GOOGLE DRIVE KONTUEN ERABILERA-POLITIKA ETA PRIBATUTASUNA

CPEIPS BERRIO-OTXOA HLBHIP
Marcelino M. y Pelayo 25, 48006 Bilbao
www.berriotxoa.eus 94 4334903

1. ZERBITZUAREN DESKRIBAPENA.

Hezkuntzarako G Suite kontuak, Googlerekin ezarritako akordioaren arabera, G Suite Education domeinua aktibatzean BERRIO-OTXOA Ikastetxean kontratatutako langile, ikasle eta haien familien arteko komunikazio-funtzioak babesteko ematen dira. Domeinu hori Googlek ikastetxeei eskaintzen dien software-soluzioen multzoa da, Software as a Service (Software zerbitzu gisa) hodeiko konputazio-eredupean.

Baliabide horiek eskuratu ahal izateko, Erabilera eta Pribatutasun Politika hau onartu behar du **erabiltzaile-kontu** bat duen erabiltzaileak, hau da, kontratatutako langileek edo boluntarioek, 14 urte edo gehiago dituzten ikasleek eta seme-alaben bidez kontua ematen zaien 14 urtetik beherako ikasleen familiek.

Lan-pedagogirako komunikazioa plataforma hau hautatu da jarraian zehaztutako arrazoiengatik:

1. Zerbitzuaren erabilgarritasun handia >% 99
2. Produktibitate-aplikazioak integratzea eta e-mailarekin lankidetzan aritzea, lankidetzako lan-tresna eskainiz.
3. Doakotasuna zerbitzu teknikoari egindako kontsultetan
4. Operatibitatea, gailu eta plataforma anitzeko soluzio integratua delako, eta gailu mugikorrei erabilera-baldintza berberak aplikatu ahal zaizkielako.
5. Web nabigatzailetik irisgarritasuna, aparteko softwarerik instalatu beharrik gabe.

Googlek eskaintzen dituen kontuetan ez bezala, zentroaren mendeko zerbitzuak ikastetxeak berak administratutako zerbitzuak dira, eta honako zerbitzu integratu hauek barne hartzen ditu: **Gmail, Google Calendar** (egutegi partekatuak), **Google Drive** (dokumentuak ostatatzea, kalkulu-orriak eta online lankidetza), **Google Sites** (talde-guneen diseinua eta argitalpena).

- **Gmail:** Gmailen mezuak zentroaren domeinua duten posta-kontu pertsonalizatuak sortzeko aukera ematen du eta spam iragazketa indartsua du.
- **Google Calendar**: zerbitzu honek aukera ematen du eskola-ordutegiak, ekitaldiak eta abar kudeatzeko; era berean, ikasleek beren egutegia sor dezakete beren ordutegiarekin, ikasketa planifikatu, zereginak gogoratu...
- **Google Drive:** gure artxiboak biltegiratzeko leku bat eskaintzen duen zerbitzua, baita testu-dokumentuak, kalkulu-orriak, aurkezpenak, formularioak eta karpetak sortzeko aukera ere. Gainera, beste erabiltzaile batzuekin partekatzeko aukera ematen du.

- **Google Sites:** zerbitzu honek web orri seguruak sortzeko aukera ematen du, programazio-ezagutzarik behar izan gabe; horrela, arlo desberdinetako edukiak, proiektuak edo lanak modu na**hiko intuitibo eta errazean erakutsi eta zabaldu daitezke.**
- **Google Classroom** aplikazio garrantzitsuenetako bat da, irakasleak eta ikasleak errazago komunikatzeko eta eguneroko lanaren jarraipena egiteko diseinatutako irtenbidea baita.
- **Beste aplikazio batzuk:** Googlek beste aplikazio batzuk ere jartzen ditu ikastetxeen eskura, administratzailearen kontrol-paneletik erabiltzaile-talde desberdinei gehitu ahal zaizkienak.

G Suite for Education institucionales erakundearen kontuetan modu bateratuan sartzen da: https://accounts.google.com /.

2. ZERBITZUAREN BALDINTZAK.

2.1. BALDINTZA OROKORRAK.

BERRIO-OTXOA IKASTETXEAREN G Suite for Education kontuak Google-ek irakasleei, administrazio eta zerbitzuetako langileei, irakaskuntza arautuak egiten dituzten eta ikastetxe batean matrikulatuta dauden ikasleei ematen dizkie.

G Suite for Education kontuak ikastetxeak eta Googlek sinatutako akordioan ezarritako baldintzen arabera sortu eta erabiltzen dira, "G Suite for Education" akordio orokorraren arabera.

G Suite for Education kontuak ikastetxeek, irakasleek, bertan lan egiten duten administrazio eta zerbitzuetako langileek eta irakaskuntza arautuak egiten dituzten ikasleek erabili beharko dituzte, beren hezkuntza-jarduerarekin lotutako zereginetan.

G Suite for Education kontuei lotutako zerbitzu eta aplikazioen bidez edozein eduki mota argitaratu eta banatzeko, datu pertsonalak babesteari buruz indarrean dagoen legeria bete beharko da.

Erabat debekatuta dago ikastetxeko G Suite for Education kontuak eta horiei lotutako zerbitzu eta aplikazio guztiak merkataritza- edo publizitate-jardueretarako erabiltzea.

Erabiltzaileak edo legezko ordezkariak dira beren sarbide-kontuekin eta lotutako postontziarekin egindako jarduera guztien erantzuleak.

Hutsegite larria da baimenik ez duten pertsonei norberaren kontuan sartzea erraztea eta eskaintzea.

Erabiltzaile bakoitzaren ardura da G Suite for Education aplikazioetako datuak zaintzen saiatzea, Data Liberation programak eskaintzen duen Google Takeout aplikazioa aldian behin erabiliz.

Elkargoak kontuak sortu ahal izango ditu backupak administratzeko, eta LDAP eta Single Sign On gaitu ahal izango ditu hirugarren zerbitzuak autentifikatzeko.

2.2. IRAKASLE ETA AZP-KOENTZAKO GMAIL KONTUEN BALDINTZAK

- G Suite for Education kontuak ikastetxeko langile guztiei ematen zaizkie: irakasleei nahiz jarduneko administrazio eta zerbitzuetako langileei.
- Kontu horiek ikastetxearen mendeko "lan-kontutzat" hartzen dira. Irakasle batek edo administrazio eta zerbitzuetako pertsona batek ikastetxe batean jarduneko langile izateari uzten dionean, ikastetxeko G Suite for Education kontuari baja eman edo etengo zaio.
- Debekatuta dago elkargoko langileek erakundekoak ez diren posta-kontuak erabiltzea esleitzen zaizkien zereginak eta funtzioak betetzean eta barne-komunikazioan, erakunde ofizialek emandako posta-kontuak izan ezik.
- Irakasle bakoitzak G Suite for Education kontu bakarra izango du, eta aldian-aldian berrikusiko du.
- Borondatezko baja edo kaleratzea gertatuz gero, erabiltzaileek baimena ematen diote ikastetxeari Google driven biltegiratutakoaren edukia Zuzendaritzak zehaztutako beste kontu batera transferitzeko.
- Posta elektronikoa pertsonen artean informazioa trukatzeko tresna da, ez informazioa modu masibo eta bereizi gabean zabaltzekoa.
- Erabiltzaileak ezin izango du onartu ezezagunengandik datozen dokumentu edo fitxategi erantsirik, ezta jatorri fidagarria ez duenik ere. Era berean, ezin izango du jarraitu gakoak edo erabiltzaileen izenak eskatzen dituzten formularioetarako estekarik.
- Gomendatzen da mezu elektroniko guztietan helarazitako mezuek bete behar dituzten lege-alderdiak hartzaileari adieraziko dizkion lege-testua sartzea:Arduraduna: **COLEGIO BERRIO-OTXOA IKASTETXEA**. Helburuak: alderdien arteko kontratu aurreko/kontratuzko harremana kudeatzea, bai eta harreman horren ondoriozko posta elektroniko bidezko komunikazioak ere, unean uneko informazioa ematea, eta arduradunaren jarduerak, ekintzak eta betebeharrak kudeatzea eta gauzatzea. Legitimazioa: erantzulearen interes legitimoa. Hartzaileak: datuen hartzaileak gure zentroko arloak izango dira, bai eta datuak lagatzen dizkiegun hirugarrenak ere, datuen babesaren arloan indarrean dagoen araudian ezarritakoaren arabera zilegi denean. Nazioarteko transferentzia: ez dago aurreikusita datuen nazioarteko transferentziarik.

“ Kontserbazio-denbora: bildu ziren helburua betetzeko behar den denboran gordeko dira. Eskubideak: eskubidea duzu datuak eskuratzeko, zuzentzeko eta ezabatzeko, bai eta beste eskubide batzuk ere, gure pribatutasun-politikan kontsulta dezakezun datuen babesari buruzko informazio gehigarrian azaltzen den bezala: https://www.berriotxoa.eus *Helbide elektroniko honetan jasotako informazioa KONFIDENTZIALA da, eta goian aipatutako hartzaileak bakarrik erabili ahal izango du. Mezu hau irakurtzen baduzu eta ez bazara adierazitako hartzailea, jakinarazten dizugu guztiz debekatuta dagoela komunikazio hau erabiltzea, zabaltzea, banatzea edota erreproduzitzea, indarrean dagoen legeriaren arabera berariazko baimenik gabe. Mezu hau akats baten ondorioz jaso baduzu, mesedez, jakinaraz iezaguzu berehala bide honetatik, eta ezaba ezazu. “*

- Hirugarrenei bidaltzeko helbide elektronikoak, komunikazio anizkoitz batean sartuz gero, **"CCO"** eremuan sartu behar dira (ezkutuko ikatzaren kopia) Datuak Babesteko Erregelamendu Orokorrean xedatutakoa ez hausteko. Horrela, posta elektronikoaren hartzaileen zerrenda ez da ikusgai egongo jasotzen duenarentzat.

- Edozein gorabehera zuzendaritzari jakinaraziko zaio: adibidez, erabilera desegokia (arrazista, xenofoboa, pornografikoa, sexista, terrorismoaren apologia edo giza eskubideen edo intimitaterako, ohorerako, norberaren irudirako edo pertsonen duintasunerako eskubideen aurka egitea; identifikatu gabeko mezuak zabaltzea; berariazko baimenik gabeko merkataritza- edo propaganda-mezuak zabaltzea; kateatutako gutunak zabaltzea) edo baimenik gabeko mezuak zabaltzea edo kontuaren funtzionamenduarekin lotutako gorabeherak.

