10.00.-Código de conducta

El Código de Conducta es un elemento clave de la política de control interno para garantizar que se dispone de los mecanismos apropiados para apoyar a los empleados en el cumplimiento de sus obligaciones y en el desarrollo de las actividades comerciales. Recoge los valores éticos, compromisos y buenas prácticas que deben ser aplicados en la gestión del negocio. Debemos garantizar que la actividad se desarrolla con la máxima integridad. Todos los empleados son responsables del cumplimiento de estas pautas como elemento imprescindible del modelo de negocio. El Código afecta a todos los empleados, independientemente de su función, localización o nivel jerárquico.

CÓDIGO CONDUCTA EMPLEADOS

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

INDICE

INTRODUCCIÓN

Nuestro Código de conducta es un documento que resume las diversas políticas y prácticas que están vigentes en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL relacionadas con el comportamiento de las personas y del centro.

El Código de conducta establece las normas de comportamiento responsable que todos los empleados de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL deben cumplir.

El presente Código de conducta está diseñado para ayudar a todas las personas a ejercer los comportamientos esperados.

Compromisos de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL con sus empleados:

- Respetarles profesional y personalmente.
- Ofrecerles un entorno y unas condiciones laborales que faciliten el cumplimiento y mejora de su trabajo y la estabilidad en el empleo.
- Facilitar los medios y recursos adecuados así como la formación para el mejor desempeño, la excelencia en su trabajo y el crecimiento profesional.
- Establecer los sistemas adecuados de reconocimiento individual y grupal bajo los principios de equidad y justicia.
- Reconocer la diversidad de personas como una fuente de riqueza para el centro y, en consecuencia, establecer las políticas de gestión del talento y de la diversidad adecuadas para que cada uno pueda contribuir al éxito de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL
- Promover la igualdad de oportunidades entre hombres y mujeres.
- Apoyar al empleado para que alcance el equilibrio entre la vida personal y la profesional.

PRINCIPIOS

Principios que han de guiar y orientar el comportamiento profesional de los empleados de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL en el marco de sus actividades y obligaciones laborales y profesionales.

Este código de conducta recoge el compromiso de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL de actuar conforme a unos valores que garanticen un comportamiento responsable y con absoluto respeto a la legalidad vigente, en todas las relaciones de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL , con sus propios empleados.

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL considera a los empleados una parte esencial de la compañía y desea mantener con ellos una relación basada en la creación de valor, la confianza mutua, la responsabilidad, el compromiso y la integridad. Para ello se compromete a:

- Promover las herramientas necesarias para que la comunicación entre los empleados y la empresa fluya adecuadamente.
- Promover la transparencia, transmitir y compartir la información necesaria para el desempeño laboral así como respecto a las decisiones que les atañen.
- Fomentar el trabajo en equipo, la delegación, la cooperación, coordinación y otras formas de apoyo mutuo impulsando el éxito colectivo.
- Fomentar la participación en las decisiones que les afectan.
- Conocer el grado de satisfacción del empleado con su trabajo así como establecer las herramientas adecuadas para incorporar sus sugerencias y aportaciones sobre cómo realizar mejor el trabajo.
- Estimular, promover, encauzar y reconocer la creatividad de los empleados.

FINALIDAD

La asunción por Servicios Centrales FUNDACION ESCOLAPIAS MONTAL de un código de conducta representa el compromiso expreso de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL de aceptar unos criterios de conducta a cuyo estricto cumplimiento se vincula.

Este código de conducta (al que, en lo sucesivo, nos referiremos como "el código") tiene la finalidad de proporcionar a todos los empleados las directrices para una conducta adecuada respecto a los compañeros y superiores, así como en su trato con las familias de nuestro alumnado . El objetivo es fomentar la integridad de los empleados y, por lo tanto, del centro.

DESTINATARIOS

Son destinatarios del código de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL todos sus empleados, que deberán conocer y aceptar su contenido y obligarse a su cumplimiento en el momento de su incorporación a la Compañía .

Todos los empleados velarán por el cumplimiento de la legislación y normativa vigente en el lugar en el que desarrollen su actividad. Asimismo, en todo momento respetarán los compromisos y obligaciones asumidos por Servicios Centrales FUNDACION ESCOLAPIAS MONTAL en sus relaciones contractuales con terceros.

¿QUE ESPERAMOS DE NUESTROS EMPLEADOS?

– El compromiso con Servicios Centrales FUNDACION ESCOLAPIAS MONTAL y sus valores.

– El compromiso con su propio desarrollo profesional y las oportunidades de formación y mejora que ofrece el centro.

– El cumplimiento de las normas y políticas del centro.

– La dedicación leal al coelgio en los horarios establecidos así como el uso honrado y eficaz del tiempo y los recursos necesarios para el desempeño de su trabajo, evitando la utilización de éstos para fines extra laborales o particulares.

– Un comportamiento respetuoso, justo e íntegro en el ámbito laboral y en las relaciones con todos los públicos con los que operamos y en especial con las familias de nuestro alumnado.

– La imparcialidad, equidad e integridad en el trato a otros empleados, alumnos, proveedores o cualquier otra persona que tenga una vinculación contractual con Servicios Centrales FUNDACION ESCOLAPIAS MONTAL evitando cualquier favoritismo así como la obtención de ventajas personales, la parcialidad o el abuso de poder o posición.

-La privacidad y la protección de datos es una de la máximas prioridades de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL siendo conscientes que la información es uno de los activos más valiosos que existen. Por esta razón, damos una serie consejos básicos sobre el tratamiento de información:

- Enviar e- mails con las direcciones de correo en Copia Oculta (CCO).
- Eliminar los papeles en destructora.
- Custodiar los papeles que se emitan o reciban por impresoras, faxes, etc.
- Cumplir con la política de "mesas limpias" (guardando el papel bajo llave).
- Custodiar los soportes de datos en los traslados.
- Cumplir con el "Compromiso de confidencialidad en el tratamiento de datos de carácter personal"

Consultar al Responsable de la empresa o a rgpd@auratechlegal.es siempre que tenga dudas, y más concretamente cuando:

- Se recojan nuevos datos personales.
- Se vaya a enviar publicidad/información comercial propia o de terceros
- Se vayan a facilitar datos a terceros.
- Se vayan a utilizar datos personales con una finalidad distinta a la inicial.
- Se traten datos que permitan elaborar perfiles.
- Se produzca o detecte una incidencia que afecte a datos personales
- Se reciba cualquier escrito relativo a la protección de datos.

CÓDIGO DE BUENAS PRÁCTICAS

- La lealtad a la compañía no desempeñando otras funciones, cargos, responsabilidades, desarrollando actividades o participando en sociedades que supongan competencia desleal, conflicto de intereses o interferencia en sus obligaciones laborales.
- El trato confidencial de la información y su utilización restringida al ámbito de nuestro trabajo con especial atención al respeto a la privacidad de los clientes.
- Una relación con las familias presidida por la profesionalidad, la atención a los detalles, la cortesía, amabilidad, confianza y la disponibilidad, interés y rapidez en atender sus necesidades, así como una actitud proactiva creativa y emprendedora.

COMPETENCIA DESLEAL

Mediante el presente documento Servicios Centrales FUNDACION ESCOLAPIAS MONTAL acota el concepto de "*competencia*", entendiéndose ésta, en su vertiente "*desleal*", como los actos llevados a cabo por uno de sus trabajadores que sirviéndose de los conocimientos, medios y contactos adquiridos durante su estancia en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL , puedan ser utilizados a favor de otra actividad, por cuenta propia o ajena, sin el consentimiento de la dirección de la fundación o del centro, siempre que con dichos actos se causen daños o perjuicios reales o predecibles.

CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

Los empleados están obligados a mantener la confidencialidad en relación con todos los asuntos internos de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL de naturaleza confidencial, así como con la información confidencial propiedad de correspondiente a las familias. La información se considera confidencial si está marcada como tal o si resulta claramente evidente que contiene secretos empresariales o comerciales. En caso de duda, se debe consultar al responsable directo o a rgpd@auratechlegal.es

Se debe prestar especial atención, para evitar la revelación involuntaria de este tipo de información en las operaciones comerciales del día a día y en las conversaciones con amigos y familiares.

La responsabilidad en cuanto a la protección de información confidencial es una obligación legal que continúa incluso después de dejar el centro.

La información confidencial debe protegerse de su divulgación a terceros. Incluso cuando se gestiona internamente y antes de que se transfiera dentro de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL, debe respetarse el principio general según el cual la información confidencial debe hacerse llegar sólo a aquellos empleados que la necesitan para el desarrollo de sus tareas oficiales.

Los empleados están obligados a respetar las normativas de protección de datos y a contribuir de forma activa a garantizar que los datos confidenciales y, en especial, los datos personales no son accesibles a terceros. Los datos personales sólo deben recopilarse, procesarse y utilizarse en la medida en que lo permitan la Ley de Protección de Datos, otras leyes aplicables y los acuerdos profesionales pertinentes. En caso de duda, el empleado debe consultar el caso con el responsable de protección de datos de la empresa escribiendo al correo rgpd@auratechlegal.es . Todos los empleados están obligados a respetar las normativas de protección de datos y a mantener la confidencialidad acerca de los secretos empresariales y operacionales.

Se deberá tratar diligentemente y de acuerdo a las reglas de la buena fe toda aquella información de carácter corporativo a la que pueda tener acceso como empleado de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

No se podrá revelar, sin el consentimiento debido, ninguna información perteneciente a Servicios Centrales FUNDACION ESCOLAPIAS MONTAL exceptuando la estrictamente necesaria para dar el debido cumplimiento de sus obligaciones o en los excepcionales casos de requerimiento judicial o autoridad competente. Estas obligaciones se desprenden del deber de confidencialidad y secreto cuando se trate de datos de carácter personal, y deberán ser cumplidas no solo durante la vigencia de dicha relación laboral sino incluso, cuando se extinga por cualquier causa la relación laboral que le une a Servicios Centrales FUNDACION ESCOLAPIAS MONTAL Las mencionadas obligaciones se desprenden del REAL DECRETO LEGISLATIVO 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (a partir de ahora ET) concretamente de su artículo 5.1 a), así como las estipulaciones del Reglamento General de Protección de Datos (en adelante RGPD) en especial el Considerando 39.

El empleado declara así mismo conocer que el incumplimiento de este compromiso puede generar el ejercicio de acciones disciplinarias por parte de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL , tal y como establece el artículo 58 ET.

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL informa que los datos personales que nos ha proporcionado así como aquellos que pueda facilitarnos en un futuro, serán utilizados para las siguientes razones en aras a dar cumplimiento a la relación laboral vigente:

- Controlar la utilización que realice de los recursos del centro a los que pudiera tener acceso, como el uso y gasto telefónico, la utilización de Internet, los servicios de mensajería instantánea, así como el correo electrónico, que son recursos de uso exclusivo en el ámbito profesional.
- Realizar el pago de las nóminas.
- Llevar a cabo las obligaciones existentes en materia de protección de la salud, prevención de riesgos laborales y demás cumplimiento normativo.
- Gestionar y controlar su participación, asistencia y aprovechamiento en las acciones formativas organizadas por la empresa en las que en su caso participe.
- Realizar el control del absentismo, así como el cumplimiento del horario laboral.
- Remitir aquellas comunicaciones que pudieran llevarse a cabo desde Servicios Centrales FUNDACION ESCOLAPIAS MONTAL o desde los servicios legales de Auratech Legal Solutions.

El trabajador se compromete al cumplimiento de las siguientes obligaciones:

- Los usuarios del sistema, deben conocer y aceptar las normas de seguridad de la organización.
- Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.
- Cumplimiento de política de “mesas limpias”.
- Las pantallas, impresoras o cualquier otro tipo de dispositivos conectados al puesto de trabajo, deberán estar ubicados en lugares que garanticen confidencialidad e impidan accesos no autorizados.
- El usuario, cuando abandone su puesto de trabajo, temporalmente o al finalizar su jornada de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- Deberán asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del fichero, cada usuario deberá retirar los documentos conforme vayan siendo impresos.
- La conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso a la información, quedan expresamente prohibidas.
- No podrán cambiar la configuración fija y sistema operativo de los equipos, salvo autorización de las personas en las que haya delegado expresamente esta autorización.

- Cada usuario será responsable de la confidencialidad de su contraseña y, en el supuesto de que ésta sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.
- Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma a rgpd@auratechlegal.es o en su caso a la dirección del centro. En este sentido, el conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad de la información por parte de dicho usuario.
- Deberán responsabilizarse de que los soportes que contengan datos personales, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, se encuentren claramente identificados con una etiqueta externa que indique de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.
- Se encargarán de que aquéllos soportes que resulten reutilizables, y que hayan contenido datos personales, sean borrados físicamente antes de su reutilización, de forma que los datos que contenía anteriormente, no sean recuperables.
- Se deberá borrar o destruir todo fichero temporal o copia de trabajo, una vez que haya dejado de ser necesario para los fines que motivaron su creación.
- En los supuestos de traslado de documentación que contenga datos personales, se deberán adoptar medidas encaminadas a evitar su pérdida o robo.
- Se ocuparán de que los soportes que contengan datos personales sean almacenados en lugares a los que no tengan acceso a personas no autorizadas para el acceso a dichos datos.
- Conservarán todos los datos en el servidor de red, quedando prohibida la conservación de información en local.
- Se compromete a cumplir con el deber de secreto en relación con la información que conozca para llevar a cabo sus funciones en la entidad, subsistiendo este deber una vez finalizada la relación en virtud de la que se ha tenido conocimiento de dicha información.

NOTIFICACIÓN DE BRECHAS O VIOLACIONES DE SEGURIDAD

Todo empleado que detecte una incidencia como las que se comunican a continuación deberá ponerlo en conocimiento de inmediato escribiendo a la dirección direcciong@fundacionescolapias.com o a rgpd@auratechlegal.es

Si bien no es posible tipificar a priori un catálogo exhaustivo de los incidentes que pueden afectar a la seguridad e integridad de los datos personales, se adjunta a modo de ejemplo, un listado orientativo de violaciones de seguridad.

1. **Incidencias que pueden afectar a la confidencialidad**

1.1.- Lectura no autorizada de la información contenida en los ficheros.

1.1.1.- Por parte de personal informático.

1.1.2.- Por parte de otras personas de la organización.

1.1.3.- Por parte de personas ajenas a la organización.

1.2.- Copia no autorizada de la información.

1.2.1.- Por parte de personal informático.

1.2.2.- Por parte de otras personas de la organización.

1.2.3.- Por parte de personas ajenas a la organización.

