VNIVERSITAT DE VALÈNCIA
Fundació General

[SGSI] NORMATIVA DE SEGURETAT

ÍNDEX

1. OBJECTE

L'objecte del present document és establir la normativa d'ús segur dels sistemes d'informació en la Fundació General de la Universitat de València (d'ara en avant, la FGUV), dins de l'abast assenyalat en l'Esquema Nacional de Seguretat.

La seguretat sempre ha sigut un concepte present en tots els sistemes de gestió de la informació. La seua implementació no és senzilla, atès que abasta totes les baules de la cadena de gestió de la informació i requereix d'un gran conjunt de mesures organitzatives i tecnològiques.

L'èxit de la seua implantació depén a més del fet que existisca en tots els nivells una cultura de la seguretat, és a dir, una conscienciació sobre la necessitat que la informació es mantinga en secret, íntegra i disponible.

Per tant, l'usuari final necessita ser conscienciat i culturitzat en matèria de seguretat de la informació i, al mateix temps, ha de disposar d'unes normes d'obligat compliment respecte a l'ús dels sistemes informàtics al seu abast, així com suports o documents en paper i, amb especial rellevància, quant a preservar la confidencialitat de la informació de caràcter personal que estiga sent tractada en compliment de la legislació vigent.

El present document estableix les normes d'ús dels dispositius assignats al lloc de treball, la xarxa corporativa, equips portàtils, aplicacions informàtiques, així com a l'accés i tractament de dades de caràcter personal en suport electrònic i en paper.

És fonamental que tots els empleats de la FGUV que utilitzen equipament informàtic i accedisquen o tracten informació de caràcter personal per a la realització de les seues funcions i tasques siguen coneixedors d'aquesta norma.

S'ha implantat la següent normativa atès el nivell de seguretat de la informació i els serveis prestats i la categoria dels sistemes de la FGUV que resulten de l'aplicació de les previsions contemplades en els annexos I i II del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica (ENS).

2. ABAST

Aquesta normativa d'ús dels sistemes d'informació és aplicable a tot l'àmbit d'actuació de la FGUV i els seus continguts provenen de les directrius de caràcter més general definides en la normativa vigent i en la `política de seguretat de la informació de la FGUV.

La present normativa és aplicable i d'obligat compliment per a tots aquells usuaris/àries dels sistemes d'informació, entenent per tals:

- Tot el personal que de manera permanent o eventual faça les seues tasques o preste els seus serveis en la FGUV.

- El personal en pràctiques de la FGUV.

- El personal de la Universitat de València amb accés als sistemes d'informació de la FGUV.

- Els proveïdors externs amb accés als sistemes d'informació de la FGUV.

I de manera especial, la present normativa es dirigeix al responsable de seguretat i als responsables dels sistemes d'informació.

Legislació i normativa aplicable

Per a la redacció d'aquest document s'han seguit les normes indicades en els documents següents:

- La Guia "CCN-STIC-821 Normes de seguretat en el ENS" i

- L'annex I de la Guia "CCN-STIC-822" – Procediments de seguretat en l'ENS".

- La llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

3. ROLS I RESPONSABILITATS

ROL	RESPONSABILITATS
Responsable de la seguretat	**Elaborar** la normativa d'ús dels sistemes d'informació
Comitè de Seguretat	**Aprovar** la normativa d'ús dels sistemes d'informació
Usuaris	**Complir** la normativa d'ús dels sistemes d'informació

4. NORMATIVA INTERNA D'ÚS DELS SISTEMES D'INFORMACIÓ

4.1 OBLIGACIONS DE LA FGUV

La FGUV proporciona als i les usuaris/àries l'equipament informàtic necessari per a la realització de les tasques relacionades amb el seu lloc de treball. Aquest equipament passarà per un procés de fortificació previ al seu lliurament, això és, el procés d'assegurar un sistema mitjançant la reducció de vulnerabilitats en aquest.

En els casos en els quals l'usuari aporte els seus propis dispositius, la FGUV procedirà a establir les mesures de seguretat adequades.

4.2 ÚS DELS DISPOSITIUS INFORMÀTICS

Els dispositius, que són propietat de la FGUV, estan destinats a un ús exclusivament laboral. No obstant això, la FGUV autoritza l'existència d'un hàbit social generalitzat de tolerància amb certs usos personals moderats dels mitjans informàtics i de comunicació facilitats al personal de la FGUV.