2.3. IKASLEEN GMAIL KONTUEN BALDINTZAK.

- COLEGIO BERRIO-OTXOA IKASTETXEAk alta eman ahal izango die ikasleei, eta horretarako zehaztu den prozedurari jarraitu beharko diote.

- 14 urtetik gorako ikasleek kontuak erabiltzeko, adierazi behar dute bat datozela ikastetxeko G Suite for Education Kontuen Erabilera Politikarekin. 14 urtetik beherakoak badira, hauen gurasoek edo legezko tutoreek.

- Ikasle bakoitzak ikastetxeko G Suite for Education kontu bakarra eduki ahal izango du, eta haren erabilera eskola- eta hezkuntza-eremurako bakarrik izango da: global Educa hezkuntza-plataforman, Moodle edo gela birtualean.

- Ikasle batek ikastetxean matrikulatuta egoteari uzten dionean, erabiltzaile-kontua eten edota ezabatu egingo da.

- Kontuaren erabilerak indarrean dauden eskola-bizikidetzako arauak errespetatu beharko ditu.

- BERRIO-OTXOA IKASTETXEAK eskubidea du aplikazioen hedapena irizpide pedagogikoen eta ikasleen adinaren arabera baldintzatzeko.

- Ikasle baten kontua diziplinako kasu larrietan, hala nola ziberjazarpenean, egon daitekeelako zantzurik badago, elkargoko zuzendaritzak esku hartu, eten edota gainbegiratu ahal izango ditu.

- Edozein gorabehera zuzendaritzari jakinaraziko zaio: adibidez, erabilera desegokia (arrazista, xenofoboa, pornografikoa, sexista, terrorismoaren apologia edo giza eskubideen edo intimitaterako, ohorerako, norberaren irudirako edo pertsonen duintasunerako eskubideen aurka egitea; identifikatu gabeko mezuak zabaltzea; berariazko baimenik gabeko merkataritza- edo propaganda-mezuak zabaltzea; kateatutako gutunak zabaltzea) baimenik gabeko mezuak zabaltzea edota kontuaren erabileraren gorabeherak.

- Erabiltzaileak ezin izango du ezezagunengandik datozen dokumentu edo fitxategi erantsirik onartu, ezta jatorri fidagarria ez duenik ere. Era berean, ezin izango du jarraitu gakoak edo erabiltzaileen izenak eskatzen dituzten formularioetarako estekarik.

- Hirugarrenei bidaltzeko helbide elektronikoak komunikazio anizkoitz batean sartuz gero, **"CCO"** eremuan sartu behar dira (ezkutuko ikatzaren kopia), Datuak Babesteko Erregelamendu Orokorrean xedatutakoa ez hausteko. Horrela, posta elektronikoaren hartzaileen zerrenda ez da ikusgai egongo jasotzen duenarentzat.

- Mezu elektroniko guztietan, helarazitako mezuei lotuta egon daitezkeen lege-alderdiak hartzaileari adieraziko dizkion lege-testua sartzea gomendatzen da: "Mezu elektroniko honetan jasotako informazioa konfidentziala dela jakinarazten dizugu, eta goian aipatutako hartzaileak baino ez duela erabiliko.

- Gomendatzen da mezu elektroniko guztietan sartzea helarazitako mezuek bete behar dituzten lege-alderdiak hartzaileari adieraziko dizkion lege-testua: "*Mezu hau irakurtzen baduzu eta ez bazara adierazitako hartzailea, jakinarazten dizugu guztiz debekatuta dagoela komunikazio hau erabiltzea, zabaltzea, banatzea eta/edo erreproduzitzea, indarrean dagoen legeriaren arabera berariazko baimenik gabe. Mezu hau akats baten ondorioz jaso baduzu, mesedez, jakinaraz iezaguzu berehala bide honetatik, eta ezaba ezazu. "*

2.4. KLAUSULA.

Kontua duten langile guztiek eta kontua duten ikasleen gurasoek, tutoreek edo legezko ordezkariek ikastetxeko G Suite for Education Kontuen Erabilera Politika honekin ados daudela adierazi beharko dute.
Zerbitzua emateari buruz aipatutako baldintzak betetzen ez direla ikusiz gero, kontuak administratzeko arduradunak ikastetxeko G Suite for Education kontu oro desaktibatzeko edo baja emateko ahalmena izango du, baita aldez aurretik abisatu gabe ere.

2.5. PRIBATUTASUNA, SEGURTASUNA ETA DATUEN ERABILERA

G Suite for Education erakundeak 2012ko maiatzetik dauka ISO 27001 ziurtagiria, lehendik dagoen SSAE 16/SAE 3402 ziurtagiriaz gain, baita Gobernuentzako G Suite for Education erakundearen FISMA ziurtagiria ere.

Privacy Shield pribatutasun akordioari atxikitako enpresa da, AEBrekin 2016ko uztailean lortu zuena. Privacy Shield, lehengo Ataka Segurua ordezkatzen duena, Europako edozein herritarren oinarrizko eskubideak babestu nahi ditu, datu pertsonalak Estatu Batuetara transferitzen direnean, eta argitasun juridikoa eman nahi die nazioarteko datu-transferentzien mende dauden enpresei.

La Mennais
BERRIO-OTXOA IKASTETXEA
BILBAO

POLÍTICA DE USO Y PRIVACIDAD DE CUENTAS GOOGLE DRIVE

CPEIPS BERRIO-OTXOA HLBHIP
Marcelino M. y Pelayo 25, 48006 Bilbao
www.berriotxoa.eus 94 4334903

Eskola Jasangarria Ziurtagiria

Euskadi

1. DESCRIPCIÓN DEL SERVICIO.

Las cuentas de G Suite para Educación son proporcionadas con el objeto de apoyar las funciones de comunicación de todo el personal contratado y del alumnado y sus familias en **COLEGIO BERRIO-OTXOA IKASTETXEA** conforme al acuerdo establecido con Google al activar el dominio en G Suite Education que es un conjunto de soluciones de software que Google ofrece a los centros educativos bajo el modelo de computación en la nube Software as a Service (Software como Servicio).
El acceso a estos recursos está condicionado a la aceptación de la presente Política de Uso y Privacidad por parte del usuario poseedor de una **cuenta de usuario**, esto es, el personal contratado o voluntario, el alumnado con edad de 14 años o mayor y las familias de alumnos menores de 14 años a los que se les proporcione cuenta por medio de sus hijos.
Se ha elegido esta plataforma de comunicación y para el trabajo pedagógico por:

- Alta disponibilidad del servicio >99%
- Integración de aplicaciones de productividad y colaboración con e-mail proporcionando una herramienta de trabajo cooperativo.
- Gratuidad en las consultas al servicio técnico
- Operatividad al ser una solución integrada multidispositivo y multiplataforma, pudiendo aplicar las mismas condiciones de uso a dispositivos móviles
- Accesibilidad desde navegador web, sin necesidad de instalar software extra.

A diferencia de las cuentas que ofrece Google los servicios bajo el dominio del centro son servicios administrados por el propio centro educativo, e incluye los siguientes servicios integrados: **Gmail**, **Google Calendar** (calendarios compartidos), **Google Drive** (alojamiento de documentos, hojas de cálculo y colaboración online), **Google Sites** (diseño y publicación de sitios en equipo).

- **Gmail**: El correo de Gmail, permite la creación de cuentas de correo personalizadas con el dominio del centro y dispone de un filtrado potente de spam.
- **Google Calendar**: Este servicio permite gestionar horarios de clase, eventos...etc; así como el alumnado pueden crear su calendario con su horario, planificarse el estudio, recordar las tareas...etc.
- **Google Drive**: Servicio que proporciona un lugar de almacenamiento para nuestros archivos, así como la posibilidad de crear documentos de texto, hojas de cálculo, presentaciones, formularios y carpetas. Además permite compartirlos con otros usuarios.

- **Google Sites**: Este servicio permite la creación de páginas web seguras sin necesidad de conocimientos de programación, permitiendo así la exposición y difusión de contenidos, proyectos o trabajos de las diferentes áreas de una forma bastante intuitiva y fácil.
- **Google Classroom** es una de las aplicaciones más importantes ya que es una solución diseñada para que el profesorado y el alumnado puedan comunicarse más fácilmente y llevar un seguimiento del trabajo diario.
- **Otras Apps**: Google también pone a disposición de los centros educativos otras aplicaciones que pueden ser añadidas a distintos grupos de usuarios desde el Panel de control del administrador.

El acceso a las cuentas de G Suite for Education institucionales se realiza de forma unificada en: https://accounts.google.com/.

2. CONDICIONES DEL SERVICIO.

2.1. CONDICIONES GENERALES.

Las cuentas de G Suite for Education de **COLEGIO BERRIO-OTXOA IKASTETXEA** constituyen un servicio que esta proporciona a docentes, personal de administración y servicios, así como al alumnado matriculado que cursan sus enseñanzas regladas y se encuentre matriculado en un colegio.

Las cuentas de G Suite for Education son creadas y utilizadas de acuerdo con las condiciones establecidas en el acuerdo suscrito entre el colegio y Google en los términos del acuerdo genérico "G Suite for Education"

Las cuentas de G Suite for Education deberán ser utilizadas por los centros, docentes y personal de administración y servicios que trabaja en ellos, y los alumnos y alumnas que cursan sus enseñanzas regladas, en tareas relacionadas con su actividad educativa.

La publicación y distribución de cualquier tipo de contenido mediante los servicios y aplicaciones vinculados a las cuentas de G Suite for Education deberán realizarse de acuerdo con la legislación vigente sobre protección de datos de carácter personal.

Queda estrictamente prohibido el uso de las cuentas de G Suite for Education del colegio, y de todos los servicios y aplicaciones vinculados a ellas, para actividades comerciales o publicitarias.

Los Usuarios o representantes legales son responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado.

Es una falta grave facilitar y ofrecer acceso a la propia cuenta a personas no autorizadas.

Es responsabilidad de cada usuario procurar la salvaguarda de los datos contenidos en las aplicaciones de G Suite for Education haciendo uso periódico de la aplicación Google Takeout ofrecido por el programa Data Liberation

El colegio podrá crear cuentas para la administración de backups, así como habilitar LDAP y Single Sign On para la autenticación con terceros servicios.