1.3.- Error en la distribución:

- de informes
- de soportes

1.4.- Error en la manipulación:

- de informes
- de soportes

1.5.- Obtención de información desde soportes desechados.

1.6.- Descifrado de la información:

1.6.1.- Por descubrimiento de claves.

1.6.2.- Por conocimiento directo de las claves.

2.0.- **Incidencias que afectan a la integridad:**

2.1.- Modificación no autorizada de la información:

2.1.1.- Por parte de personal de la organización.

2.1.2.- Por parte de personas ajenas a la organización.

2.2.- Borrado no autorizado de la información:

2.2.1.- Por parte de personal informático de la organización.

2.2.2.- Por parte de personas de la organización.

2.2.3.- Por parte de personas ajenas a la organización.

2.3.- Destrucción parcial o total de la información por:

2.3.1.- Fallos en equipos.

2.3.2.- Fallos en instalaciones ocasionadas por:

- Incendios
- Inundaciones
- Tormentas

2.4.- Imposibilidad de recuperar datos, partiendo de las copias de respaldo.

2.5.- Alteración o borrado de la información durante su explotación por:

2.5.1.- Fallos ocasionados por aplicaciones.

2.5.2.- Fallos ocasionados por sistemas operativos.

3.0.-Incidencias que afectan a la disponibilidad:

3.1.- Modificaciones no autorizadas de permisos de acceso lógico a los ficheros.

3.2.- Imposibilidad o limitación del uso de las instalaciones:

3.2.1.- Fenómenos meteorológicos.

3.2.2.- Huelgas, manifestaciones.

3.2.3.- Otras.

3.3.- Indisponibilidad de los sistemas:

3.3.1.- Por fallos informáticos.

4.0.-Incidencias que afectan a la autenticación:

4.1.- Suplantación del usuario autorizado por el no autorizado:

4.1.1.- Cesión de la clave.

4.1.2.- Por conocimiento de la clave de acceso.

4.1.3.- Por violación de los controles de acceso.

4.2.- Por fallos en los programas o dispositivos de control de acceso lógico.

4.3.- Por fallos en su gestión:

4.3.1.- Bajas de personas no comunicadas.

4.3.2.- Autorizaciones de acceso improcedentes.

USO ADECUADO DE LOS SISTEMAS INFORMÁTICOS

Los empleados de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL utilizarán los sistemas y los recursos informáticos que Servicios Centrales FUNDACION ESCOLAPIAS MONTAL ponga a su disposición cumpliendo con la política de usos de medios tecnológicos de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL y en todo caso con las directrices o normas internas de utilización de los mismos.

No obstante, en todo caso los empleados deben tener en cuenta lo siguiente:

- Se hará un uso de las herramientas informáticas (correo electrónico, internet, intranet, teléfono, fax, etc.) en condiciones acordes con el desempeño del puesto y con las funciones que le son propias. No se utilizarán de forma abusiva ni en beneficio propio o para actuaciones que pudieran afectar a la reputación o imagen de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

- No está permitido almacenar datos de carácter personal de los empleados en los ordenadores que Servicios Centrales FUNDACION ESCOLAPIAS MONTAL les facilite, ni en ningún otro dispositivo.

- Los programas que se utilicen en los ordenadores y sistemas informáticos de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL serán exclusivamente los que instale el departamento de IT.

- Los empleados únicamente podrán acceder a los sistemas informáticos a los que estén autorizados y con las licencias oportunas. No se instalará, utilizará o distribuirá ningún tipo de software que pudiera afectar a la seguridad de los sistemas, ni podrán hacerse copias no autorizadas o efectuar acciones que permitan la entrada de virus informáticos.

- El acceso a Internet y el correo electrónico corporativo se proporciona como instrumento de trabajo y por ello se exige un uso exclusivamente profesional.

- Las comunicaciones que se pudieran realizar a través de las herramientas informáticas no deben contener declaraciones ofensivas o difamatorias.

- Se prohíbe la divulgación o transmisión de información ilegal, sexista, abusiva, obscena, difamatoria, racista, difamatoria, pornográfica o cualquier otro tipo de información ofensiva o no autorizada por las Leyes, ya sea por cualquier tipo de medio (fotografías, textos, enlaces a páginas externas, etc.).

- Queda prohibida igualmente la publicación, transmisión, reproducción, distribución o explotación de cualquier información, material pirateado o software que contenga virus o cualquier otro componente dañino para la integridad de los sistemas informáticos o que puedan ser contrarios a los derechos de propiedad intelectual.

INTEGRIDAD DE LA INFORMACIÓN Y LA COMUNICACIÓN

Todos los registros e informes, independientemente de que sean sólo para uso interno o también para comunicación externa, deben ser correctos, completos y fiables. Esto se aplica especialmente a la contabilidad y al mantenimiento de libros contables, así como a otros informes referentes a la situación financiera de Servicios Centrales FUNDACIÓN ESCOLAPIAS MONTAL

Sólo los empleados autorizados pueden realizar comunicaciones oficiales a los medios de comunicación .

Lo anterior también se aplica a las declaraciones dadas a organismos públicos y autoridades supervisoras. Las comunicaciones con dichos órganos sólo deben llevarse a cabo a través de las personas autorizadas para ello.

Además, se deben seguir las directrices internas relativas a documentos sobre temas profesionales, seminarios, debates, y similares.

Si los empleados hacen apariciones públicas o participan en debates, de tal forma que pareciese que lo hacen en representación de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL , sin haber sido autorizados para ello, deben dejar claro que están actuando a título particular.

Todos los empleados deben desempeñar una conducta profesional íntegra en todas sus actuaciones y evitar cualquier conducta que, aun sin violar la ley, pueda perjudicar la reputación de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL y afectar de manera negativa a sus intereses y su imagen pública.

La profesionalidad es la actuación diligente, responsable, eficiente y enfocada a la excelencia, la calidad y la innovación.

La integridad es la actuación leal, honrada, de buena fe, objetiva y alineada con los intereses de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

IMPLEMENTACIÓN DE DENUNCIAS E INFRACCIONES

La dirección de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL deberá asegurarse de que sus empleados estén familiarizados con los contenidos del código y respeten las reglas y principios de conducta aplicables, de forma que el personal cumpla las reglas de conducta establecidas en el código. La dirección de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL se encargará de enviar este código ético a todos sus empleados siendo obligación del empleado abrirlo y dar contestación para confirmar que el código ha sido recibido. El departamento legal de Auratech Legal Solutions está disponible para cualquier consulta y para responder a preguntas relacionadas con este código en la dirección rgpd@auratechlegal.es

Los empleados que tengan conocimiento de una infracción significativa de la legislación o de las normas de este código, en especial en relación con casos de fraude, corrupción, malas prácticas contables u otras contravenciones equivalentes que puedan ser sancionadas según el Derecho civil o penal, deberán informar a Servicios Centrales FUNDACION ESCOLAPIAS MONTAL a través de direcciong@fundacionescolapias.com o de cualquiera de los canales de comunicación establecidos. Los informes sobre infracciones se tratarán de forma confidencial y con la discreción necesaria. Los empleados que informen acerca de posibles infracciones no se verán perjudicados en modo alguno, salvo que desde un principio fueran conocedores de que dicha información era falsa y esto pudiera ser evidente para ellos.

CONSUMO DE DROGAS Y ALCOHOL

Está prohibido el consumo de bebidas alcohólicas durante el horario de trabajo, en la medida en que su ingesta puede atentar contra la seguridad y la productividad en el entorno de trabajo y el mantenimiento de la profesionalidad y la responsabilidad de los empleados.

