COL·LEGI ASUNCION NTRA. SRA.
Centre concertat per la Generalitat de Catalunya
www.asuncion.cat

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

4.- PROTOCOL D'ÚS DE LES TIC

4.1.- DEFINICIONS.

• **Accessos autoritzats**: Autoritzacions o permisos atorgats a un usuari per què pugui fer servir diversos recursos.

• **Administrador del sistema:** Usuari privilegiat del sistema informàtic que li permet canviar configuracions. Té la responsabilitat d'executar, mantenir, operar i assegurar el funcionament correcte d'un sistema informàtic i/o xarxa.

• **Autenticació**: Procediment de comprovació de la identitat d'un usuari. Garanteix que l'usuari que accedeix a un sistema d'ordinador és qui diu ser. En general, els sistemes d'autenticació estan basats en una clau, codi o contrasenya privada i secreta posada pel propi usuari.

• **Autenticador:** Codi d'accés, contrasenya.

• **Bloc:** Pàgina *web*, generalment de caràcter personal, amb una estructura cronològica que s'actualitza regularment i que presenta informació o opinions sobre temes diversos

• **Contrasenya**: Informació de caràcter confidencial, freqüentment constituïda per una cadena de caràcters, que es pot fer servir per a autenticar un usuari.

• **Còpia de suport**: Còpia de les dades d'un fitxer automatitzat a un suport que permeti la recuperació. Es pot desar al mateix lloc en el que s'ha fet la còpia.

• **Còpia de recuperació**: Còpia de les dades d'un fitxer automatitzat a un suport que permeti la recuperació. La còpia de recuperació s'ha de desar fora dels locals en els que estigui l'ordinador origen de la còpia.

• **Directoris de correu**: Conjunt d'adreces electròniques, estructurat per fer recerques. És un concepte similar al de "guia telefònica", aplicat a les adreces electròniques.

• **Domini o Nom de Domini**: És un nom registrat que identifica el lloc de la xarxa d'una organització accessible pels usuaris d'Internet. Per exemple, <cipdi.com> és el nom de domini del Centre Integral de Protecció de la Informació.

• **Driver**: Es un controlador de dispositiu, anomenat normalment controlador (en anglès, device driver) és un programa informàtic que permet al sistema operatiu interactuar amb un perifèric. El programa interactua amb un dispositiu extern a l'aparell que conté el sistema operatiu. El "driver" conté informació especifica sobre el dispositiu i fa de mitjancer entre el dispositiu i el sistema operatiu.

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

• **Firewall**: Aplicació de seguretat que regula i controla l'accés als sistemes connectats a Internet.

• **HTML (HyperText Markup Language)**: Llenguatge de marcat d'Hipertext. És el llenguatge estàndard per descriure el contingut i l'aparença de les pàgines en Internet. Els navegadors interpreten aquest llenguatge per presentar la informació a l'usuari.

• **HTTP (HiperText Transfer Protocol)**: Protocol de Transmissió Hipertext. Protocol de comunicacions utilitzat pels programes clients i servidors de WWW per comunicar-se entre si.

• **Identificador:** Símbol, caràcter o grup de caràcters, usat per a designar un element individual de les dades d'un programa**.**

• **Internet**: Xarxa digital de transmissió basada en el protocol TCP/IP que interconnecta entre si xarxes de menor mida, permetent la comunicació entre qualsevol parell d'ordinadors connectats a aquestes xarxes subsidiàries.

• **Núvol:** model que permet, de forma pràctica i des de qualsevol ubicació, l'accés sota demanda a una sèrie de recursos informàtics configurables compartits (xarxes, servidors, sistemes d'emmagatzematge, aplicacions i serveis), que poden ser ràpidament dotats i posats en funcionament amb un mínim esforç de gestió i interacció amb el proveïdor de serveis ".

• **Núvol públic:** És aquell tipus de cloud (núvol) en el qual la infraestructura i els recursos lògics estan sota el control del proveïdor de serveis que l'allotja, opera i gestiona, estant disponible per al públic en general.

• **Núvol privat:** D'ús exclusiu per a una organització, es crea generalment amb recursos propis de l'empresa.

• **Núvol comunitari:** Un cloud comunitari es dóna quan dues o més organitzacions integren una comunitat que comparteix interessos i comparteixen els beneficis d'una infraestructura cloud comuna, que es gestiona per una d'elles o per una tercera part en nom seu.