2.2. CONDICIONES DE LAS CUENTAS DE GMAIL PARA DOCENTES Y PAS.

- Las cuentas de G Suite for Education se conceden a todo el personal del centro: docentes y personal de administración y servicios en activo.
- Estas cuentas tienen consideración de "cuentas de trabajo" bajo el dominio del centro. Cuando un docente o persona de administración y servicios deje de cumplir la condición de trabajador en activo de un centro se suspenderá o dará de baja su cuenta de G Suite for Education del colegio.
- Está prohibido el uso de cuentas de correo **no** institucionales por parte del personal del colegio en el desempeño de las tareas y funciones que le son asignadas y en la comunicación interna, a excepción de las cuentas de correo facilitadas por organismos oficiales.
- Cada docente solo podrá disponer de una única cuenta de G Suite for Education que revisará periódicamente.
- En caso de baja voluntaria o despido, los usuarios autorizan al colegio a transferir el contenido de lo almacenado en Google Drive a otra cuenta que la Dirección determine.
- El correo electrónico es una herramienta para el intercambio de información entre personas, no un medio de difusión masiva e indiscriminada de información.
- El usuario no deberá aceptar documentos ni archivos adjuntos que provengan de desconocidos o que tengan origen poco fiable, ni seguir vínculos a formularios donde se pidan claves o nombres de usuarios.
- Se recomienda incluir en todos los correos electrónicos el texto legal que indique al destinatario aquellos aspectos legales a los que puedan estar sujetos los correos remitidos:

  " Responsable: ***COLEGIO BERRIO-OTXOA IKASTETXEA****. Finalidades: Gestionar la relación precontractual/contractual entre las partes, así como las comunicaciones vía correo electrónico derivadas de la misma, proporcionarle información puntual, gestionar y ejecutar las actividades, acciones y obligaciones del Responsable. Legitimación: El interés legítimo por parte del Responsable. Destinatarios: Los destinatarios de sus datos serán las distintas áreas de nuestro centro, así como los terceros a los que cedamos sus datos, cuando sea lícito conforme a lo dispuesto en la normativa vigente en materia de protección de datos. Transferencia internacional: No están previstas transferencias internacionales de los datos. Tiempo de conservación: Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron. Derechos: Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional sobre Protección de Datos que puede*

consultar en nuestra Política de privacidad: https://www.berriotxoa.eus La información incluida en este mail es CONFIDENCIAL, siendo para uso exclusivo del destinatario arriba mencionado. Si Usted lee este mensaje y no es el destinatario indicado, le informamos que está totalmente prohibida cualquier utilización, divulgación, distribución y/o reproducción de esta comunicación sin autorización expresa en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos nos lo notifique inmediatamente por esta misma vía y proceda a su eliminación."

- En el supuesto de introducir las direcciones de correo electrónico para su envío a terceras personas, en una comunicación múltiple, es preciso insertarlas en el campo ***"CCO"*** (**copia carbón oculta**) para no infringir lo dispuesto en el Reglamento General de Protección de Datos y de esta manera la lista de destinatarios del correo electrónico no será visible para quien lo reciba.
- Cualquier incidencia será puesta en conocimiento de la dirección: como el uso indebido (difusión de contenidos de carácter racista, xenófobo, pornográfico, sexista, apología del terrorismo o atentar contra los derechos humanos o derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas; difusión de mensajes sin identificar, difusión de mensajes comerciales o propagandísticos sin autorización expresa, propagación de cartas encadenadas) o no autorizado de su cuenta de correo electrónico, o incidencias relacionadas con el funcionamiento de la cuenta.

2.3. CONDICIONES DE LAS CUENTAS DE GMAIL DEL ALUMNADO.

- El **COLEGIO BERRIO-OTXOA IKASTETXEA** podrá dar de alta cuentas para su alumnado, para lo cual deberán seguir el procedimiento que se ha determinado al efecto.
- El uso de las cuentas por parte del alumnado requiere manifestar la conformidad con la Política de Uso de Cuentas G Suite for Education del colegio para el alumnado de 14 años en adelante y por parte de los padres/madres o responsables legales del alumno-a si fueran menores de 14 años.
- Cada alumno-a solo podrá tener una única cuenta de G Suite for Education del colegio y su uso es exclusivo para el ámbito escolar y educativo: en la plataforma educativa Global Educa, en el Moodle o aula virtual.
- Cuando un alumno-a deje de estar matriculado-a en el centro, se procederá a suspender y/o eliminar su cuenta de usuario.
- El uso de la cuenta deberá respetar las normas de convivencia escolares vigentes.
- El **COLEGIO BERRIO-OTXOA IKASTETXEA** se reserva el derecho a condicionar el despliegue de las aplicaciones según criterios pedagógicos y la edad del alumnado.

- En el caso de que haya indicios de que la cuenta de un alumno-a pueda verse involucrado-a en casos graves de disciplina como *ciberacoso*, podrán ser intervenida, suspendida y/o supervisada por la Dirección del colegio.

- Cualquier incidencia será puesta en conocimiento de la dirección: como el uso indebido (difusión de contenidos de carácter racista, xenófobo, pornográfico, sexista, apología del terrorismo o atentar contra los derechos humanos o derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas; difusión de mensajes sin identificar, difusión de mensajes comerciales o propagandísticos sin autorización expresa, propagación de cartas encadenadas) o no autorizado de su cuenta de correo electrónico, o incidencias relacionadas con el funcionamiento de la cuenta.

- El usuario-a no deberá aceptar documentos ni archivos adjuntos que provengan de desconocidos o que tengan origen poco fiable, ni seguir vínculos a formularios donde se pidan claves o nombres de usuarios.

- En el supuesto de introducir las direcciones de correo electrónico para su envío a terceras personas, en una comunicación múltiple, es preciso insertarlas en el campo ***"CCO"*** (**copia carbón oculta**) para no infringir lo dispuesto en el Reglamento General de Protección de Datos y de esta manera la lista de destinatarios del correo electrónico no será visible para quien lo reciba.

- Se recomienda incluir en todos los correos electrónicos el texto legal que indique al destinatario aquellos aspectos legales a los que puedan estar sujetos los correos remitidos: "Le informamos que la información incluida en este correo electrónico es CONFIDENCIAL, siendo para uso exclusivo del destinatario arriba mencionado. Si Usted lee este mensaje y no es el destinatario indicado, le informamos que está totalmente prohibida cualquier utilización, divulgación, distribución y/o reproducción de esta comunicación sin autorización expresa en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos nos lo notifique inmediatamente por esta misma vía y proceda a su eliminación."

2.4. CLÁUSULA.

Todos los empleados con cuenta y los padres, tutores o representantes legales de los alumnos con cuenta, deberán manifestar su conformidad con la presente Política de Uso de las Cuentas de G Suite for Education del colegio.

En caso de que se advierta un incumplimiento de las condiciones antedichas sobre prestación del servicio, el responsable de la administración de las cuentas se reserva la potestad de desactivar o dar de baja cualquier cuenta de G Suite for Education del colegio, incluso sin previo aviso.

2.5. PRIVACIDAD, SEGURIDAD Y TRATAMIENTO DE DATOS

G Suite for Education posee desde mayo 2012, la certificación ISO 27001, además de la ya existente SSAE 16/SAE 3402 y el certificado FISMA de G Suite for Education para Gobiernos

Es una empresa adherida al acuerdo de privacidad, Privacy Shield, alcanzado con EEUU en Julio de 2016. El Privacy Shield, que sustituye al antiguo Puerto Seguro, busca proteger los derechos fundamentales de cualquier ciudadano europeo cuyos datos personales se transfieran a los Estados Unidos, y aportar claridad jurídica para las empresas que dependen de transferencias internacionales de datos.

DATUEN BABESAREN ARLOKO KONTZEPTUEN GLOSARIOA

- **DATU PERTSONALAK**
  - Neurriz kanpoko ahaleginik egin gabe identifikatutako edo identifika daitekeen pertsona fisiko bati buruzko informazio oro: interesatua edo kaltetua (adibidez: izena, helbidea, telefonoa, kontu-zenbakia).
- **DATUEN KATEGORIA BEREZIAK**
  - Ideologia, sindikatu-afiliazioa, erlijioa eta sinesmenak adierazten dituztenak, arraza-jatorriari, osasunari eta sexu-bizitzari erreferentzia egiten dietenak, bai eta datu biometrikoak eta genetikoak ere. (Batez ere orientazio-sailean aurki ditzakegu).
- **OSASUN DATUAK**
  - Pertsona fisiko baten osasun fisiko edo mentalari buruzko datu pertsonalak, haren osasun-egoerari buruzko informazioa ematen duten osasun-arretako zerbitzuak barne. (Alergien ziurtagiria).
- **DATUEN TRATAMENDUA**
  - Datu pertsonalak dituen edozein jarduera, eskuz edo modu automatizatuan egiten bada: bilketa, erregistroa, kontserbazioa, aldaketa, kontsulta, komunikazioa, etab. (Ikasturte hasieran ikasleen eta gurasoen datuak biltzea datu pertsonalen tratamenduaren adibide argia da).
- **SEUDONIMIZAZIOA**
  - Datu pertsonalak informazio gehigarria erabili gabe interesdun bati egozteko moduan tratatzea, betiere informazio gehigarri hori bereizita badago eta datu pertsonalak identifikatutako edo identifikatzeko moduko pertsona fisiko bati esleitzen ez zaizkiola bermatzeko neurri tekniko eta antolamenduzkoen mende badago. (Adibidez: azterketak ikasleen matrikula-zenbakiarekin izendatzea, eta ez izen-abizenekin).
- **FITXATEGIA**
  - Datu pertsonalen multzo egituratu oro, irizpide jakin batzuen arabera irisgarriak, zentralizatua, deszentralizatua edo modu funtzional edo geografikoan banatua. (Datu-basea).
- **TRATAMENDUAREN ARDURADUNA**
  - Tratamenduaren helburuak eta bitartekoak zehazten dituen pertsona fisiko edo juridikoa, agintaritza publikoa, zerbitzua edo beste erakunde bat. (Adibidez: ikastetxea matrikulan ikasleen datuak jasotzean).
- **TRATAMENDUA KUDEATZEA**
  - Tratamenduaren arduradunaren kontura datu pertsonalak tratatzen dituen pertsona fisiko edo juridikoa, agintaritza publikoa, zerbitzua edo beste erakunde bat. (Adibidez: eskola Kudeaketako Plataformaren hornitzailea).
- **DATUAK BABESTEKO ORDEZKARIA**
  - Tratamenduaren arduradunak izendatutako pertsona fisikoa edo juridikoa, modu independentean aholkatzeko ,datuen babesaren arloko arauak betetzeari eta barne-aplikazioari buruz informatzeko eta gainbegiratzeko behar bezala kualifikatua.