ACEPTACIÓN DE INCLUSIÓN EN GRUPOS DE MENSAJERIA INSTANTANEA (WHATSAPP)

Como empleado de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL se da por informado y consiente el tratamiento de sus datos de carácter personal en los siguientes términos:

El receptor de este código presta su consentimiento a Servicios Centrales FUNDACION ESCOLAPIAS MONTAL con el objeto de ser incluido en el grupo de WhatsApp (o tecnología análoga) habilitado para compartir y poder complementar información relacionada con la relación laboral , y acabando las funciones propias del mismo el día en que el empleado deje de prestar sus servicios en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

Los datos que se generen sólo estarán en el citado grupo de whastapp (o tecnología análoga)

El interesado tiene la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y supresión, así como cualesquiera que pudieran estar reconocidos en el RGPD 2016/679. Para ejercer dichos derechos será necesario dirigirse por escrito a los siguientes correos electrónicos direcciong@fundacionescolapias.com y rgpd@auratechlegal.es.

No se permite la cesión de datos de carácter personal del titular firmante, así como la publicación de contenidos que puedan atentar contra la moral, la dignidad o el respecto de cualquier persona, comprometiéndose los participantes en el mismo a dar al grupo un uso diligente y un respeto.

El plazo de conservación de los datos personales será hasta 30 días naturales después de la finalización de contrato laboral, en ese plazo el administrador eliminará al empleado que ya no esté prestando servicios en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL del grupo de whatsapp (o tecnología análoga)

CLÁUSULA INFORMATIVA MONITORIZACIÓN DE EQUIPOS

El administrador de sistemas de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL pondrá en funcionamiento herramientas de control automatizadas para analizar y detectar los usos y comportamientos indebidos o ilícitos en la red, no implicado dicho control violación a la privacidad o a la intimidad de los usuarios.

Las partes acuerdan que por cuestiones de seguridad toda la información que circula por la red, así como por el correo electrónico de las cuentas administradas por el centro, podrá ser monitoreada y sujeta a controles y reportes sobre su uso, brindando información como: usuario, fecha de accesos, hora de accesos, bytes transferidos, almacenamiento de ficheros, acceso a los servidores, sitios visitados, tiempo de navegación por la red, entre otros.

El empleado es informado de que el sistema informático será usado únicamente para fines relacionados con la actividad del centro y su trabajo en el mismo, quedando prohibido expresamente el uso del sistema informático para usos distintos de los mencionados. Asimismo, el empleado reconoce que todos los archivos, informes, correspondencia vía email, software y, en general, cualesquiera otros datos o información de cualquier tipo que hayan sido generados o se encuentren en el sistema informático son propiedad de la compañía y podrán ser usados por la misma para cualquier propósito dentro de los límites legalmente permitidos. El empleado autoriza expresamente al centro para acceder a la información referida, así como a realizar los controles que se consideren oportunos.

¿COMO SABER SI ACTÚO CORRECTAMENTE?

Como se ha expuesto al inicio del presente código de conducta, no se pueden describir todas las situaciones que pueden producirse, por lo que por tal motivo, para saber si se está actuando éticamente, ante cualquier duda o situación determinada, nos podemos preguntar lo siguiente:

- ¿Es legal?
- ¿Es lo correcto?
- ¿Va en línea con el código de conducta ?
- ¿Estoy siguiendo las políticas y manuales establecidos por la compañía?
- ¿Puede tener un impacto negativo en mi o en la reputación de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL ?

Sí ante cualquiera de las anteriores situaciones te surgeran dudas, plantea tus preguntas al correo electrónico disponible para ello rgpd@auratechlegal.es

ACEPTACIÓN DEL PRESENTE CÓDIGO DE CONDUCTA

Los empleados de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL deben conocer y desarrollar su trabajo conforme a las normas establecidas en el presente código de conducta .

El desconocimiento del código de conducta no excusará a ninguna persona de su cumplimiento.

COMPROMISO DE CUMPLIMIENTO

Mediante la puesta a disposición de este documento, el usuario reconoce haber leído y entendido todas y cada una de las políticas de tratamiento siendo consciente de su responsabilidad y obligado cumplimiento.

Madrid, 10 de junio de 2021

POLÍTICA DE SEGURIDAD
PROTECCIÓN EN EL PUESTO DE TRABAJO (v2.1)

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

1.- PROPÓSITO

La gestión de la información empresarial se realiza fundamentalmente desde el puesto de trabajo, tanto desde dispositivo digital como de forma más tradicional (papel, teléfono...). De ahí la importancia de que el empleado se conciencie y se responsabilice del cumplimiento de ciertas normas para la seguridad en, y desde, su puesto.

Por una parte, el empleado debe conocer los riesgos no tecnológicos, por ejemplo:

- información en papel al alcance de personas no autorizadas;
- la falta de confidencialidad de los medios de comunicación tradicionales;
- el peligro de robo o extravío de los dispositivos extraíbles (pendrives, discos duros externos, etc.);
- el acceso físico de terceras personas a las zonas de trabajo (repartidores, personal de limpieza, etc.).

Por otra parte, desde en muchos puestos de trabajo se tiene acceso a ordenadores, dispositivos móviles y portátiles con conexión a la red de la empresa y al exterior (internet). Son pues una «puerta de entrada» a la empresa y a sus recursos de información. Es esencial que el empleado tenga conciencia de lo que esto implica a fin de evitar incidentes que puedan iniciarse en su puesto de trabajo, acentuados por desconocimiento o por falta de preparación:

- accesos no autorizados a los ordenadores y desde ellos a aplicativos de la empresa;
- infecciones por malware;
- robo y fuga de datos en formato digital;
- ataques de ingeniería social, es decir, engaños para manipular a la víctima para obtener información (credenciales, información confidencial...) o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso, etc.).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto Servicios Centrales FUNDACION ESCOLAPIAS MONTAL ha implantado una política de protección del puesto de trabajo. A continuación, se facilita una serie de obligaciones y buenas prácticas en materia de seguridad que aplican a su puesto de trabajo, con el objetivo es garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo.

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

[SEG.01.A]	DESTRUCCIÓN AVANZADA DE DOCUMENTACIÓN
La información confidencial obsoleta o que ya no sea útil debe ser destruida de forma segura teniendo en cuenta el método apropiado para cada soporte de almacenamiento	
	La información obsoleta se destruirá de forma segura: • *mediante destructoras de papel;* • *contratando un servicio externo de destrucción segura, notificando a los empleados de su existencia y obligación de uso;*

[SEG.01.B]	BLOQUEO PROGRAMADO DE SESIÓN
Como usuario debe programar el bloqueo automático de sesión en su equipos al no detectarse actividad durante un corto periodo de tiempo (Máximo 10 minutos)	
	En caso de que como usuario no sepa configurarlo debe avisar a su responsable para que se le programe un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo. Adicionalmente se puede contemplar llevar a cabo la programación del apagado general de equipos una vez terminada la actividad empresarial.

[SEG.01.C]	SISTEMA OPERATIVO ACTUALIZADO
Se deben mantener actualizados los sistemas operativos de los equipos informáticos. En caso necesario, solicitar ayuda del personal técnico o responsable.	
	El personal responsable de los sistemas aplicará la Política de actualizaciones de software revisando los equipos periódicamente para garantizar su actualización o activando las actualizaciones automáticas. Si no se tiene personal técnico lo realizará el propio usuario consultando a su responsable.