• **Núvol híbrid:** La infraestructura és el resultat de la combinació de diverses de les anteriors, incloent-hi els mitjans per a la connexió i la portabilitat de la informació entre les diferents estructures

• **IRC (*Internet Relay Chat***): Xerrada Interactiva a Internet. Protocol per a converses simultànies que permet comunicar-se entre si a diverses persones en temps real.

• **Recurs**: Qualsevol part que integra un sistema d'informació.

COL·LEGI ASUNCION NTRA. SRA.
Centre concertat per la Generalitat de Catalunya
www.asuncion.cat

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

• **Servidor Web**: És el programa que, utilitzant el protocol de comunicacions HTTP, és capaç de rebre peticions d'informació d'un programa client (navegador), recuperar la informació sol·licitada i enviar-la al programa client per a que l'usuari la pugui veure.

• **Servidor Web segur**: Servidor Web que utilitza protocols de seguretat (SSL o SHTTP generalment) quan executa transaccions. Un protocol de seguretat utilitza tècniques de xifrat i autenticació com instrument per incrementar la confidencialitat i la fiabilitat de les transaccions.

• **SHTTP (Secure HTTPS**): Sistema encaminat a proporcionar transaccions segures dins de l'entorn World Wide Web.

• **Sistema d'informació**: Conjunt de fitxers automatitzats, programes, suports i equips que es fan servir per a enregistrar i tractar dades.

• **Suport**: Objecte físic susceptible de ser tractat en un sistema d'informació i sobre el qual es poden gravar o recuperar dades. El suport no forma part de la informació. Així, les fotografies són suports que contenen informació sobre les persones. L'afectat té dret a la informació que contenen els suports i, de vegades, a la titularitat dels suports.

• **Spam**: Tramesa massiva de missatges publicitaris que el destinatari no ha demanat expressament, fent servir el correu electrònic. Els qui es dediquen a aquesta activitat reben el nom de "spammers".

• **SSL (Secure Sockets Layer**): El protocol de seguretat més usat en Internet. Fa servir criptografia asimètrica per generar una clau de sessió amb què es xifren les comunicacions entre el client i el servidor. Proporciona també serveis d'autenticació del servidor i, opcionalment, del client.

• **Transferència de dades**: el transport de dades entre sistemes informàtics per qualsevol mitjà de transmissió, així com el transport de suports de dades per correu o per qualsevol altre mitjà convencional.

• **Usuari**: Subjecte o procés autoritzat per accedir a dades o recursos. A efectes de la normativa sobre telecomunicacions, la persona que utilitza un servei públic de telecomunicacions amb finalitats privades o comercials, encara que no sigui ell directament qui hagi contractat aquest servei.

• **Xarxa pública de telecomunicacions**: Els sistemes de transmissió i, quan sigui procedent, els equips de commutació i altres recursos que permeten la transmissió de senyals entre punts d'acabament definits per cable, per mitjans radioelèctrics, per mitjans òptics o per mitjans electromagnètics que s'utilitzin, de manera total o parcial, per a la prestació de serveis públics de telecomunicacions.

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

• **Xifrat**: Transformació d'un missatge en un altre, utilitzant una clau per impedir que el missatge transformat pugui ser interpretat per aquells que no coneixen la clau.

4.2.- GENERAL.

S'ha d'identificar a totes les persones amb permisos per a accedir al sistema d'informació del centre. A més de la identificació, cal establir un procediment d'autenticació. L'identificador i l'autenticador, en conjunt, es nomena contrasenya.

L'autenticador ha de ser secret i intransferible. Si l'usuari detecta, o sospita, que algú pot conèixer el seu autenticador, ho ha de posar en coneixement de la Direcció, mitjançant una comunicació d'incidència.

La informació és propietat del col·legi. S'han de fer còpies de seguretat de tota la informació que hi ha al centre. Les còpies de seguretat han d'estar permanentment a disposició de la direcció del centre.

El sistema d'informació del centre només es pot fer per als fins expressament autoritzats per la direcció.