- **DBLO-KOORDINATZAILEA**
  - Barne-mailan izendatutako zentroko pertsona, datuak babestearekin zerikusia duten gai guztiak koordinatzeko arduraduna. Datuak Babesteko ordezkariarekin etengabeko lankidetzan aritu beharko du.
- **DBLO LAGUNTZAILEA**
  - Barne-mailan izendatutako zentroko pertsona, DBLO koordinatzaileari laguntza emango diona esleituta dituen zereginak betetzeko.
- **HARTZAILEA**
  - Pertsona fisiko edo juridikoa, agintaritza publikoa, zerbitzua edo beste erakunde bat. Hala ere, ez dira hartzailetzat hartuko Batasuneko edo estatu kideetako zuzenbidearekin bat etorriz ikerketa zehatz baten esparruan datuak jaso ditzaketen agintari publikoak ez dira hartzailetzat hartzen. Agintari publiko horiek datu horiek tratamendu-helburuei aplikatu beharreko datu-babesaren arloko arauen arabera tratatuko dituzte. (Eskola Kontseilua, Administrazioa eta abar).
- **INTERESDUNAREN BAIMENA**
  - Interesdunak, adierazpen baten bidez edo baiezko ekintza argi baten bidez, berari dagozkion datu pertsonalen tratamendua onartzeko duen borondate-adierazpen aske, zehatz, informatu eta argi eta garbi oro. (Sare sozialetan edo web orrian argazkiak argitaratzeko baimena matrikulan).
- **DATU PERTSONALEN SEGURTASUN URRATZEA**
  - Transmititutako, kontserbatutako edo beste era batera tratatutako datu pertsonalak ustekabean edo legez kontra suntsitzea edo aldatzea, edo datu horiek baimenik gabe jakinaraztea edo eskuratzea eragiten duen segurtasun-urraketa oro. (Ikasleen datuak dituen USB bat galtzea).
- **DATU BIOMETRIKOAK**
  - Tratamendu tekniko espezifiko batetik lortutako datu pertsonalak, pertsona fisiko baten ezaugarri fisiko, fisiologiko edo jokabidezkoei buruzkoak, pertsona horren identifikazio bakarra ahalbidetzen edo baieztatzen dutenak, hala nola aurpegiko irudiak edo datu daktiloskopikoak. (Adibidez: hatz-marka, begiaren irisa, etab.)
- **KONTROL-AGINTARITZA**
  - Estatu kide batek DBEOren 51. artikuluan xedatutakoaren arabera ezarritako agintaritza publiko independentea. Espainiaren kasuan, Datuak Babesteko Espainiako Agentzia da.(DBEA)
- **ERANTZUKIZUN PROAKTIBOAREN PRINTZIPIOA**
  - Erakundeek jarrera kontzientea, arduratsua eta proaktiboa izan behar dute egiten dituzten datu pertsonalen tratamendu guztien aurrean. Datuak babesteko araudia betetzeaz gain, araudi hori betetzen ari garela frogatu ahal izango dugu. (Printzipio hori betetzeko modu bat tratamendu-jardueren Erregistroa eta harekin batera doazen prozedurak dira).

GLOSARIO DE CONCEPTOS EN MATERIA DE PROTECCIÓN DE DATOS

- **DATO DE CARÁCTER PERSONAL**
  - Toda información sobre una persona física identificada o identificable sin realizar esfuerzos desproporcionados: el interesado-a/afectado-a (Por ejemplo: nombre, dirección, teléfono, número de cuenta).
- **CATEGORÍAS ESPECIALES DE DATOS**
  - Son aquellos que revelen ideología, afiliación sindical, religión y creencias, que hagan referencia al origen racial, a la salud y a la vida sexual, así como datos biométricos y genéticos. (Sobre todo podremos encontrarlos en el departamento de orientación).
- **DATOS DE SALUD**
  - Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. (Certificado de alergias).
- **TRATAMIENTO DE DATOS**
  - Cualquier actividad en la que estén presentes datos de carácter personal, ya se realice de manera manual o automatizada: Recogida, registro, conservación, modificación, consulta, comunicación, etc. (La recogida de datos del alumnado y de sus padres al inicio del curso escolar, es un ejemplo claro de tratamiento de datos de carácter personal).
- **SEUDONIMIZACIÓN**
  - El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado-a sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (Por ejemplo: nombrar los exámenes con el número de matrícula del alumnado y no con su nombre y apellidos).
- **FICHERO**
  - Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica. (Base de datos).
- **RESPONSABLE DEL TRATAMIENTO**
  - La persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. (Por ejemplo: Colegio al recabar los datos del alumnado en la matricula).
- **ENCARGADO-A DEL TRATAMIENTO**
  - La persona física o jurídica, autoridad, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. (Por ejemplo: Proveedor de la Plataforma de Gestión Escolar).

- **DELEGADO-A DE PROTECCIÓN DE DATOS**
  - Persona, física o jurídica, designada por el responsable o el encargado-a del tratamiento, debidamente cualificada para asesorar, informar y supervisar de manera independiente, acerca de la aplicación interna y el cumplimiento de las normas en materia de protección de datos.
- **COORDINADOR-A LOPD**
  - Persona del Centro designada a nivel interno como el-la responsable de coordinar todas las cuestiones relacionadas con la materia de protección de datos, que deberá trabajar en constante colaboración con el/la delegado/a de Protección de Datos.
- **AYUDANTE LOPD**
  - Persona del Centro designada a nivel interno, que dará soporte al Coordinador LOPD en el cumplimiento de las tareas que este tiene atribuidas
- **DESTINATARIO-A**
  - La persona física o jurídica, autoridad, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se consideran destinatarios las autoridades que puedan recibir datos en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento. (Consejo Escolar, Administración etc.).
- **CONSENTIMIENTO DEL INTERESADO-A**
  - Toda manifestación de voluntad libre, especifica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. (Consentimiento en matrícula para publicar fotos en Redes Sociales o Página Web).
- **VIOLACIÓN DE SEGURIDAD DE LOS DATOS PERSONALES**
  - Toda violación de la seguridad que ocasione la destrucción perdida o alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. (Pérdida de un USB con datos de los alumnos-as).
- **DATOS BIOMÉTRICOS**
  - Datos personales obtenidos a partir de un tratamiento técnico especifico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. (Por ejemplo: huella dactilar, iris del ojo, etc.)
- **AUTORIDAD DE CONTROL**
  - La autoridad independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51 RGPD. En el caso de España es la Agencia Española de Protección de Datos (AEPD).
- **PRINCIPIO DE RESPONSABILIDAD PROACTIVA**
  - Exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo. No solamente cumplir con la normativa en materia de protección de datos, sino también poder probar que estamos cumpliendo con esta normativa. (Una forma de cumplir con este principio es mediante el Registro de actividades del tratamiento y los procedimientos que lo acompañan).

ARSOPOL ESKUBIDEAK ERABILTZEKO PROZEDURA

1.SARRERA.

COLEGIO BERRIO-OTXOA IKASTETXEAK (MENESIANOS BILBAOK) interesdunei beren eskubideak baliatzeko aukera emango die, eta, horretarako, irispidea izateko, zuzentzeko, ezabatzeko (ahazteko eskubidea), tratamendua mugatzeko, eramangarritasuna mugatzeko eta aurka egiteko (ARSO – Pol eskubideak) eskubideak erabiltzeko ereduak jarriko ditu haien esku.
MENESIANOS BILBAOK interesdun baten eskaera jaso dela jakin bezain laster, eskaera jasotzen duen pertsonak edo pertsonek lehenbailehen jakinarazi beharko diote dagokion erakundeko erreferentziako pertsonari (sistemen arduraduna/DBLO/DPD koordinatzailea), izapidetu dezan.

2. INFORMAZIOAREN GARDENTASUNA, KOMUNIKAZIOA ETA INTERESDUNAKRENESKUBIDEAK BALIAZTEKO MODUAK.

Eskaerak bitarteko elektronikoen bidez aurkezteko aukera emango du **MENESIANOS BILBAOK**, bereziki tratamendua bitarteko horien bidez egiten denean.

Interesdunak doan baliatuko ditu eskubideak, argi eta garbi funsgabeak edo gehiegizkoak diren eskaerak egiten direnean izan ezik; kasu horietan, **MENESIANOS BILBAOK** kanon bat kobratu ahal izango du, eskaerari erantzuteak edo jarduteari uko egiteak dakartzan administrazio-kostuak konpentsatzeko. Kanon horrek ezin izango die diru-sarrera gehigarririk eragin **MENESIANOS BILBAORI;** aitzitik, benetan bat etorri beharko du eskaera izapidetzearen benetako kostuarekin.

MENESIANOS BILBAOK interesdun bati buruzko informazio asko tratatzen badu, informazio hori zehazteko eskatu ahal izango dio interesdun horri.

3. NORTASUNA EDO ORDEZKARITZA EGIAZTATZEA.

MENESIANOS BILBAOK ARSO – Pol eskubideak eskatu eta baliatzen dituztenen nortasuna egiaztatu beharko du. Horretarako, interesdunak egindako eskabidearekin batera **nortasun-agiri nazionalaren, pasaportearen edo identifikatzeko balio duen beste edozein agiriren kopia aurkeztu beharko da.** Eskubideak erabiltzeko prozedura telematikoki egiten denean ere, sinadura elektronikoaren bidez egiazta daiteke nortasuna. Legezko edo borondatezko ordezkaritzaren kasuan, ordezkaritza egiaztatzen duen agiria aurkeztu beharko da.

4. EPEAK.

Eskaera jasotakoan, **MENESIANOS BILBAOK** **hilabeteko epean** jakinarazi beharko dizkio demandatuak interesdunari bere eskaeraren ondoriozko jarduerak. Epe hori beste bi hilabetez luzatu ahal izango da eskaera bereziki konplexuak direnean, eta luzapen hori interesdunari jakinarazi beharko zaio lehenengo hilabetearen barruan.

MENESIANOS BILBAOK eskaera bati ez erantzutea erabakitzen badu, ezezkoaren berri eman beharko du, eskaera aurkeztu eta **hilabeteko epean.**

5. TRATAMENDUAREN ARDURADUAREN AURREAN ESKUBIDEAK BETETZEA.

MENESIANOS BILBAOK eragileen laguntza izan ahal izango du interesdunen eskubideak baliatzeko, eta lankidetza hori tratamendu-enkarguaren kontratuan sartu ahal izango du.