Els i les usuaris/àries han de complir les següents mesures de seguretat per a l'ús de l'equipament informàtic que se'ls haja proporcionat per a les tasques relacionades amb el seu lloc de treball:

Connexió d'altres dispositius	- No està permès connectar a la xarxa de la UV dispositius que no estiguen autoritzats. - Tampoc es poden connectar als dispositius autoritzats altres dispositius que no estiguen autoritzats expressament (per exemple, discos durs externs, pendrives...)
Localització del dispositiu	- No està permès canviar la localització física dels dispositius assignats a una lloc concret sense l'autorització prèvia del responsable del sistema.
Configuració del dispositiu	- No està permès alterar la configuració física ni la de seguretat ni el programari dels dispositius.

Ús de dispositius i de la xarxa	Els dispositius, així com la xarxa d'informació que la FGUV posa a la disposició dels usuaris estan destinats a permetre l'acompliment de les funcions i tasques professionals que aquests tenen encomanades.
Ús de la informació	- Està prohibit utilitzar, copiar o transmetre informació continguda en els sistemes informàtics per a ús privat o qualsevol altre diferent del servei al qual està destinada. - L'usuari s'abstindrà de copiar la informació continguda en els fitxers en els quals s'emmagatzemen dades de caràcter personal o un altre tipus d'informació de la FGUV en un ordinador propi, pendrives o qualsevol altre suport informàtic, llevat que sol·licite l'autorització al responsable de seguretat i s'adopten les mesures de seguretat corresponents. - Així mateix, les dades contingudes en aquest tipus de suports han de ser suprimides una vegada hagen deixat de ser útils i pertinents per a la satisfacció de les finalitats que van motivar la seua creació. - Durant el període de temps que els fitxers o arxius romanguen en l'equip o suport informàtic extern s'haurà de restringir l'accés i l'ús de la informació que estiga en aquests. - S'establiran mesures de protecció addicionals que asseguren la confidencialitat de la informació emmagatzemada en l'equip o quan es tracte de dades de caràcter personal que requerisquen les mesures de seguretat establertes per la legislació vigent.

Identificació i autenticació	Les contrasenyes d'accés a l'equip, el sistema i/o la xarxa, concedides per la FGUV són personals i intransferibles. L'usuari serà l'únic responsable de les conseqüències que es puguen derivar del seu mal ús, divulgació o pèrdua. - Per qüestions de seguretat no estan permeses pràctiques com: 1. Emprar identificadors i contrasenyes d'altres usuaris per a accedir al sistema i a la xarxa de la UV. 2. Intentar modificar o accedir al registre d'accessos. 3. Burlar les mesures de seguretat establertes en el sistema informàtic intentant accedir a fitxers.
Identificació i autenticació - doble factor d'autenticació	Amb la finalitat de reforçar la seguretat de l'accés als sistemes, la FGUV implementa un mecanisme d'autenticació multifactor (2FA) per als comptes d'usuari de les plataformes Google Workspace i Microsoft 365. Aquesta mesura està alineada amb els principis de l'Esquema Nacional de Seguretat (ENS), especialment amb els relatius a la protecció enfront d'accessos no autoritzats. - Tots els usuaris amb accés a informació tindran actiu i habilitat el 2FA. - Està prohibit desactivar aquest sistema de verificació sense l'autorització expressa de l'àrea de seguretat de la informació. - La pèrdua del dispositiu configurat per al segon factor s'ha de comunicar immediatament al Departament d'Informàtica. **Aplicació en Microsoft 365** Per als comptes de Microsoft 365 s'utilitza Microsoft Authenticator mitjançant notificació push o codis temporals. Opcionalment es permet l'ús de codi temporal de seguretat enviat per SMS i/o per telefonades. L'accés al portal de Microsoft i a aplicacions vinculades

	requereix obligatòriament aquesta segona verificació. **Aplicació en Google Workspace** En l'entorn de Google Workspace s'empra el doble factor mitjançant notificacions push a través de l'aplicació Google Authenticator. Opcionalment es permet l'ús de codi temporal de seguretat enviat per SMS i codis de seguretat generats en el panell d'administració. **Aplicació SAGE50** En l'entorn de Sage50 s'empra el doble factor mitjançant notificacions push a través de l'aplicació d'autenticació (recomanable Google Authenticator). Opcionalment es permet l'ús de codi temporal de seguretat enviat per SMS i/o per telefonades.