No està permès:

1. Compartir o facilitar la clau d'accés (contrasenya) a una altra persona física o jurídica, inclòs el personal del col·legi, ni que tingui més categoria jeràrquica. En cas d'incompliment d'aquesta prohibició, l'usuari es el responsable dels actes que faci la persona física o jurídica que hagi simulat ser el titular de la contrasenya
2. Intentar distorsionar o falsejar els registres LOG del sistema.
3. Intentar desxifrar les claus, sistemes, o algoritmes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics del col·legi.
4. Destruir, alterar, inutilitzar o, de qualsevol altra forma, fer malbé les dades, programes, o documents electrònics del col·legi.
5. Obstaculitzar voluntàriament l'accés d'altres usuaris a la xarxa mitjançant el consum massiu dels recursos informàtics i telemàtics, així com fer accions que facin malbé, interrompin, o generin errors en els sistemes.
6. Enviar missatges de correu electrònic de forma massiva o amb finalitats comercials, o publicitàries sense el consentiment del destinatari (Spam).
7. Intentar llegir, esborrar, copiar, o modificar els missatges de correu electrònic o arxius d'altres usuaris.
8. Fer servir el sistema per intentar accedir a àrees restringides dels sistemes informàtics del col·legi.
9. Intentar augmentar el nivell de privilegis d'un usuari del sistema, sense el

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

permís exprés de la direcció.

10. Introduir voluntàriament programes, virus, macros, applets, controls ActiveX o qualsevol altre dispositiu lògic o seqüència de caràcters que causin, o siguin susceptibles de causar, qualsevol tipus d'alteració als sistemes informàtics del col·legi sense el permís de la direcció.
11. Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics o arxius que no estiguin autoritzats expressament per la direcció del col·legi.
12. Instal·lar còpies il·legals de qualsevol programa, incloses les dels estandarditzats.
13. Esborrar qualsevol dels programes instal·lats legalment.
14. Fer servir els recursos telemàtics del col·legi per a activitats que no es trobin directament relacionades amb el lloc de treball de l'usuari.
15. Introduir, consultar o descarregar continguts obscens, immorals o ofensius i, en general, mancats d'utilitat per assolir els objectius del col·legi.
16. Enviar o reexpedir missatges en cadena o de tipus piramidal sense permís de la direcció.
17. Accedir i/o fer servir informació sobre persones físiques o jurídiques identificades o identificables a la xarxa sense el permís de la direcció.
18. Fer servir suports de qualsevol tipus, núvols, correus electrònics, xarxes socials, xats, pàgines de noticies, blocs i programes de descàrrega, sense l'autorització de la direcció.

S'han de bloquejar els usuaris quan s'acabi la relació entre l'usuari i el centre, o quan es detecti que l'usuari ha fet alguna de les activitats que no estan permeses.

4.3.- XARXA INTERNA.

Només es pot accedir a la xarxa interna del col·legi amb l'identificador i el primer autenticador assignat per la direcció del centre.

S'ha de bloquejar l'accés al sistema quan s'acabi de treballar en xarxa, o durant períodes d'inactivitat superior a cinc minuts.

El primer cop que es connecti a la xarxa, li apareixerà el missatge que s'adjunta com a document PT1, que haurà de ser acceptat expressament per poder validar-se.

A la xarxa han d'haver-hi diferents tipus de carpetes:

a) Carpetes personals: són les que contenen informació personal de l'usuari i només hi poden accedir les persones que consenti el propi usuari titular.

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

b) Carpetes compartides: Carpetes a les que poden accedir persones amb els mateixos privilegis.

c) Carpetes públiques: Carpetes d'accés lliure als usuaris de la xarxa.

És important que es respecti aquesta distribució de carpetes per evitar l'accés a informació per part de persones no autoritzades.

4.3.1.- Accés a la xarxa amb els ordinadors del col·legi.

4.3.1.1.- Accés del personal.

No es pot connectar cap suport (pendrive, portàtil, etc.) sense el permís exprés de la direcció del centre.

4.3.1.2.- Accés dels alumnes.

L'exploració de l'equip i la navegació per la xarxa ha d'estar limitada, i serà controlada pel professors.

Els alumnes només poden desar els documents a les carpetes autoritzades pel professor.

4.3.2.- Accés a la xarxa amb ordinadors i aparells propis.

4.3.2.1- Accés per part del personal

Ha de ser expressament autoritzada per la direcció. El director només autoritzarà la connexió d' aparells a la xarxa del centre quan:

a) Estigui justificada.

b) L'usuari garanteixi que aplicarà les mesures de seguretat previstes al Reglament Intern de Seguretat.

4.3.2.2.- Accés per part dels alumnes.

Per poder donar accés als alumnes a la xarxa, els seus representants legals han de signar el document d'assumpció de responsabilitat (PT2).

4.3.2.2.1.- Els aparells són dels alumnes.