6. ERAGINDAKOEN ESKUBIDEAK.

DBEO Eskubideak	Zertan dautzan eragindakoen eskubideak?
Sartzeko eskubidea 	**<u>Langileari informazioa emango zaio (arduraduna aplikatzen duenean):</u>** ➔ Tratamenduaren helburuak; tratatzen diren datu pertsonalen kategoriak eta izan daitezkeen datu-komunikazioak eta hartzaileak. ➔ Ahal izanez gero, zure datuak gordetzeko epea. Hala ez bada, epe hori zehazteko irizpideak. ➔ Datuak zuzentzeko edo ezabatzeko, tratamendua mugatzeko edo horri aurka egiteko eskatzeko eskubidea. ➔ Kontrol Agintaritzan erreklamazio bat aurkezteko eskubidea. ➔ Tratamenduaren xede diren datuen kopia bat eskuratzeko eskubidea. ➔ Erabaki automatizatuak egotea, erabilitako logika eta tratamendu horren ondorioak.
Zuzentzeko eskubidea 	**<u>Zuzenketa-eskubideak aukera ematen dio eraginpekoari okerreko atzerapenik gabe alda daitezen zehaztugabeak edo osatugabeak diren datu pertsonalak.</u>** Zuzenketa-eskabidean adierazi beharko da zer daturi buruzkoa den, bai eta zer zuzenketa egin behar den ere, eta eskatutakoa justifikatzeko dokumentazioa erantsi beharko da.
Ezabatzeko eskubidea (Ahaztua izateko eskubidea) 	**<u>Jarduera horren bitartez interesdunak honako hauek eska ditzake:</u>** ★ Datu pertsonalak bidegabeko atzerapenik gabe ezabatzea, arauan jasotako kasuren bat gertatzen denean. Adibidez: o Datuen legez kontrako tratamendua. o Datu pertsonalak jada ez dira beharrezkoak bildu ziren helburuei dagokienez. o Datu pertsonalak ezabatu egin behar dira legezko betebehar bat betetzeko. ★ Hala ere, zenbait salbuespen arautzen dira, eta horietan ez da bidezkoa izango eskubide hori. Adibidez: o Adierazpen- eta informazio-askatasunerako eskubidea nagusitzea. o Osasun publikoaren arloko interes publikoko arrazoiengatik. o Interes publikoaren izenean artxibatzeko, ikerketa zientifiko edo historikorako edo estatistika helburuetarako.
Aurka egiteko eskubiea 	**<u>Interesdunak tratamenduaren aurka egin dezake:</u>** ➔ Egoera pertsonalarekin zerikusia duten arrazoiengatik, zure datuen tratamendua eten behar denean, interes legitimoa egiaztatzen ez bada, edo erreklamazioak egiteko edo defendatzeko beharrezkoa ez bada. ➔ Tratamenduaren xedea zuzeneko marketina denean.

Erabaki automatizatuen tratamenduaren aurka egiteko eskubidea 	Eskubide horren bidez, **<u>interesdunari aukera ematen zaio bere datuen tratamenduan soilik oinarritutako erabaki baten aurka egiteko, profilak egitea barne,</u>** baldin eta erabaki horrek bere pertsonarengan ondorio juridikoak baditu edo antzeko eragin nabarmena badu. Hala ere, **<u>eskubide hori ez da aplikatuko honako kasu hauetan</u>**: ➔ Beharrezkoa bada eragindako pertsonaren eta arduradunaren arteko kontratu bat egiteko edo gauzatzeko. ➔ Interesdunaren datuen tratamendua interesdunak aldez aurretik emandako baimenean oinarritzen da. ➔ Batasuneko edo estatu kideetako zuzenbideak baimentzen badu, eta interesdunaren eskubide, askatasun eta interes legitimoak babesteko neurri egokiak ezartzen badira.
Tratamendua mugatzeko  **eskubidea**	**<u>Eragindakoari ahalbidetzen dio:</u>** <u>Arduradunari datuen tratamendua eteteko eskatzea, baldin eta:</u> ➔ Datuen zehaztasuna aurkaratzen da, arduradunak zehaztasuna egiaztatzen duen bitartean ➔ Interesdunak datuen tratamenduaren aurka egiteko eskubidea baliatu du, eta bitartean egiaztatzen da erantzulearen legezko arrazoiak eraginpekoaren gainetik dauden. <u>Arduradunari zure datu pertsonalak gordetzeko eskatzea, kasu hauetan:</u> ➔ Datuen tratamendua legez kontrakoa bada eta ukituak datuak ezabatzearen aurka egiten badu, eta, horren ordez, datuen erabilera mugatzeko eskatzen badu; ➔ Arduradunak jada ez ditu datuak behar tratamenduaren helburuetarako, baina ukituak behar baditu erreklamazioak egiteko, egikaritzeko edo defendatzeko.
Eramangarritasun erako eskubidea 	**<u>nteresdunak eskubidea du bere datuak beste arduradun bati transmititzeko</u>**, eman zaizkion arduradunal eragozpenik jarri gabe, baldin eta: ● Tratamendua adostasunean edo kontratu bat gauzatzean oinarritzen da. ● Tratamendua bitarteko automatizatuen bidez egiten denean. –

PROCEDIMIENTO DE EJERCICIO DE DERECHOS ARSOPOL

1. INTRODUCCIÓN.

COLEGIO BERRIO-OTXOA IKASTETXEA (MENESIANOS BILBAO) facilitará a los interesados el ejercicio de sus derechos, poniendo para ello a su disposición los modelos de ejercicio de derechos de acceso, rectificación, supresión (derecho al olvido), limitación del tratamiento, portabilidad y oposición (derechos ARSO – POL).
Tan pronto como **MENESIANOS BILBAO** conozca que se ha recibido una solicitud de un interesado, la persona o personas que lo reciban deberán comunicárselo, en la mayor brevedad posible a la persona de referencia dentro de la entidad o personas que corresponda (responsable de sistemas/coordinadora LOPD/DPD) para proceder a su trámite.

2. TRANSPARENCIA DE LA INFORMACIÓN, COMUNICACIÓN Y MODALIDADES DE EJERCICIO DE LOS DERECHOS DEL INTERESADO.

MENESIANOS BILBAO posibilitará la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.
El ejercicio de los derechos por parte del interesado/a será gratuito, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, en cuyo caso **MENESIANOS BILBAO** podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar. Este canon no podrá implicar un ingreso adicional para **MENESIANOS BILBAO**, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud.
En el supuesto de que **MENESIANOS BILBAO** trate una gran cantidad de información sobre un/a interesado/a, podrá pedir a éste/a que especifique la información a que se refiere su solicitud de acceso.

3. ACREDITACIÓN DE LA PERSONALIDAD O REPRESENTACIÓN.

MENESIANOS BILBAO deberá verificar la identidad de quienes soliciten y ejerzan los derechos ARSO – POL. Para ello, la solicitud formulada por el interesado **deberá acompañar copia del documento nacional de identidad, pasaporte u otro documento válido que lo identifique**. También es posible acreditar la identidad mediante firma electrónica cuando el procedimiento de ejercicio de derechos se realice de forma telemática. En el caso de representación, ya sea legal o voluntaria, deberá aportarse el documento que acredite la representación.

4. PLAZOS.

Recibida la solicitud, **MENESIANOS BILBAO** deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de **un mes**. Este plazo se podrá extender dos meses más cuando se trate de solicitudes especialmente complejas, debiendo notificar esta ampliación al interesado dentro del primer mes.

Si **MENESIANOS BILBAO** decide no atender una solicitud, deberá informar de ello motivando su negativa, dentro del plazo de **un mes** desde su presentación.

5. EJERCICIO DE DERECHOS ANTE EL ENCARGADO-A DEL TRATAMIENTO.

MENESIANOS BILBAO podrá contar con la colaboración de los/as encargados/as para atender al ejercicio de los derechos de los/as interesados/as, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

6. DERECHOS DE LOS/LAS AFECTADOS/AS.

Derechos RGPD	¿En qué consisten los derechos de los/las afectados/as?
Derecho de acceso 	**El/La afectado/a será informado/a (cuando aplique al responsable/encargado-a):** – Los fines del tratamiento; categorías de datos personales que se traten y de las posibles comunicaciones de datos y sus destinatarios/as. – De ser posible, el plazo de conservación de tus datos. De no serlo, los criterios para determinar este plazo. – Del derecho a solicitar la rectificación o supresión de los datos, la limitación al tratamiento, u oponerse al mismo. – Del derecho a presentar una reclamación ante la Autoridad de Control. – De su derecho a obtener una copia de los datos objeto del tratamiento. – De la existencia de decisiones automatizadas, la lógica utilizada y las consecuencias de ese tratamiento.
Derecho de rectificación 	**El derecho de rectificación permite al afectado/a que se modifiquen sin dilación indebida los datos personales que resulten ser inexactos o incompletos.** La solicitud de rectificación deberá indicar a qué datos se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.
Derecho de supresión (Derecho al olvido) 	**Con su ejercicio el afectado/a puede solicitar**: – La supresión de los datos personales sin dilación indebida cuando concurra alguno de los supuestos contemplados en la norma. Por ejemplo: o Tratamiento ilícito de datos. o Datos personales ya no sean necesarios en relación con los fines para los que fueron recogido. o Los datos personales deban suprimirse para el cumplimiento de una obligación legal. – No obstante, se regulan una serie de excepciones en las que no procederá este derecho. Por ejemplo: o Prevalezca el derecho a la libertad de expresión e información. o Por razones de interés público en el ámbito de la salud pública. o Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
Derecho de oposición 	**El/La afectado/a puede oponerse al tratamiento**: – Cuando por motivos relacionados con su situación personal, debe cesar el tratamiento de tus datos salvo que se acredite un interés legítimo, o sea necesario para el ejercicio o defensa de reclamaciones. – Cuando el tratamiento tenga por objeto la mercadotecnia directa.

Derecho de oposición al tratamiento de decisiones automatizadas 	A través de este derecho, **se permite al interesado/a oponerse a ser objeto de una decisión basada únicamente en el tratamiento de sus datos**, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre su persona o le afecte significativamente de forma similar. No obstante, **este derecho no será aplicable cuando**: – Sea necesario para la celebración o ejecución de un contrato entre el/la afectado/a y el/la responsable. – El tratamiento de sus datos se fundamente en el consentimiento previamente prestado por el/la interesado/a. – Esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado/a.
Derecho a la limitación del tratamiento 	**Permite al afectado/a:** Solicitar al/la responsable que suspenda el tratamiento de datos cuando: – Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el/la responsable; – El/La afectado/a ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre el afectado/a. Solicitar al responsable que conserve tus datos personales cuando: – El tratamiento de datos sea ilícito y el afectado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso; – El/La responsable ya no necesita los datos para los fines del tratamiento, pero el afectado si los necesite para la formulación, ejercicio o defensa de reclamaciones.
Derecho a la portabilidad 	**El/La interesado/a tiene derecho a transmitir sus datos a otro/a responsable** sin obstáculos por parte del responsable al cual le han sido proporcionados, cuando: – El tratamiento se basa en el consentimiento o en la ejecución de un contrato. – El tratamiento se haga a través de medios automatizados.