La normativa es complementa en la política d'ús de dispositius mòbils i en el *Manual d'ús del correu corporatiu*, que formen part del *Manual de protecció de dades de la FGUV*.

4.3 ÚS DE LA XARXA CORPORATIVA

La xarxa corporativa és un recurs compartit i limitat. Aquest recurs serveix no sols per a l'accés dels usuaris interns de la FGUV a la intranet o internet, sinó també per a l'accés a les diferents aplicacions informàtiques corporatives i la comunicació de dades entre sistemes de temps real i explotació.

Ús d'internet	- La utilització d'internet per part dels usuaris autoritzats ha de limitar-se a l'obtenció d'informació relacionada amb el treball que es fa.

Ús del correu electrònic	- El correu electrònic corporatiu es considera com un instrument bàsic de treball. - L'ús del correu electrònic corporatiu és exclusivament laboral. - L'accés al correu es realitzarà mitjançant una identificació consistent proporcionada pel proveïdor del servei. - Els enviaments massius d'informació, així com els correus que es destinen a gran nombre d'usuaris seran els estrictament necessaris per a impedir un col·lapse del sistema de correu i s'hauran de regir pel procediment de creació de llistes de distribució establert en la FGUV, que garanteix el compliment de la normativa de protecció de dades. - No s'hauran d'obrir annexos de missatges ni fitxers sospitosos o dels quals no es conega la procedència. - La normativa completa sobre l'ús del correu electrònic es pot consultar en l'annex 13-*Manual del correu corporatiu,* que forma part del *Manual de protecció de dades de la FGUV*.
Compartició de continguts	Es prohibeix l'ús de programes de compartició de continguts no autoritzats, que s'utilitzen habitualment per a descarregar arxius de música, vídeo, etc.

4.4. ACCÉS A APLICACIONS I SERVEIS CORPORATIUS

Tant l'equipament informàtic com tots els recursos facilitats a l'usuari per a la realització de les tasques relacionades amb el seu lloc de treball (com ara aplicacions informàtiques, servidor de dades, etc.) són propietat de la FGUV, per la qual cosa se n'haurà de fer un ús diligent.

Els usuaris han de complir les següents mesures de seguretat establertes per la FGUV per a l'ús d'aplicacions i serveis corporatius:

Identificació i autenticació	- Tant l'accés a l'ordinador com a les diferents aplicacions corporatives serà identificat (mitjançant l'usuari i la contrasenya). - Els sistemes que ho permeten (AzureAD per a accedir als equips i GSuite) aplicaran la política de contrasenyes següent: - Longitud mínima: vuit caràcters - Ha d'incloure com a mínim un caràcter, una majúscula i un nombre. - Obligatorietat de canvi cada 365 dies.
Custòdia de les contrasenyes	- La custòdia de la contrasenya és responsabilitat de l'usuari. No s'ha d'utilitzar mai el compte d'usuari assignat a una altra persona. - Les contrasenyes no s'han d'anotar, s'han de recordar.
Renovació de les contrasenyes	- En els sistemes que ho permeten es demanarà a l'usuari que canvie la contrasenya cada 365 dies. A més, els usuaris disposen de mecanismes per a modificar la contrasenya d'accés sempre que ho consideren convenient i en sistemes que no permeten el canvi automatitzat. Això garanteix l'ús privat d'aquestes.
Incidències amb les contrasenyes	- Quan es considere que la identificació d'accés s'ha vist compromesa s'haurà de comunicar al responsable de seguretat enviant un correu-e a la següent adreça de correu: comitedeseguretat.fguv@uv.es, segons el procediment de registre i gestió d'incidències. Això resulta també d'aplicació a la informació en paper. El procediment es complementa amb l'annex 4 del *Manual de protecció de dades de la FGUV*.