[SEG.01.D]	ANTIVIRUS ACTUALIZADO Y ACTIVO
Se ha de mantener el antivirus actualizado y activo en todos los equipos informáticos.	
	El personal responsable de los sistemas aplicará la Política antimalware que incluya la instalación y actualización de herramientas antimalware en todos los equipos y sistemas, y su revisión periódica de manera que se garantice la protección antimalware.

[SEG.01.E]	USO DE MEDIOS DE ALMACENAMIENTO
La información debe ser almacenada en dispositivos autorizados y de forma segura. Por ejemplo, los dispositivos externos como pendrives o discos duros externos, deben ser encriptados.	
	Para que el empleado haga un uso correcto de los dispositivos de almacenamiento disponibles, debe conocer como cifrar dispositivos externos.

[SEG.01.F]	PROHIBICIÓN DE ALTERACIÓN
No está permitido alterar la configuración del equipo o instalar aplicaciones no autorizadas. Siempre debe solicitarse al personal informático la instalación de software específico o el cambio de configuración del equipo si es necesario para el desempeño del trabajo.	
	Es un riesgo que el empleado cambie la configuración del equipo o instale las aplicaciones que considere necesarias. Esta modificación podría tener consecuencias de infección de equipos y por lo tanto de pérdida de información. Si el empleado requiere una configuración o software específico para el desempeño de su trabajo, deberá solicitarlo formalmente al equipo informático o a su responsable.

[SEG.01.G]	POLÍTICA DE MESAS LIMPIAS
La mesa de trabajo debe encontrarse siempre despejada y sin documentación confidencial ni dispositivos extraíbles al alcance de otras personas.	
	Conocemos como política de mesas limpias la obligación de guardar la documentación al ausentarse del puesto de trabajo y al terminar la jornada laboral. No se debe dejar información sensible a la vista de personas que pudieran hacer un uso indebido de la misma. El cumplimiento de esta política conlleva: • *mantener el puesto de trabajo limpio y ordenado;* • *guardar la documentación y los dispositivos extraíbles que no están siendo usados en ese momento, y especialmente al ausentarnos del puesto o al fin de la jornada laboral;* • *no apuntar usuarios ni contraseñas en post-it o similares.*

[SEG.01.H]	CUSTODIA DE DOCUMENTACIÓN SENSIBLE
Se debe recoger inmediatamente aquellos documentos enviados a imprimir y guardar la información una vez escaneada, especialmente si se trata de información sensible.	
	Para evitar que la información acabe en manos no deseadas el usuario debe: • *recoger inmediatamente aquellos documentos enviados a imprimir;* • *guardar la documentación una vez escaneada;* • *utilizar los mecanismos de impresión segura si los hubiera.*

[SEG.01.I] NO REVELAR INFORMACIÓN A USUARIOS NO DEBIDAMENTE IDENTIFICADOS

Se debe identificar previa y correctamente el destinatario de los datos, teniendo en cuenta los peligros de la ingeniería social y la información que no se debe desvelar.

La información es uno de los activos empresariales más cotizados. Por este motivo es posible que alguien intente obtener parte de esta información (contraseñas de usuario, información de cuentas bancarias, etc.) engañando a un empleado. Esta práctica se conoce como ingeniería social.

Los delincuentes se hacen pasar por algún responsable, persona o empresa conocida para que el empleado se confíe y facilite la información que le solicitan empleando para ello una llamada telefónica, el correo electrónico, las redes sociales o mensajes del tipo SMS o Whatsapp.

[SEG.01.J] OBLIGACIÓN DE CONFIDENCIALIDAD

El usuario de datos debe aceptar y cumplir el código de conducta que se entrega junto a esta documentación.

El empleado debe aceptar un compromiso de confidencialidad relativo a cualquier información a la que tenga acceso durante su participación laboral en la empresa. La obligación de confidencialidad tendrá validez todo el tiempo que se haya exigido en el contrato laboral. La información debe protegerse aun cuando el empleado ya no forma parte de la empresa.

[SEG.01.K] CUSTODIA Y USO DE CONTRASEÑAS ROBUSTAS

No se deben publicar ni compartir las claves. Tampoco deben anotarse en documentos, agendas ni en cualquier otro tipo de soporte. Y deben ser dificilmente descrifrables.

El usuario debe tener presente:

- *las credenciales (usuario y contraseña) son confidenciales y no pueden ser publicadas ni compartidas;*
- *no deben anotarse las credenciales en documentos ni en cualquier otro tipo de soporte;*
- *las contraseñas deben ser robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,], ?, etc.);*
- *se deben cambiar periódicamente.*

[SEG.01.L] CAMBIO PERIÓDICO DE CONTRASEÑAS

Se deben cambiar las contraseñas al menos cada 6 meses.

Para garantizar la confidencialidad de nuestras contraseñas estas deben ser cambiadas periódicamente. La periodicidad dependerá de la criticidad de la información a la que dan acceso. No deben utilizarse contraseñas que hayan sido usadas con anterioridad. Pueden utilizarse sistemas que fuercen al cambio de contraseña en el plazo elegido.

[SEG.01.M] OBLIGACIÓN DE BLOQUEO DE SESIÓN Y APAGADO DE EQUIPO

Es obligatorio bloquear la sesión al ausentarse del puesto de trabajo y apagar el equipo al finalizar la jornada laboral.

Para evitar el acceso indebido o por personal no autorizado al equipo del puesto de trabajo:

- *el empleado deberá bloquearlo cada vez que se ausente de su puesto;*
- *el empleado apagará su equipo al finalizar la jornada laboral.*

[SEG.01.N]	NOTIFICACIÓN DE INCIDENTES
Es obligatorio notificar a rgpd@auratechlegal.es cualquier incidencia de seguridad (virus, pérdida de información o de dispositivos, etc.)	
	El empleado debe advertir de cualquier incidente relacionado con su puesto de trabajo: • *alertas de virus/malware generadas por el antivirus;* • *llamadas sospechosas recibidas pidiendo información sensible;* • *correos electrónicos que contengan virus;* • *pérdida de dispositivos móviles (portátiles, smartphones o tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.);* • *borrado accidental de información;* • *alteración accidental de datos o registros en las aplicaciones con información crítica;* • *comportamientos anómalos de los sistemas de información;* • *hallazgo de información en ubicaciones no designadas para ello;* • *evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes…);* • *evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros;* • *cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.*

POLÍTICA DE SEGURIDAD
USO DEL CORREO ELECTRÓNICO (v2.1)

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

1.- PROPÓSITO

El correo electrónico es una herramienta de comunicación imprescindible para el funcionamiento de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL. Sus beneficios son evidentes: accesibilidad, rapidez, posibilidad de enviar documentos adjuntos, etc., aunque cuando se creó, no se hizo pensando en sus aplicaciones actuales ni en la seguridad.

Como toda herramienta de comunicación corporativa es necesario definir su uso correcto y seguro, ya que, además de abusos y errores no intencionados en su uso que puedan causar perjuicio en la empresa, el correo electrónico se ha convertido en uno de los medios que utilizan los ciberdelincuentes para llevar a cabo sus ataques.

Los empleados pueden enviar documentos confidenciales a quien no deberían por error, desvelar, sin querer, la dirección del correo electrónico de clientes o usuarios, o utilizar su correo corporativo para usos no permitidos.