SEGURTASUN-URRAKETEN AURREAN JARDUTEKO PROTOKOLOA

1. SARRERA.

BERRIO-OTXOA IKASTETXEAK (MENESIANOS BILBAO) tratatzen dituen datuei buruzko segurtasun-urraketa guztiak jasoko ditu (suntsiketa, galera edo ustekabeko edota legez kontrako aldaketa), eta datuak babesteko agintaritza eskudunari jakinaraziko dio, non eta ez den gertagaitza urratzeak eragindakoen eskubide eta askatasunak arriskuan jartzea.

MENESIANOS BILBAO erakundearen barruan segurtasun-arrakala bat gertatu dela jakin bezain laster, detektatzen duen pertsonak edo pertsonek ahalik eta lasterren (24 ordu) jakinarazi beharko diote dagokion pertsonari (dbo@berrio-otxoaikstetxea.com), **erregistratu, jakinarazi eta ebatzi ahal izateko**.

Jarraian, ezinbestean erregistratuko diren segurtasun-urraketa edo segurtasun-arrailen zerrenda zehazten da. Zerrenda hori ez da mugatzailetzat hartu behar; aitzitik, zabaldu ahal izango da alde batera utzitako beste edozein urraketarekin:

- ★ erabiltzaileen identifikazioan eta autentifikazioan eragina dutenak:
  - Pasahitzak galtzea.
  - Birusa, malwarea, ransomwarea, etab.
  - Sarbidea kontrolatzeko tresnen eta sarbide pribilegiatuen gaineko eskubideak gaizki erabiltzea.
  - Segurtasun-tresnak desaktibatzea.
- ★ datuen sarbidea baldintzatzen dutenak:
  - Sarbideetan huts egindako saiakeren kopurua gainditzea,
  - Bulegotik kanpoko sarbideak
  - Nortasuna ordezkatzeko susmoak.
  - Lanpostuetan idatzizko pasahitzak hautematea.
- ★ Euskarrien kudeaketari eragiten diotenak:
  - Euskarriak ustekabean edo legez kontra galtzea edo aldatzea.
  - Euskarriak leku desegokietan kokatzea.
  - Jasotako euskarrien eduki-akatsak.
- ★ Babes- eta berreskuratze-kopien prozedurei eragiten dietenak:
  - Akatsak babes-kopiak egiteko prozesuetan.
  - Erroreak datuak berreskuratzeko egindako prozesuetan.

2. SEGURTSUN-URRAKETEN ERREGISTROA.

MENESIANOS BILBAO datu pertsonalen segurtasunaren edozein urraketa dokumentatu behar du, horrekin lotutako gertaerak, ondorioak eta hartutako neurri zuzentzaileak barne. Horretarako, proposatutako eredua erabiliko da.

Kontsulta edo azterketa egin behar duten sailei edo pertsonei baino ez zaie emango erregistro horretarako sarbidea.

3. SEGURTASUN-URRAKETEN JAKINARAZPENAK.

Datu pertsonalen segurtasuna urratuz gero, **MENESIANOS BILBAOK** urraketa horren berri eman beharko dio kontrol-agintaritza eskudunari, bidegabeko atzerapenik gabe eta horretarako ezarritako epean (gertakaritik 24 ordura), **non eta ez den gertagaitza pertsona fisikoen eskubide eta askatasunentzat arriskutsua izatea.**

Arrazoia edozein dela ere, ezin bada epearen barruan jakinarazi, **MENESIANOS BILBAOK**atzerapenaren arrazoiak ere adierazi beharko ditu.

3.1 MENESIANOS BILBAO DATUEN TRATAMENDUAREN ARDURADUN GISA JARDUTEN DUENEAN

MENESIANOS BILBAO datuen erabileraren arduraduna denean, tratamenduaren arduradunarekin harremanetan jarri beharko du, bere ardurapean dituen datu pertsonalen segurtasunaren urraketen berri emateko. Gorabehera dokumentatzeko eta jakinarazteko garrantzitsua den informazio guztiarekin, ahal izanez gero. Hori guztia ahalik eta lasterren, bidegabeko atzerapenik gabe eta, ahal dela, horren berri izan eta hurrengo 24 orduetan.

3.2 MENESIANOS BILBAO DATUEN ERABILERAREN ARDURADUNA DENEAN:

3.2.1 KONTROL-AGINTARITZARI JAKINARAZPENA

MENESIANOS BILBAOK tratamenduaren arduradun gisa jarduten badu, segurtasun-urraketa jakin bezain laster jakinarazi beharko du; izan ere, porrotaren jakinarazpena lehenbailehen egin behar zaie agintariei, eta, ahal dela, **horren berri izan eta hurrengo 72 orduetan.**

3.2.2 INTERESADUNEI JAKINARAZPENAK

Gainera, **MENESIANOS BILBAOK** zenbait kasutan segurtasun urraketaren berri eman beharko die interesatuei. Hala ere, interesdunei jakinaraztea ez da beharrezkoa izango honako kasu hauetan:

- **MENESIANOS BILBAOK** neurri tekniko edo antolatzaile egokiak hartuko zituen segurtasuna urratu aurretik.
- Porrota gertatu eta gero, arrisku handia gauzatzeko aukerarik ez dagoela bermatzeko neurri teknikoak hartu baditu **MENESIANOS BILBAOK.**
- Jakinarazpenak neurriz kanpoko ahalegina eskatzen du, eta kasu horietan ordezko neurriekin ordeztu beharko da, esaterako, komunikazio publiko batekin.

4. SEGURTASUN-URRAKETAREN EBAZPENA

Halaber, **MENESIANOS BILBAOK** ondorio negatiboak arintzeko antzeman den segurtasun-urraketari irtenbidea emateko hartu diren neurri zuzentzaileak dokumentatuko ditu.

PROTOCOLO DE ACTUACIÓN ANTE VIOLACIONES DE SEGURIDAD

1. INTRODUCCIÓN.

COLEGIO BERRIO-OTXOA IKASTETXEA (MENESIANOS BILBAO), recogerá cuantas violaciones de seguridad (*destrucción, pérdida o alteración accidental o ilícita)* que se produzcan sobre los datos que trata y lo va a notificar a la autoridad de protección de datos competente, a no ser que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

Tan pronto como se conozca que se ha producido una brecha de seguridad dentro de **MENESIANOS BILBAO**, la persona o personas que lo detecten deberán comunicárselo con la mayor brevedad posible (24 h.) a la persona o personas que corresponda (dbo@berrio-otxoaikastetxea.com) para proceder a su **registro, notificación y resolución**.

A continuación, se presenta una lista de violaciones o brechas de seguridad que serán inexcusablemente registradas. Esta lista no debe entenderse como limitativa, sino que podrá ser ampliada con cualquier otro tipo de violaciones que hubieran quedado omitidas:

- Que afecten a la identificación y autenticación de los usuarios:
  - ★ Pérdida de contraseñas.
  - ★ Virus, malware, ransomware, etc.
  - ★ Mal uso de derechos sobre herramientas de control de acceso y accesos privilegiados.
  - ★ Desactivación de las herramientas de seguridad.
- Que afecten al a la accesibilidad a los datos:
  - ★ Superar el número de intentos fallidos de accesos,
  - ★ Accesos fuera de horas de oficina
  - ★ Sospechas de suplantación de personalidad.
  - ★ Detección de contraseñas escritas en los puestos de trabajo.
- Que afecten a la gestión de soportes:
  - ★ Pérdida o alteración accidental o ilícita de soportes.
  - ★ Localización de soportes en lugares inadecuados.
  - ★ Errores de contenido en soportes recibidos.
- Que afecten a los procedimientos de copias de salvaguarda y recuperación:
  - ★ Errores en los procesos de realización de copias de salvaguarda.
  - ★ Errores en procesos de recuperaciones de datos realizadas.

2. REGISTRO DE VIOLACIONES DE SEGURIDAD.

MENESIANOS BILBAO tiene que documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Para ello, se utilizará el modelo propuesto

El acceso a este registro será facilitado estrictamente a aquellos departamentos o personas que lo necesiten para su consulta o análisis.

3. NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD.

En caso de violación de seguridad de los datos personales, **MENESIANOS BILBAO** deberá notificar tal violación a la autoridad de control competente sin dilación indebida y en el plazo establecido para hacerlo (24h. desde el suceso), **SALVO que sea improbable que constituya un riesgo para los derechos y libertades de las personas físicas.**

Si por el motivo que fuere, resulta imposible notificar en el plazo, **MENESIANOS BILBAO** deberá acompañar una indicación de los motivos de la dilación.

3.1 CUANDO MENESIANOS BILBAO ACTÚA COMO ENCARGADO DEL TRATAMIENTO

MENESIANOS BILBAO actuando como ENCARGADO DEL TRATAMIENTO, tendrá que ponerse en contacto con el responsable del tratamiento, para comunicarle las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento. Con toda la información relevante para la documentación y comunicación de la incidencia, en caso de que sea posible. Todo ello con la mayor brevedad posible, sin dilación indebida y, a ser posible, dentro de las 24 horas siguientes a que se tenga constancia de ella.

a. CUANDO MENESIANOS BILBAO ES RESPONSABLE DEL TRATAMIENTO:

i. NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

Si **MENESIANOS BILBAO** actúa como RESPONSABLE DEL TRATAMIENTO, deberá notificar la violación de seguridad tan pronto como se conozca, pues la notificación de la quiebra a las autoridades debe producirse **sin dilación indebida y, a ser posible, dentro de las 72 horas** siguientes a que se tenga constancia de ella.

ii. NOTIFICACIÓN A LOS INTERESADOS

Además, **MENESIANOS BILBAO** en algunos casos deberá comunicar la violación de seguridad a los interesados. Ahora bien, la notificación a los interesados no será necesaria cuando:

- **MENESIANOS BILBAO** hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad.
- **MENESIANOS BILBAO** haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- La notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

4. RESOLUCIÓN DE LA VIOLACIÓN DE SEGURIDAD

MENESIANOS BILBAO documentará también las medidas correctivas que han sido adoptadas para poner solución a la violación de seguridad que se ha detectado para mitigar los posibles efectos negativos.

PASAHITZEN POLITIKA ETA SARBIDE-KONTROLA

1.SARRERA

BERRIO-OTXOA IKASTETXEAK (MENESIANOS BILBAO) erabiltzaileak identifikatzeko eta autentifikatzeko jarraitu duen prozedura (erakundearen barruan datu pertsonaletarako sarbidea duen pertsona oro, zuzenean edo zeharka), sistemara, sarera edo aplikazioetara sartzen saiatzen direnean, erabiltzailea identifikatzeko kode baten (ID) eta pasahitz baten konbinazioan oinarritzen da. Erabiltzaile bakoitzari identifikatzaile bakarra esleitu zaio, bai sisteman sartzeko, bai aplikazioetan sartzeko (ahal den kasuetan). ID partekatuen erabilera salbuespenezkoa izango da, eta arduradunak edo Zuzendaritzak argi eta garbi justifikatu beharko du negozio-beharrengatik edo negozio-eragiketak garatzeko beharrezkoak diren aplikazioen mugaketengatik.

