistema totes les dades de l'usuari, els seus paràmetres estàndard i s'hi associa l'acreditació de la universitat activa.
• El període d'actualització ha de ser com a màxim de set dies. En usuaris amb privilegis especials és menor (seguretat: 12 hores, neteja: 24 hores, etc.).

Gestió:

• El gestors de l'aplicació són nominals.
• Els noms de portes, grups i nivells d'accés han de ser fàcilment identificables per a facilitar la localització i gestió, per exemple: SDI.PuertaPrincipal.
• En donar d'alta una porta, és important emplenar els camps:
o Espai UPV: codi de l'espai (per exemple: V.2E.0.063).
o Actualitzador/lliure: "Actualitzador" si s'escau, en blanc o un altre comentari si no es tracta d'un actualitzador.
o Marcar l'opció "Auditar en les claus".
o Mai s'ha de marcar l'opció "Admetre les claus que han expirat".
• Totes les entitats tenen una zona (grup de portes) amb totes les portes, anomenada "nom de l'entitat/departament" seguit d'un punt i "Totes", per exemple: SDI.Totes.
• Els grups Seguretat. Superusuarios, gestionat pel servei responsable de la seguretat, i el Servei d'Infraestructures. Superusuaris, gestionat pel Servei d'Infraestructures, tenen accés a la zona "Totes" de totes les entitats.
• Les portes s'actualitzen amb el PPD *(portable programming device)* almenys una vegada a l'any o quan l'aplicació ho especifique. Les entitats amb poques portes que no disposen de PPD poden sol·licitar l'actualització o el préstec del PPD a l'Àrea de Sistemes d'Informació i Comunicacions o al Servei d'Infraestructures.

Usuarios:

• Se crearán desde la aplicación de gestión accesible a los gestores del sistema de cerraduras electrónicas. De este modo automáticamente se cargan en el sistema todos los datos del usuario, sus parámetros estándar y se asocia la acreditación de la Universitat activa.
• El periodo de actualización será como máximo de siete días. En usuarios con privilegios especiales será menor (seguridad doce horas, limpieza veinticuatro horas, etc.).

Gestión:

• Los gestores de la aplicación serán nominales.
• Los nombres de las puertas, grupos y niveles de acceso deben ser fácilmente identificables para facilitar la localización y gestión, por ejemplo SDI.PuertaPrincipal.
• Al dar de alta una puerta es importante rellenar los campos:
o Espacio UPV: código del espacio (por ejemplo V.2E.0.063).
o Actualizador/libre: "Actualizador" en su caso, en blanco u otro comentario si no se trata de un actualizador.
o Marcar el check "Auditar en las llaves".
o Nunca marcar el check "Admitir llaves expiradas".

• Todas las entidades tendrán una zona (grupo de puertas) con todas sus puertas llamada "nombre de la entidad/departamento" seguido de un punto y "Todas", por ejemplo SDI.Todas.
• Los grupos Seguridad. Superusuarios gestionados por el servicio responsable de seguridad y el Servicio de Infraestructuras. Superusuarios gestionado por el Servicio de Infraestructuras, tendrán acceso a la zona "Todas" de todas las entidades.
• Las puertas se actualizarán (con el PPD, Portable Programming Device) al menos una vez al año o cuando la aplicación lo especifique. Las entidades con pocas puertas que no dispongan de PPD pueden solicitar la actualización o el préstamo del PPD al Área de Sistemas de Información y Comunicaciones o al Servicio de Infraestructuras.

3. Consulta de registres.

El sistema Salto permet disposar dels perfils gestor, auditor i observador:

- Gestor: pot configurar elements del Salto i permisos d'usuari de la pròpia entitat.
- Auditor: pot veure tots els registres del sistema de la pròpia entitat.
- Observador: pot veure alguns registres del sistema de la pròpia entitat (bateries baixes, etc.) exclosos els d'accés.

Només els usuaris amb perfil auditor poden accedir als registres del sistema.

El responsable de cada entitat indica a l'Àrea de Sistemes d'Informació i Comunicacions o al Servei d'Infraestructures quins usuaris ha de tenir cada perfil: gestor, auditor i observador. Un usuari gestor pot modificar els perfils dels usuaris gestor, auditor i observador del seu departament.

En portes compartides per diverses entitats, els registres visibles per cada entitat són només els dels usuaris de la seua entitat, mai els de la resta d'entitats.

3. Consulta de registros.

El sistema Salto permite disponer de los perfiles gestor, auditor y ojeador:

- Gestor: puede configurar elementos de salto y permisos de usuario de la propia entidad.
- Auditor: puede ver todos los registros del sistema de la propia entidad.
- Ojeador: puede ver algunos registros del sistema de la propia entidad (baterías bajas, etc) excluyendo los de acceso.

Solo los usuarios con perfil auditor pueden acceder a los registros del sistema.

El responsable de cada entidad indicará al Área de Sistemas de Información y Comunicaciones o al Servicio de Infraestructuras qué usuarios deben tener cada perfil: gestor, auditor y ojeador. Un usuario gestor podrá modificar los perfiles de los usuarios gestor, auditor y ojeador de su departamento.

En puertas compartidas por varias entidades, los registros visibles por cada entidad serán solo los de los usuarios de su entidad, nunca los del resto de entidades.