Suports informàtics (pendrives i discos durs externs, USB, CD, DVD, disquets, etc.)	- L'eixida de suports dels locals de la FGUV que continguen dades de nivell alt l'ha d'autoritzar expressament el responsable de la informació (o el responsable del tractament si tal figura està personalitzada). - L'entrada de suports que continguen dades personals haurà de quedar registrada d'acord amb el procediment de transport i entrada i eixida de suports en la FGUV. Així mateix, el suport haurà de ser donat d'alta en l'inventari de suports, d'acord amb el procediment establert en la FGUV. - No estan permeses les unitats externes d'emmagatzematge de la informació per a ús privat, com ara disquets, pendrives, discos durs externs, CD-R, DVD-R, etc. - En cas de necessitar rebutjar un suport que continga dades personals, es dirigirà una petició en tal sentit al Departament d'Informàtica i es destruirà mitjançant l'adopció de mesures dirigides a evitar l'accés a la informació continguda en aquest o la seua recuperació posterior. El Departament d'Informàtica compta amb l'equipament necessari per a destruir la informació de manera segura i irreversible. Així mateix, el suport haurà de ser donat de baixa de l'inventari corresponent.

4.5. FITXERS EN FORMAT NO DIGITAL

En relació amb els fitxers en suport o documents en paper, l'usuari haurà d'observar les següents diligències, indicades anteriorment, respecte a la confidencialitat de la informació, accés autoritzat a la informació en atenció a les necessitats del seu treball, la gestió de suports i documents i el treball fora de les instal·lacions de la FGUV.

Arxivadors o dependències	- Mantenir degudament custodiades les claus d'accés als locals o dependències, despatxos, així com els armaris, arxivadors o altres elements que continguen suports o documents en paper amb dades de caràcter personal.
Emmagatzematge de documents	- Els suports o documents en paper hauran de ser emmagatzemats seguint el criteri d'arxiu de la FGUV. Aquests criteris hauran de garantir la correcta conservació dels documents i la localització i consulta de la informació.
Custòdia de documents	- Quan els documents en suport paper no es troben emmagatzemats per estar sent revisats o tramitats, serà la persona que es trobe al seu càrrec la que haja de custodiar i impedir en tot moment que un tercer no autoritzat hi puga tenir accés. - Guardar tots els suports o documents que continguen informació de caràcter personal en un lloc segur quan aquests no siguen usats, particularment fora de la jornada de treball. - Assegurar que no queden documents impresos que continguen dades personals en la safata d'eixida de la fotocopiadora, la impressora o els faxos. - S'haurà de mantenir la confidencialitat de les dades personals que consten en els documents dipositats o emmagatzemats en les taules de treball, els taulells o en un altre mobiliari.

Trasllat	- En els trasllats de documents s'hauran d'adoptar mesures dirigides a impedir l'accés o manipulació per tercers de manera que no se'n puga veure el contingut, sobretot si hi ha dades de caràcter personal. - En cas de canviar de dependència, el trasllat dels documents en suport paper s'haurà de fer amb l'ordre degut. Així mateix, es procurarà mantenir fora de l'abast de la vista de qualsevol membre del personal de l'entitat aquells documents o suports en paper en què consten dades de caràcter personal.
Destrucció	- No tirar suports o documents en paper que continguen dades personals a papereres o contenidors, de manera que la informació puga ser llegible o fàcilment recuperable. - A aquest efecte, s'haurà de rebutjar o destruir sempre mitjançant una destructora de paper o un altre mitjà de què dispose la FGUV.

Incidències	- Comunicar amb la major diligència possible al responsable de seguretat (enviant un correu electrònic a comitedeseguretat.fguv@uv.es) les incidències de seguretat de les quals es tinga coneixement i que puguen afectar la seguretat de les dades personals. - Entre altres, tenen la consideració d'incidència de seguretat que afecta els fitxers en paper els fets següents: o Pèrdua de les claus d'accés als arxius, armaris i/o dependències on s'emmagatzema la informació de caràcter personal. o Ús indegut de les claus d'accés. o Accés no autoritzat d'usuaris als arxius, armaris i/o dependències on es troben fitxers amb dades de caràcter personal. o Pèrdua de suports o documents en paper amb dades de caràcter personal. o Deterioració dels suports o documents, armaris o arxius on es troben dades de caràcter personal.

4.6. INCIDÈNCIES DE SEGURETAT

Els usuaris hauran de notificar al Departament d'Informàtica com més prompte millor qualsevol comportament anòmal del seu ordinador personal, especialment quan existisquen sospites que s'haja produït algun incident de seguretat en aquest.