Ezarritako sistemak informazio-sistemara baimenik gabe behin eta berriz sartzen saiatzeko aukera mugatzen duen mekanismo bat du.

2. PASAHITZAK SORTZEKO, BILTEGIRATZEKO ETA MANTENTZEKO PROZEDURA.

2.1 SORRERA:

- IKT/sistemen sailak pribilegioen esleipena eta erabilera murriztu eta kontrolatuko du.
- Pribilegio espezifikoak esleituko dira, ez orokorrak. Pribilegioak aplikazioaren eta dokumentazio-mailaren arabera definituko dira. Hau da, aplikazio espezifiko bakoitza bereizita hartuko da kontuan, baimendu gabeko informaziorako sarbiderik ez izateko.
- Pribilegioak erabiltzeko benetako premien arabera esleituko zaizkio pertsona bakoitzari, eta erabiltzailearen arduradun nagusiaren jarraibideen arabera, hark adieraziko dizkio sistema-sailari eman beharreko pribilegioak.
- Behin-behineko pasahitzek bakarrak izan behar dute, eta ezin dira asmatu. Ezin da beti behin-behineko gako bera sortu, eta gako horiek ez dute erraz asma daitekeen parametrorik izan behar, hala nola NANa edo erraztasunez asma daitezkeen datak.

2.2 PRIBATUTASUNA:

- Erabiltzaile-identifikadoreak eta horiekin lotutako sarbide-pasahitzak erabilera pertsonalekoak eta besterenezinak izango dira; hortaz, ezin izango dira partekatu.
- Pasahitzak pasahitzaren jabe den erabiltzaileak baino ez ditu ezagutu behar, eta informazio pertsonal eta besterenezin gisa tratatu behar dira. Erabiltzailearen ardura da pasahitzaren konfidentzialtasuna eta zaintza ziurtatzea.
- Erakundeak zenbait ohar egin ditu pasahitz bat aukeratzerakoan, eta sistemaren erabiltzaile guztiek aplikatu beharko dituzte:
    - Pasahitz seguruak sortuko dira luzeran eta karaktereetan (gutxienez 6 eta alfanumerikoak), eta erreferentzia pertsonalak, seme-alaben izenak, jaiotza-datak eta aba saihestu egingo dira.
    - Pasahitzak erraz gogoratzeko modukoak izan behar dira.

- Kontuan izan pasahitz bat hiztegi-erasoen aurrean kaltebera izan daitekeela (pasahitza aurkitu arte hiztegiko hitzak automatikoki probatzen dituzten aplikazioak daude).
- Ez erabili zenbakizko segidako karaktereak edo alfabetikoak, hala nola "uuuuu" "555555".
- Pasahitzak tarte erregularretan aldatzea. Zenbat eta sarbide-maila handiagoa izan, orduan eta txikiagoa izango da pasahitzak aldatzeko maiztasuna.
- Pasahitza aldatu beharko litzateke lehenengo sarreran.
- Ez erabili lan-inguruneko aplikazioetan eremu indibidual edo pertsonaletan erabiliko zenuke pasahitz bera. Ez jarri beti pasahitz bera sistema guztietan.
- Edozein erabiltzaileren pasahitza adierazten duen idatzizko komunikazioa saihestuko da.

2.3 BILTEGIRATZEA:

- Pasahitzak hirugarrenek ezin ulertzeko moduan biltegiratzen dira.
- Pasahitzen konfidentzialtasunari eutsi beharko zaio, eta ez zaizkio inori emango inolako egoeraren aurrean, edozein dela ere pasahitza galdetu duen pertsona.
- Goi-mailako profilek behar duten informazioa eskuratu ahal izango dute. Horrela ez bada, baimena eskatu beharko dute, baina gakoak ez dizkiote inoiz lankide edo hirugarren bati eskatuko.
- Debekatuta dago gakoen erregistro bat gordetzea (paperean, ekipoko dokumentu batean, edo eskuzko gailuetan: agendetan, libretetan, etab.).
- Pasahitzak aldatu beharko dira, baldin eta pasahitzen segurtasuna arriskuan egon daitekeela antzematen bada.
- Gakoak prozesu automatikoetan ez sartzea. Debekatuta dago pasahitzak gordetzea pasahitza gogoratzea eskatzen duten aplikazioetan.
- Pasahitzak erabiltzailearen erantzukizuna dira.

2.4 MANTENTZEA:

- Erabiltzaileak pasahitz guztiak aldatu behar ditu, gutxienez aldizkakotasun-atalean ezarritako maiztasunarekin. Posible den inguruneetan automatizatu egingo da iraungitze-errekerimendu hori. Ezinezkoa denean, erabiltzailea izango da aldaketa sistematikoaren erantzule.
- Ahaztuz gero edo pasahitzekin lotutako edozein zailtasun izanez gero, erabiltzaileek IKT sistemaren/sailaren administratzailearen laguntza izango dute.

3.SARBIDE-KONTROLA.

Informaziorako sarbidea, informazioa tratatzeko baliabideak eta negozio-prozesuak erakundearen beharren arabera kontrolatuko dira.

Informazio-aktiboak dituzten eta, beraz, zuzendaritzaren aurrean "beren" aktiboak babesteko ardura duten pertsonek, zuzendaritzak hala ezarri duenean, sarbidea kontrolatzeko arauak eta beste segurtasun-kontrol batzuk definitu edota onartu beharko dituzte.

Erabiltzaileek gutxieneko pribilegio-politikari jarraituz jasoko dituzte sarbide-eskubideak. Hau da, beren eginkizunak betetzeko behar dituzten datu eta baliabide informatikoen sarbidea.

Erabiltzaile bakoitzaren saileko arduradunak, egingo dituen lanen arabera, erabiltzaileak zer aplikazio erabili ahal izango dituen erabakiko du.

Prozedura honen ERANSKIN 1 dokumentuak erabiltzaile bakoitzarentzako SARBIDE BAIMENDUA DUTEN ERABILTZAILEEN ZERRENDAREN eredua jasotzen du, eta sail bakoitzeko arduradunak osatu beharko du.

Bestalde, Segurtasuneko Arduradunak/IKT Arduradunak LAN-PROFILAREN ARABERAKO SARBIDE-ESKUBIDEEN eredua egingo eta eguneratuta mantenduko du. Eredu hori prozedura honen ERANSKIN 2 dokumentuan dago jasota.

Segurtasuneko Arduraduna/IKT Arduraduna sistemaren eta aplikazioen erabiltzaileen mantentze-lanez arduratzen da, honako irizpide hauek kontuan hartuta:

3.1 ERABILTZAILEAREN ALTA:

Segurtasuneko Arduradunak/IKT Arduradunak bakarrik du erabiltzaileen identifikatzaileei alta emateko eta aplikazioetarako eta tratamenduetarako sarbide-maila desberdinetarako definitutako profilekin lotzeko eskumena.

Sisteman edo aplikazioetan berri bati alta eman behar dioten erabiltzaileen zuzeneko arduradunek Segurtasun-Arduradunari/IKT Arduradunari jakinarazi beharko diote.

Erakundearen Zuzendaritzak du erabiltzaileen sarbide-eskubideei buruzko azken erabakia.

Alta eman ondoren, Segurtasun-Arduradunak/IKTen Arduradunak erabiltzaile berriari eta eskaera baimendu zuen arduradunari jakinaraziko die, haren datuak eta esleitutako erabiltzailearen identifikatzailea adierazita.

Erabiltzailea sisteman lehen aldiz sartzeko, Segurtasun-Arduradunak/IKT Arduradunak isilpean jakinaraziko ditu bere identifikatzailea eta hasierako sarbide-pasahitza, politika honen 2. atalean xedatutakoaren arabera.

Honako arau hauek hartuko dira kontuan identifikatzaileak esleitzerakoan:

- Ez da identifikatzaile bat berrerabiliko.
- Gutxienez bost karaktere erabili behar dira erabiltzailearen identifikatzailearen konposizioan.
- Aldatu ezin diren sistema eragileen eta software-aplikazioen berezko erabiltzaile-izenak baino ezin dira mantendu

3.2 ERABILTZAILE BATEN BAJA:

Giza Baliabideen arloak edo erabiltzaileak baja hartzen duen saileko arduradunak Segurtasun-Arduradunari/IKT Arduradunari baja hori jakinarazi beharko dio, eta azken hori arduratuko da erabiltzailea eta sarbide-eskubideak ezeztatzeaz.

3.3 ERABILTZAILE BATEN BAIMENAK ALDATZEA:

Erabiltzaile baten sarbide-eskubideak edo baimenak aldatzeko, baimen hierarkiko bera beharko da, erabiltzaile-tipologia bakoitzerako bereizia, alta emateko protokoloan deskribatuta dagoena. Beraz, alta-atalean adierazitako prozedura baimenak aldatzeko puntu honetara hedatu ahal izango da.

3.4 ERABILTZAILEAK BERRAKTIBATZEA:

Erabiltzaileak berraktibatzeko, aurretik aipatutako gainerako protokoloekiko prozedura desberdina behar da; izan ere, aldez aurretik alta bat izatearen premisatik abiatzen da, eta ez da beharrezkoa erabiltzaileak sisteman baimenak aldatzea.

Erabiltzailea sisteman sartzen ez bada ustekabeko arrazoiengatik (pasahitza ahaztea, jarduerarik gabeko denbora luzea edo huts egindako saio gehiegi), erabiltzailea berraktibatu ahal izateko, Segurtasun-Arduradunari/IKT Arduradunari jakinarazi beharko zaio egoera konpon dezan.

4. SARBIDE-ERREGISTROA.

Erabiltzaile guztiek beren lanpostua konfiguratuta eduki beharko dute jarduerarik gabeko 10 minutuko aldi baten ondoren sistemara itzultzen saiatzean pasahitz bat sartzea eska dezan.

Segurtasun-Arduradunak/IKT Arduradunak baimendutako langileak soilik sartu ahal izango dira informazio-sistemen euskarri diren ekipo fisikoak instalatuta dauden lekuetara (Datuak Prozesatzeko Zentroa).