También es habitual que a los buzones corporativos llegue spam, correos de phishing que intentan robar credenciales o correos que suplantan entidades o personas. En estos casos utilizan técnicas de ingeniería social para conseguir sus fines maliciosos, por ejemplo: infectarnos, robar credenciales o que les demos datos confidenciales. En un correo malicioso tanto el remitente como el asunto, el cuerpo, los adjuntos o los enlaces que contiene, pueden estar diseñados para engañar al receptor del mensaje. Para evitar caer en la trampa de los ciberdelincuentes debemos además de utilizar medios tecnológicos (antivirus, antimalware, antispam, etc.), comprobar si nuestros saben identificar estos mensajes.

Para evitar los riesgos que conlleva el uso del correo corporativo debemos concienciar a nuestros empleados para que hagan un uso seguro del mismo e informarles de las normas que regulan las condiciones y circunstancias en las que puede utilizarse, así como las posibles sanciones y acciones a tomar en caso de detectarse un mal uso.

El objetivo es establecer unas normas de uso permitido y seguro del correo electrónico corporativo que sirva para impedir errores, incidentes, usos ilícitos, y ataques.

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

[SEG.02.A]	ANTIMALWARE Y ANTISPAM
Tanto el servidor como el servidor de correos debe disponer de aplicaciones antimalware y antispam instaladas y activadas.	
	Debes instalar aplicaciones antimalware y activar los filtros antispam tanto en el servidor como en el cliente de correo. Estos filtros permitirán que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada evitando asi su posible apertura. Si tiene dudas sobre si están activados debe comunicárselo a su responsable.

[SEG.02.B]	CIFRADO Y FIRMA DIGITAL
Se aconseja utilizar tecnología de cifrado y firma digital que se puede usar con el correo electrónico para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.	
	Se considera conveniente instalar una tecnología de cifrado y firma digital para proteger la información confidencial y asegurar la autenticidad de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL como remitente.

[SEG.02.C]	DESACTIVAR ELEMENTOS NO SEGUROS
Se debe desactivar el formato HTML, la ejecución de macros y la descarga de imágenes para una protección adicional de las cuentas de correo electrónico.	
	El formato HTML permite utilizar colores, negritas, enlaces, etc. También permite incluir un lenguaje de programación denominado JavaScript. Este lenguaje puede ser usado con fines ilícitos, por ejemplo, para verificar que nuestra cuenta de correo es válida o para redirigirnos a un sitio web malicioso. Por ello es más seguro tenerlo desactivado. Como seguridad complementaria también se deberían deshabilitar las macros y las descargas de imágenes.

[SEG.02.D] OFUSCAR LA DIRECCIÓN DE CORREO ELECTRÓNICO

No se deben publicar las direcciones de correo corporativas en https://fundacionescolapiasmontal.org u otras web ni en redes sociales sin utilizar técnicas de ofuscación.

No se deben publicar las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación. De lo contrario esas cuentas pueden ser captadas para incluirlas en listas de envío de spam. Técnicas que puedes utilizar:

- *crea una imagen con la dirección de correo que quieras publicar y utiliza la imagen en lugar de introducir el correo como texto;*
- *reemplazar '@' y '.' por texto; de esta forma, nombre@miempresa.com se sustituiría por nombrearrobamiempresapuntocom.*

[SEG.02.E] USO APROPIADO DEL CORREO CORPORATIVO

Nunca se debe usar el correo corporativo con fines personales y el contenido cumple las reglas marcadas por Servicios Centrales FUNDACION ESCOLAPIAS MONTAL, es decir, asuntos extrictamente profesionales.

El empleado conoce y acepta la normativa relativa al uso del correo corporativo.

[SEG.02.F] CONTRASEÑA SEGURA

Se debe usar una contraseña segura para acceder al correo.

En todas las cuentas debe utilizar contraseñas de acceso se recomienda:

- *usar una contraseña segura para evitar accesos no autorizados;*
- *utilizar doble factor de autenticación para las cuentas críticas;*
- *si se accede al correo a través desde una interfaz web nunca se marcará la opción de recordar contraseña.*

[SEG.02.G] CORREOS SOSPECHOSOS

Se debe sospechar de la autenticidad el correo cuando el mensaje: Presenta cambios de aspecto, contiene una "llamada a la acción" que urge, invita o solicita hacer algo no habitual o solicita credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).ANTE CUALQUIER DUDA NUNCA PINCHE EN LOS ENLACES O ABRA LOS ADJUNTOS.

Debe aprender a identificar correos fraudulentos y sospechar cuando:

- *el cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente;*
- *el mensaje contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual;*
- *se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.)*

[SEG.02.H] IDENTIFICACIÓN DEL REMITENTE

Se debe identificar a los remitentes antes de abrir un correo electrónico. Si se sospecha que ha sido suplantado, se debe contactar con el remitente por otro medio para confirmarlo.

Nunca abrirá un correo sin identificar el remitente. Si el remitente no es un contacto conocido habrá que prestar especial atención ya que puede tratarse de un nuevo cliente o de un correo malicioso.

Si el remitente es un contacto conocido pero por otros motivos (cuerpo del mensaje, archivos adjuntos, enlaces...) sospechas que se ha podido suplantar su identidad, debes contactar con éste por otro medio para confirmar su identidad.

[SEG.02.I] ANÁLISIS DE ADJUNTOS

Se debe analizar cuidadosamente los adjuntos de correos de remitentes desconocidos antes de abrirlos. Si se sospecha de su autenticidad, no se debe descargar ni abrir.

Al recibir un mensaje con un adjunto, este se debe analizar cuidadosamente antes de abrirlo. Aunque el remitente sea conocido puede haber sido suplantado y no apercibirnos. La descarga de adjuntos maliciosos podría infectar nuestros equipos con algún tipo de malware. Tener el antivirus activo y actualizado puede ayudarnos a identificar los archivos maliciosos. Estas son algunas medidas para identificar un adjunto malicioso:

- *tiene un nombre que nos incita a descargarlo, por ser habitual o porque creemos que tiene un contenido atractivo;*
- *el icono no corresponde con el tipo de archivo (su extensión), se suelen ocultar ficheros ejecutables bajo iconos de aplicaciones como Word, PDF, Excel, etc.;*
- *tiene una extensión familiar, pero en realidad está seguida de muchos espacios para que no veamos la extensión real (ejecutable) en nuestro explorador de ficheros, por ejemplo: listadoanual.pdf .exe;*
- *nos pide habilitar opciones deshabilitadas por defecto como el uso de macros;*
- *no reconoces la extensión del adjunto y puede que se trate de un archivo ejecutable (hay muchas extensiones con las que no estamos familiarizados);*
- *es o encubre un archivo JavaScript (archivos con extensión .js).*

[SEG.02.J] INSPECCIÓN DE ENLACES

Se deben examinar atentamente los enlaces incluidos en los correos antes de acceder a ellos.

Al recibir un mensaje con un enlace, antes de hacer clic debe:

- *revisar la URL, sitúate sobre el texto del enlace, para visualizar la dirección antes de hacer clic en él;*
- *identificar enlaces sospechosos que se parecen a enlaces legítimos fijándonos en que:*
  - *A.-pueden tener letras o caracteres de más o de menos y pasarnos desapercibidas;*
  - *B.-podrían estar utilizando homógrafos, es decir caracteres que se parecen entres sí en determinadas tipografías (1 y l, O y 0).*

[SEG.02.K] NO RESPONDER AL SPAM (CORREO BASURA)

Nunca se debe responder al corro basura. Se debe agregar a la lista de spam y eliminarlo.