Ha de ser expressament autoritzada per la direcció del col·legi. El director del col·legi només autoritzarà la connexió d' aparells a la xarxa del centre quan:

c) Estigui justificada.

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

d) L'usuari garanteixi que aplicarà les mesures de seguretat descrites al Reglament Intern de Seguretat.

A l'aula, els ordinadors personals han d'estar tancats. El professor pot decidir el moment en què els alumnes estan autoritzats a obrir o tancar l'ordinador. Dins de les aules, els ordinadors han de romandre amb la pantalla tancada fins que el professor en permeti l'ús.

Quan no s'estiguin fent servir, els ordinadors es poden guardar a unes taquilles personals. La taquilla per desar el portàtil ha de disposar d'una clau d'obertura pròpia. Els tutors i els coordinadors tindran a la seva disposició una còpia de la clau de les taquilles dels alumnes, però no la faran servir si no es estrictament necessari i sempre que la direcció ho permeti.

Està prohibit fer servir els ordinadors al pati, als passadissos, al menjador i en els espais d'esbarjo, sense una autorització expressa (per escrit) d'un professor autoritzat.

Només es poden fer servir els ordinadors portàtils personals dins el recinte del col·legi per fer tasques relacionades amb el centre.

Només es poden fer servir auriculars i "webcams" quan el professor ho permeti.

L'alumne ha de portar la bateria carregada de casa i els portàtils han de estar degudament identificats amb etiquetes amb el seu nom.

Quan l'ordinador o un altre aparell que contingui informació és propietat exclusiva de l'alumne, el professor no pot accedir al seu contingut sense el consentiment exprés de l'alumne. No obstant això, si observa que l'alumne vulnera alguna de les normes establertes en el reglament del centre, pot intervenir l'ordinador, demanant-li a l'alumne que el tanqui i que el dugui a la Direcció. El director podrà demanar a l'alumne que l'obri i li lliuri per a comprovar el que calgui o, en cas de que l'alumne es negui, el director podrà requerir al representant legal de l'alumne per lliurar-li l'aparell prèvia signatura de l'imprès assolint la responsabilitat que el Director consideri adient.

4.3.2.2.2.- Els aparells estan dintre del programa educat 1 x 1

S'ha d'aplicar la mateixa normativa descrita al punt anterior. El sistema sancionador varia en el sentit que el coordinador d'informàtica pot restaurar el sistema si els professors detecten que l'alumne ha fet servir l'ordinador de manera antireglamentària.

4.3.2.2.3.- La connexió de telèfons mòbils.

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

Està prohibida sense l'autorització expressa de la direcció. Es poden intervenir de la manera descrita al punt 3.2.2.1 d'aquest protocol.

4.4.- PLATAFORMA.

Per accedir a la plataforma convé fer servir protocols de connexió segurs HTTPS.

4.4.1.- Accés del personal.

S'ha de generar un usuari i una contrasenya amb els permisos definits per la direcció del centre. Es pot enviar un arxiu de pas a l'usuari per correu electrònic Aquest arxiu de pas es pot fer servir com a signatura (identificació electrònica). Aquest arxiu de pas hauria de caducar cada tres mesos.

4.4.1.1.- Accés des de l'escola.

L'accés es pot regular de la mateixa manera que l'accés a la xarxa interna.

4.4.1.2.- Accés des de fora del col·legi.

Quan ha sortit del centre, l'usuari és el responsable de mantenir la seguretat de l'accés. Per això, cal que:

a) Tingui un antivirus actualitzat.

b) Tanqui les sessions que no fa servir.

4.4.2.- Accés dels alumnes i de les famílies.

S'ha de crear un usuari i una contrasenya per persona autoritzada, no per família. L'administrador de la plataforma ha de configurar els accessos de manera que cada progenitor tingui accés a la informació del seu fill, però només tingui accés a la informació pròpia, no a la de l'altre progenitor.

Un cop creat l'accés, el col·legi ha de notificar la contrasenya a l'usuari en un sobre tancat. Al sobre s'ha d'incloure la clàusula que s'acompanya com a document PT3

4.5.- ÚS DELS SUPORTS.

Suports físics

Només es poden fer servir si la direcció ho permet.

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

Els suports i documents que continguin dades de caràcter personal han de permetre identificar el tipus d'informació que contenen, han de ser inventariats i només hi ha de poder accedir-hi el personal autoritzat en el document de seguretat.per fer-ho

La sortida de suports i documents que continguin dades de caràcter personal, inclosos els compresos i/o annexos a un correu electrònic l'ha d'autoritzar la direcció.