Quan un usuari detecte qualsevol anomalia o incidència de seguretat que puga comprometre el bon ús i funcionament dels sistemes d'informació de la Fundació General de la Universitat de València o la seua imatge, haurà d'informar immediatament al Departament d'Informàtica per correu-e a informatica.fguv@uv.es, que ho registrarà degudament i elevarà si és el cas.

Cal notificar al Departament d'Informàtica qualsevol anomalia detectada en l'ús de l'accés a internet, així com la sospita de possibles problemes o incidents de seguretat relacionats amb aquest accés.

4.7. MONITORITZACIÓ I APLICACIÓ D'AQUESTA NORMATIVA

La FGUV, per motius legals, de seguretat i de qualitat del servei i complint en tot moment els requisits que a aquest efecte estableix la legislació vigent pot:

A. Revisar periòdicament l'estat dels equips, el programari instal·lat, els dispositius i les xarxes de comunicacions de la seua responsabilitat.
B. Monitorar els accessos a la informació continguda en els seus sistemes.
C. Auditar la seguretat de les credencials i les aplicacions.
D. Monitorar els serveis d'internet, correu electrònic i altres eines de col·laboració.

La FGUV portarà a cap aquesta activitat de monitoratge de manera proporcional amb el risc, amb les cauteles legals pertinents i les assenyalades en la jurisprudència, i amb observança dels drets dels usuaris

Els sistemes en els quals es detecte un ús inadequat o en els quals no es complisquen els requisits mínims de seguretat, podran ser bloquejats o suspesos temporalment, amb l'avís previ a l'usuari. El servei es restablirà quan la causa de la seua inseguretat o degradació desaparega. El Departament d'Informàtica, amb la col·laboració de les restants unitats de la FGUV, vetlarà pel compliment de la present normativa general.

El sistema que proporciona el servei de correu electrònic podrà rebutjar, bloquejar o eliminar de manera automatitzada part del contingut dels missatges enviats o rebuts en els quals es detecte algun problema de seguretat o d'incompliment de la present normativa. Es podrà inserir algun contingut addicional en els missatges enviats a fi d'advertir els receptors d'aquests dels requisits legals i de seguretat que hauran de complir en relació amb aquests correus.

5. PROCÉS DISCIPLINARI

Tots els usuaris dels sistemes d'informació i dels recursos informàtics de la FGUV estan obligats a complir el que s'estableix en la present normativa de seguretat.

Qualsevol incompliment del que s'ha indicat en la present normativa, ja siga de manera intencionada o per un comportament negligent, pot donar lloc a la suspensió temporal o definitiva de l'ús dels recursos i serveis assignats a l'usuari, sense perjudici de la revisió dels fets concrets en l'àmbit de la normativa disciplinària, i, de manera general, de les responsabilitats que, si és el cas, corresponguen en matèria administrativa, civil o penal.

Les conseqüències de l'incompliment per a l'infractor i les mesures aplicables seran adoptades de conformitat amb les normes que regulen la relació laboral i/o de prestació de serveis entre la FGUV i l'usuari.

6. MODEL D'ACCEPTACIÓ I COMPROMÍS DE COMPLIMENT

Tots els usuaris dels recursos informàtics i/o sistemes d'informació de la FGUV hauran de tenir accés permanent durant el temps d'acompliment de les seues funcions a la present normativa de seguretat, que es trobarà disponible en la intranet de la FGUV.

Els usuaris dels sistemes d'informació de la FGUV hauran de signar el següent compromís de compliment de la normativa de seguretat de la FGUV.

Organització:

Treballador/a (nom i cognoms):

DNI núm.:

COMPROMÍS DE COMPLIMENT DE LA NORMATIVA DE SEGURETAT DE LA FGUV

Per mitjà del present compromís, el/la Sr./Sra ……., com a usuari/ària de recursos informàtics i sistemes d'informació de la FGUV, declara haver llegit i comprès la present normativa de seguretat, accepta els termes i condicions d'ús establertes en aquesta, està d'acord a complir-los i a atendre les modificacions del document que li hagen sigut degudament comunicades, i es compromet, sota la seua responsabilitat, al seu compliment.

_____, a ____ d _____ de 20_