Cuando recibimos correo no deseado no respondemos al mismo. De lo contrario confirmaremos que la cuenta está activa y seremos foco de futuros ataques. Agrégalo a tu lista de spam y elimínalo. Tampoco lo reenviaremos en caso de cadenas de mensajes.

NUNCA DEBEMOS DARNOS DE BAJA AL SPAM, AL PULSAR EN DARSE DE BAJA LO QUE REALMENTE HACEMOS ES CONFIRMAR QUE NUESTRA DIRECCIÓN ES CORRECTA Y ESTÁ VIVA.

[SEG.02.L] UTILIZAR LA COPIA OCULTA (BCC O CCO)

Se debe utilizar la copia oculta cuando se envía correos a múltiples direcciones.

Cuando se envíen mensajes a múltiples destinatarios, envíatelo a ti mismo y utiliza la opción de copia oculta, (CCO o BCO en la mayoría de los clientes de correo) en lugar de la copia normal CC. La copia oculta impide que los destinatarios vean a quién más ha sido enviado. De esta forma evitaremos que cualquiera pueda hacerse con unas cuantas direcciones de correo válidas a las que enviar spam o mensajes fraudulentos. Recuerda que el correo electrónico es un dato personal de nuestros clientes y usuarios, que no debemos utilizar para otros fines distintos de aquellos para los que fue solicitado. No debemos divulgarlo o comunicarlo a terceros sin su consentimiento.

[SEG.02.M] REENVÍO DE CORREOS

En caso de necesitar el reenvío de algún correo corporativo a una cuenta personal, debe solicitar autorización previa a la dirección de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.

Se informade la prohibición del reenvío de correos corporativos a cuentas personales salvo casos excepcionales que deben ser autorizados por la dirección.

[SEG.02.N]	EVITAR REDES PÚBLICAS
No debe consultar el correo corporativo si se está conectado a redes públicas como wifis de hoteles, restaurantes o aeropuertos.	
	Evitar utilizar el correo electrónico desde conexiones públicas (la wifi de una cafetería, el ordenador de un hotel, etc.) ya que nuestro tráfico de datos puede ser interceptado por cualquier usuario de esta red. Como alternativa, es preferible utilizar redes de telefonía móvil como el 4G o 5G.

[SEG.02.O]	NORMATIVA DE USO DE CORREO ELECTRÓNICO
Debe existir una normativa referente al uso del correo electrónico a disposición del empleado.	
	Servicios Centrales FUNDACION ESCOLAPIAS MONTAL dispone de un apartado en el código de conducta referente al uso del correo electrónico que el empleado acepta su puesta a disposición al incorporase a su puesto de trabajo. Se informará de la prohibición del uso del correo corporativo con fines personales que no tengan que ver con la empresa. El contenido del correo deberá cumplir con la normativa y su uso inadecuado podrá conllevar sanciones. El correo corporativo puede ser supervisado por la dirección de la empresa.

POLÍTICA DE SEGURIDAD
CONTRASEÑAS (v2.1)

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

1.- PROPÓSITO

El tratamiento diario de la información de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos la pareja de credenciales: usuario y contraseña. Por la seguridad de los servicios y sistemas en los que existen cuentas de usuarios, tenemos que garantizar que las credenciales de autenticación se generan, actualizan y revocan de forma óptima y segura.

Existen distintos mecanismos de gestión de identidades y control de accesos. Algunos están implementados en los sistemas operativos habituales, otros están disponibles a través de servicios online, como pueden ser el social login, la federación de identidades, los servicios de intermediarios de seguridad de acceso a la nube o CSAB, etc. En cualquier caso, debemos establecer un procedimiento claro para habilitar y revocar las credenciales y permisos de acceso a los distintos servicios y aplicaciones: correo electrónico, servidor de ficheros, gestor de contenidos web, CRM, ERP, etc.

En el control de accesos el nombre de usuario nos identifica y la contraseña nos autentica (con ella se comprueba que somos quienes decimos ser). Todo sistema de autenticación de usuarios se basa en la utilización de uno, o varios, de los siguientes factores:

- algo que sabes: contraseñas, preguntas personales, etc.
- algo que eres: huellas digitales, iris o retina, voz, etc.
- algo que tienes: tokens criptográficos, tarjeta de coordenadas, etc.

Como la contraseña es el más utilizado de estos factores, la gestión de las contraseñas es uno de los aspectos más importantes para asegurar nuestros sistemas de información. Las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos y servicios de nuestra empresa.

Dentro de la gestión de contraseñas se incluye el deber de difundir y hacer cumplir unas buenas prácticas: actualizarlas periódicamente, garantizar su fortaleza (dificultad para adivinarla o craquearla), no utilizar contraseñas por defecto o cómo custodiarlas.

El objetivo es establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de contraseñas.

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

[SEG.03.A]	GESTIÓN DE CONTRASEÑAS
Se debe definir un sistema de gestión de contraseñas avanzado que contemple todos los aspectos relativos a su ciclo de vida. Solicita más información a tu responsable.	

	La gestión de contraseñas es uno de los aspectos más delicados para asegurar el acceso a nuestros sistemas. Se ocupa de:
	• *Identificar los distintos equipos, servicios y aplicativos para los que es necesario activar credenciales de acceso.*
	• *Definir la manera con la que se generarán las claves, así como su formato.*
	• *Distribuir las claves generadas a los usuarios correspondientes, teniendo en cuenta:*
	  • *si esta distribución ha de ser cifrada y con qué método;*
	  • *cómo se activarán las claves.*
	• *Almacenar las claves en repositorios seguros, considerando la necesidad de realizar copias de respaldo.*
	• *Determinar quién puede acceder a estos repositorios y cómo.*
	• *Establecer el periodo de validez para cada tipo de clave.*
	• *Revocar las claves, ya sea por baja de un empleado, por considerar que una clave está comprometida por robo, etc. Además, se determinará la manera con la que las claves serán eliminadas.*
	• *Registrar:*
	  • *motivo por el que se genera una clave;*
	  • *fecha de creación;*
	  • *responsable de la custodia;*
	  • *periodo de validez;*
	  • *posibles observaciones, incidentes, etc.*

[SEG.03.B] HERRAMIENTAS PARA GARANTIZAR LA SEGURIDAD DE LAS CONTRASEÑAS

Debes ayudarte de técnicas y herramientas informáticas para garantizar la seguridad de las contraseñas. Solicita más información a tu responsable.

Para garantizar que nuestras contraseñas se generan y usan de forma robusta, podemos ayudarnos de diversas herramientas como LDAP, Active Directory o servicios externos que obligan al cumplimiento de ciertos requisitos. En todos los casos se contemplarán los aspectos más relevantes como:

- *periodos de validez para las contraseñas;*
- *posibilidad de reutilización de contraseñas ya usadas;*
- *formato de la contraseña:*
  - *longitud mínima;*
  - *tipos de caracteres que deben incluir;*
  - *cumplimiento de reglas semánticas.*
- *posibilidad de elección y modificación de la contraseña por parte del usuario;*
- *almacenamiento de las claves:*
  - *tamaño del histórico de claves a almacenar para cada usuario;*
  - *método de encriptación de las claves.*
- *número de intentos de autenticación permitidos.*

[SEG.03.C] NO UTILIZAR LAS CONTRASEÑAS POR DEFECTO

Se deben cambiar las contraseñas que vienen incluidas por defecto para el acceso a aplicaciones, equipos y sistemas.