4.1 SARBIDE-ERREGISTROA:

Langileek babes bereziko datuak eskuratzen dituztenean (*etnia- edo arraza-jatorria, iritzi politikoak, sinesmen erlijioso edo filosofikoak, sindikatu-afiliazioa, datu genetikoen tratamendua, pertsona fisiko bat identifikatzeko datu biometrikoak, osasunari buruzko datuak edo pertsona baten bizitzari edo sexu-orientazioei buruzko datuak)*, datu-basearen aplikazioak edo sistema kudeatzaileak honako informazio hau erregistratu beharko du:

1. Erabiltzailearen identifikazioa,
2. Sartzeko data eta ordua,
3. Ikusitako fitxategia,
4. Sarbide-mota eta
5. Baimendu edo ukatu den.
6. Sarbidea baimenduta badago, sartutako erregistroaren identifikatzailea erregistratuko da.

Sarbideen erregistroa hilero berrikusiko da, eta antzemandako gorabeherak deskribatzen dituen txosten bat egingo da.

Sarbideen erregistroko informazioa gutxienez bi urterako gordeko da.

Sarbideen erregistroa gaitzen duten mekanismoak ezin izango dira inola ere desaktibatu.

POLÍTICA DE CONTRASEÑAS Y CONTROL DE ACCESO

1.INTRODUCCIÓN.

El procedimiento seguido por **COLEGIO BERRIO-OTXOA IKASTETXEA (MENESIANOS BILBAO)**, para la identificación y autenticación de los usuarios (*toda persona dependiente directa o indirectamente dentro de la entidad con acceso a datos de carácter personal*) cuando intentan acceder al sistema, la red o las aplicaciones está basado en la combinación de un código de identificación de usuario (ID) y una contraseña. A cada usuario se le ha sido asignado un identificador único tanto para el acceso al sistema, como para el acceso a las aplicaciones (en aquellos casos en los que sea posible). La utilización de ID compartidos será excepcional y deberá estar justificada claramente por necesidades de negocio o limitación de aplicaciones necesarias para el desarrollo de las operaciones de negocio por el responsable de éste o la Dirección.

El sistema implementado dispone de un mecanismo que limita la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

2. PROCEDIMIENTO DE GENERACION, ALMACENAMIENTO Y MANTENIMIENTO DE CONTRASEÑAS.

2.1 Generación:

- La asignación y el uso de privilegios estarán restringidos y controlados por el departamento de sistemas/TIC.
- Se asignarán privilegios específicos y no generales. Los privilegios estarán definidos por aplicación y por nivel de documentación. Esto es, cada aplicación específica será tomada en consideración por separado para evitar accesos a información no autorizados.
- Los privilegios se asignarán a cada persona en base a las necesidades reales de uso y conforme a las indicaciones del superior responsable del usuario, será este quien indicará al departamento de sistemas los privilegios que deberá de conceder.
- Las contraseñas provisionales deben ser únicas y no adivinables. No se puede generar siempre la misma clave provisional y estas no deben contener parámetros que se puedan llegar a desentrañar como, por ejemplo, un DNI o fechas fácilmente adivinables.

2.2 Privacidad:

- Los identificadores de usuario y contraseñas de acceso asociadas serán de uso personal e intransferible y por tanto no pueden ser compartidos.
- Las contraseñas deben ser conocidas exclusivamente por el usuario propietario de la misma y tratadas como información personal e intransferible. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña.
- La entidad ha establecido ciertas consideraciones a la hora de elegir una contraseña que deberán ser aplicadas por todos los usuarios del sistema:
  - ✓ Se generarán contraseñas seguras, en longitud y caracteres (mínimo 6 y alfanuméricos) y evitar cualquier referencia de índole personal, nombres de hijos o hijas, fechas de nacimiento etc.
  - ✓ Las contraseñas deben ser fáciles de recordar.
  - ✓ Evitar que una contraseña sea vulnerable a ataques de diccionario (aplicaciones que automáticamente prueban palabras de diccionario hasta dar con la contraseña).

- ✓ No utilizar caracteres consecutivos numéricos o alfabéticos., como por ejemplo “aaaaa” “555555”.
- ✓ Cambiar las contraseñas a intervalos regulares. Cuanto mayor nivel de acceso menor deberá ser la periodicidad del cambio de las contraseñas.
- ✓ Se debería cambiar la contraseña en la primera entrada.
- ✓ No usar la misma contraseña para las aplicaciones individuales o personales que las del entorno laboral y evitar poner siempre la misma contraseña en los distintos sistemas.
- ✓ Se evitará la comunicación escrita que revele la contraseña de cualquier usuario.

2.3 Almacenamiento:

- Las contraseñas se almacenan de forma ininteligible para terceros.
- Se deberá mantener la confidencialidad de las contraseñas y no proporcionárselas a nadie ante ninguna situación, independientemente de la persona que se las pregunte.
- Los perfiles superiores tendrán acceso a la información que necesiten y, en caso contrario, deberán solicitar autorización, pero nunca solicitar las claves a un compañero/a o tercero.
- Está prohibido guardar un registro de claves (en papel, en un documento en el equipo, o en dispositivos manual como agendas, libretas, etc.).
- Se deberá cambiar las contraseñas siempre que detecte que la seguridad de las mismas ha podido quedar comprometida.
- No incluir las claves en los procesos automáticos. Está prohibido almacenar las contraseñas en las aplicaciones que solicitan recordar contraseña.
- Las contraseñas son responsabilidad del usuario o la usuaria.

2.4 Mantenimiento:

- Todas las contraseñas deben ser modificadas por el usuario al menos con la frecuencia establecida en al apartado de periodicidad. En los entornos en los que sea posible se automatizará este requerimiento de caducidad. Cuando no sea posible, el usuario será responsable del cambio sistemático.
- En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia del administrador del sistema/departamento TIC.

3.CONTROL DE ACCESO.

El acceso a la información, los recursos de tratamiento de información y los procesos de negocio serán controlados según las necesidades de la entidad.

Las personas que poseen activos de información y que, por tanto, son responsables ante la dirección de la protección de "sus" activos, cuando la dirección así lo haya establecido tendrán/deberán definir y/o aprobar las reglas de control de acceso y otros controles de seguridad.

Los usuarios recibirán sus derechos de acceso siguiendo la política de mínimo privilegio. Es decir, únicamente a aquellos datos y recursos informáticos que precisen para el desempeño de sus funciones.

El responsable del departamento de cada usuario, en función de las tareas que prevea que va a desempeñar, determinará qué aplicaciones serán accesibles por el usuario.

El ANEXO 1 de este procedimiento incluye modelo de *RELACIÓN DE USUARIOS CON ACCESO AUTORIZADO* para cada usuario, que deberá ser completado por el responsable de cada departamento.

Por su parte el Responsable de Seguridad/Responsable TIC elaborará y mantendrá actualizado el modelo de *DERECHOS DE ACCESOS POR PERFIL LABORAL* correspondiente ANEXO 2 incluido en este procedimiento.

El Responsable de Seguridad/Responsable TIC es el encargado del mantenimiento de los usuarios del sistema y aplicaciones, teniendo en cuenta los siguientes criterios:

3.1 ALTA DE USUARIOS:

Únicamente el Responsable de Seguridad/Responsable TIC tiene competencias para dar de alta los identificadores de usuarios y asociarlos a los perfiles definidos para los distintos niveles de acceso a las aplicaciones y tratamientos.

Los responsables directos de los usuarios que tengan que dar de alta a uno nuevo en el sistema o a las aplicaciones, deberán notificárselo al Responsable de Seguridad/ Responsable TIC.

La Dirección de la entidad es quien tiene la última decisión sobre los derechos de acceso de los usuarios.

Una vez dada el alta, el Responsable de Seguridad/Responsable TIC comunicará al nuevo usuario y al responsable que autorizó la solicitud, indicando los datos de éste y el identificador de usuario asignado.

Para el primer acceso del usuario al sistema, el Responsable de Seguridad/Responsable TIC comunicará de forma confidencial su identificador y su contraseña de acceso inicial, según lo dispuesto en el apartado 2 de la presente política.

Se tendrán en cuenta las siguientes normas en la asignación de identificadores:

- No se reutilizará un identificador.
- Deben utilizarse al menos cinco caracteres en la composición del identificador del usuario.
- Se pueden mantener únicamente aquellos nombres de usuario propios de los sistemas operativos y de las aplicaciones de software que no puedan ser modificados.

3.2 BAJA DE UN USUARIO:

El área de Recursos Humanos o el responsable del departamento donde el usuario cause baja deberán comunicar dicha baja al Responsable de Seguridad/Responsable TIC quien se encargará de cancelar el usuario y sus derechos de acceso.

3.3 MODIFICACIÓN DE PERMISOS DE UN USUARIO:

La modificación de los derechos o permisos de acceso de un usuario requerirá de la misma autorización jerárquica, diferenciada para cada tipología de usuarios, ya descrita en el protocolo de alta. Por lo tanto, el procedimiento enunciado en el apartado de alta será extensible a este punto de modificación de permisos.

3.4 REACTIVACIÓN DE USUARIOS:

La reactivación de usuarios exige un procedimiento diferenciado respecto al resto de protocolos enunciados anteriormente, ya que parte de la premisa de la existencia de un alta previa y no requiere de un cambio de permisos del usuario en el sistema.

Para aquellos casos en que el acceso del usuario al sistema se haya revocado por causas accidentales, como el olvido de la contraseña, un periodo prolongado de inactividad o un excesivo número intentos fallidos, la reactivación del usuario exigirá su comunicación al Responsable de Seguridad/Responsable TIC para subsanar la situación.

4. REGISTRO DE ACCESOS.

Todos los usuarios deberán tener configurado su puesto de trabajo para que se exija la introducción de una contraseña al intentar volver al sistema, tras un periodo de 10 minutos de inactividad.

Exclusivamente el personal autorizado por Responsable de Seguridad/Responsable TIC podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información (Centro de Procesado de Datos).

REGISTRO DE ACCESOS:

Cuando el personal accede a datos especialmente protegidos (*origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, afiliación sindical, tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o las orientaciones sexuales de una persona*) la aplicación o el sistema gestor de la base de datos deberá registrar la siguiente información:

1. Identificación del usuario,
2. La fecha y hora en que se realizó el acceso,
3. El fichero accedido,
4. El tipo de acceso y,
5. Si ha sido autorizado o denegado.
6. En el caso de que el acceso haya sido autorizado, se registrará el identificador del registro accedido.

El registro de accesos será revisado mensualmente y se elaborará un informe describiendo las incidencias detectadas.

La información del registro de accesos se conservará por un período mínimo de dos años.

Los mecanismos que habilitan el registro de los accesos no podrán, bajo ningún concepto, ser desactivados.