En el trasllat de la documentació s'han d'adoptar les mesures dirigides a evitar la sostracció o pèrdua de la informació o l'accés indegut durant el transport. Quan el suport contingui informació dels alumnes, o de les famílies, la informació ha d'estar xifrada.

Sempre que s'hagi de rebutjar qualsevol document o suport que contingui dades de caràcter personal, s'ha de destruir o esborrar mitjançant l'adopció de mesures dirigides a evitar la recuperació posterior.

Es poden identificar els suports que continguin dades de caràcter personal especialment sensibles fent servir sistemes d'etiquetatge que en dificultin la identificació per a les persones que no tenen permís de la Direcció per a accedir a la informació que contenen

Suports virtuals (núvols).

La direcció del centre pot permetre que es facin servir núvols si:

a) L'empresa que gestiona el núvol reuneix les garanties adequades segons la normativa europea. Convé evitar l'ús dels núvols públics.

b) Controla el compte vinculat al núvol. El centre té l'obligació de controlar tota la informació que gestionen els usuaris del sistema. No és possible que algú tracti informació del col·legi, dels alumnes, professors, famílies o d'altra mena, sense que el col·legi en tingui coneixement del contingut, un accés sense límit i el poder de tractament i gestió en règim de responsable del fitxer.

4.6.- LA WEB.

El centre ha de controlar el contingut de la web. A la web s'ha d'incloure l'avís legal PT4.

Només es poden publicar les fotografies de les persones que hagin permès expressament la publicació de les seves imatges. El centre ha de gestionar el fitxer Robinson en el que s'ha de deixar constància de les dades i/o informació de les persones que han posat objeccions al tractament de la seva informació i/o no han autoritzat l'ús de la seva imatge.

COL·LEGI ASUNCION NTRA. SRA.
Centre concertat per la Generalitat de Catalunya
www.asuncion.cat

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat

4.7.- ELS BLOCS I DEMÉS EINES DE PARTICIPACIÓ.

Els blocs que impliquin directa o indirectament la imatge, el nom o, de qualsevol manera, al col·legi o a les institucions vinculades, han de complir els requisits de consentiment i permisos de la direcció.

Només es podran allotjar en dominis que siguin segurs.

Al col·legi ha d'haver-hi un administrador de continguts. Quan es publiqui una entrada que vagi contra el caràcter propi del centre, o sigui ofensiva per algú, s'ha de treure sense més requisit que l'ordre de la direcció.

Només es poden registrar alumnes més grans de 14 anys, o menors amb el compromís de responsabilitat manifestada expressament pel seu representant legal.

4.8.- EL CORREU ELECTRÒNIC.

Al col·legi només es pot fer servir el correu electrònic corporatiu.

Els correus personals només es poden fer servir en cas d'emergència o si es té el permís de la direcció.

No es considera privat cap missatge de correu electrònic corporatiu. Tots els missatges que entrin, o surtin, pel domini del col·legi, es consideren correu del centre. Es considera correu electrònic tant l'intern, entre terminals de la xarxa corporativa, com l'extern, dirigit o procedent d'altres xarxes públiques o privades, i, especialment, d'Internet.

El Col·legi pot revisar els missatges de correu electrònic dels usuaris de la xarxa corporativa sense avisar.

S'han de desar còpies dels correus electrònics que involucrin entrades o sortides de dades de la base de dades en directoris protegits i amb el control del responsable del sistema.

S'han de mantenir còpies dels correus durant, almenys, un any. També s'han de desar durant un mínim d'un any, en directoris protegits, una còpia de les bases de dades rebudes o transmeses per sistemes de transferència de bases de dades, per xarxa, deixant constància a un registre, de la data i hora en què es va fer l'operació i el destí de la base de dades que s'ha enviat o s'ha rebut.

Si s'ha d'enviar informació per correu electrònic o per sistemes de transferència de base de dades, per xarxes públiques, o que no estiguin protegides, s'han de xifrar de manera que només les puguin llegir o interpretar els destinataris.

COL·LEGI ASUNCION NTRA. SRA.
Centre concertat per la Generalitat de Catalunya
www.asuncion.cat

Rambla Poblenou, 94-96
08005 Barcelona
Telèfon 933 000 931
escola@asuncion.cat