Debes cambiar las claves por defecto, las que traen los equipos y sistemas al adquirirlos, por otras elegidas por nosotros mismos. Con esta medida evitamos el acceso no permitido, que sería posible si dejamos la contraseña por defecto por ser estas conocidas o que pueden encontrarse fácilmente en internet. Esto es especialmente importante para el acceso a la configuración de ciertos dispositivos como routers, switches, etc.

[SEG.03.D] DOBLE FACTOR PARA SERVICIOS CRÍTICOS

Se deben incorporar sistemas de autenticación multifactor en los accesos a servicios con información muy sensible.

Es recomendable implantar un sistema de autenticación de doble en el acceso a servicios que contengan información especialmente sensible o crítica. Se pueden considerar además de la contraseña otro factor como:

- *huella digital;*
- *tokens criptográficos hardware;*
- *sistemas OTP (One Time Password);*
- *tarjetas de coordenadas.*

[SEG.03.E] NO COMPARTIR LAS CONTRASEÑAS CON NADIE

Las contraseñas son unipersonales, por lo que deben mantenerse en secreto y evitar compartirlas. Si se sospecha que se ha violado la integridad de una contraseña, se debe cambiar inmediatamente.

Si compartimos nuestras contraseñas estas dejarán de ser secretas y por tanto perderán su utilidad. Debemos asegurarnos de lo siguiente:

- *no debemos compartirlas con nadie;*
- *no debemos apuntarlas en papeles o post-it;*
- *no debemos escribir nuestras contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.*

[SEG.03.F] LAS CONTRASEÑAS DEBEN SER ROBUSTAS

Se deben generar las contraseñas teniendo en cuenta su fortaleza.

Para que nuestras contraseñas sean fuertes, difíciles de adivinar o calcular, debemos cumplir las siguientes directrices:

- *deben contener al menos ocho caracteres;*
- *deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);*
- *no deben contener los siguientes tipos de palabras:*
  - *palabras sencillas en cualquier idioma (palabras de diccionarios);*
  - *nombres propios, fechas, lugares o datos de carácter personal;*
  - *palabras que estén formadas por caracteres próximos en el teclado;*
  - *palabras excesivamente cortas.*
- *tampoco utilizaremos claves formadas únicamente por elementos o palabras que puedan se públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento);*
- *se establecerán contraseñas más fuertes para el acceso a aquellos servicios o aplicaciones más críticas;*
- *se tendrá en cuenta lo expuesto en los puntos anteriores también en el caso de utilizar contraseñas de tipo passphrase (contraseña larga formada por una secuencia de palabras).*

[SEG.03.G] NO UTILIZAR LA MISMA CONTRASEÑA PARA SERVICIOS DIFERENTES

Debes asegurarte de elegir distintas contraseñas para cada uno de los servicios que se utiliza.

Nunca debes utilizar la misma contraseña para diferentes servicios. Tampoco las mismas contraseñas para uso profesional y doméstico. De esta forma evitaremos tener que cambiar todas nuestras contraseñas en el caso de que solo una haya sido comprometida.

[SEG.03.H] CAMBIO PERIÓDICO DE CONTRASEÑAS

Se deben modificar las contraseñas periódicamente, como mínimo cada 6 meses.

Para garantizar la confidencialidad de nuestras contraseñas estas deben ser cambiadas periódicamente. La periodicidad dependerá de la criticidad de la información a la que dan acceso. No deben utilizarse contraseñas que hayan sido usadas con anterioridad. Pueden utilizarse sistemas que fuercen al cambio de contraseña en el plazo elegido.

[SEG.03.I] NO HACER USO DEL RECORDATORIO DE CONTRASEÑAS

No debe utilizarse nunca las opciones de recordatorio de contraseñas de los navegadores y aplicaciones.

No es recomendable utilizar las funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personal no autorizado. Esto es especialmente frecuente en el uso de navegadores web.

[SEG.03.J] UTILIZAR GESTORES DE CONTRASEÑAS

Debe usarse gestores de contraseñas seguros para poder recordarlas, tales como KeePass, LastPass, Enpass, etc. Solicita más información a tu responsable.

Debemos considerar el uso de gestores de contraseñas en aquellos casos en los que tengamos que recordar un gran número de ellas para acceder a muchos servicios. En estos casos es muy recomendable elegir un gestor cuyo control quede bajo nuestra supervisión, que cifre las credenciales e implantar doble factor de autenticación para acceder al mismo.

[SEG.03.K]	PRECAUCIÓN AL USAR TÉCNICAS DE AUTENTICACIÓN EXTERNAS
Existen métodos de autenticación externa que pueden facilitar el registro y/o el acceso a otros servicios. Estos sistemas deben de usarse con precaución.	
	Los avances en el mundo digital posibilitan la elección de mecanismos de autenticación descentralizados que permiten el uso de contraseñas únicas para acceder a varios servicios. En ciertos casos la empresa puede plantearse el uso de alguna de estas técnicas, teniendo siempre en cuenta el riesgo que supone permitir que terceros gestionen nuestras credenciales: • ***Social-login.*** *Se basa en la utilización de identidades ya creadas en redes sociales (como Facebook, Linkedin, Google o Twitter) para registrarnos automáticamente en otros servicios.* • ***Autenticación federada.*** *Permite disponer de un único punto de autenticación para acceder a servicios de distintas compañías. Puede ser de utilidad para empresas muy integradas con proveedores y partners.* • ***Single-sign-on.*** *Se trata de un mecanismo que permite a un usuario autenticado en un servicio el acceso automático a otras muchas aplicaciones y servicios.* • ***Autenticación condicionada al dispositivo.*** *Nos permiten la autenticación a través de alguna característica del dispositivo previamente registrada en el servidor de autenticación.* • ***CSAB (Cloud Access Security Brokers).*** *Especialmente pensado para empresas que hacen uso de servicios cloud.*

POLÍTICA DE SEGURIDAD
USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS(v2.1)

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

1.- PROPÓSITO

El uso de dispositivos personales (portátiles, smartphones, tablets), propiedad del empleado, en el ámbito corporativo es lo que se conoce como BYOD (Bring Your Own Device / trae tu propio dispositivo). Se trata de una práctica muy frecuente, por lo tanto, se debe prestar una especial atención para que su uso no comprometa la seguridad de la información de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.

Existen ciertos riesgos que debemos conocer antes de permitir el uso de dispositivos personales en el ámbito corporativo:

- La exposición a redes inseguras en el ámbito personal. Este tipo de conexión podría tener como consecuencia que la información corporativa fuera accesible o pudiera ser interceptada por terceras personas no autorizadas.
- La instalación de aplicaciones que solicitan permisos para acceder a partes del dispositivo donde puede haberse almacenado información sensible, e incluso solicitar la activación de la geolocalización.
- La inexistencia de mecanismos de control de acceso a los dispositivos y la ausencia de medidas de seguridad en cuanto al almacenamiento de la información. Si alguien tuviera acceso a nuestro dispositivo no tendría ninguna dificultad a la hora de acceder o extraer información confidencial.
- La carencia de herramientas antivirus y de una normativa de actualizaciones adecuada. Actualizar las aplicaciones y disponer de un antivirus protegen al terminal de posibles ataques y accesos no autorizados.
- La opción (activada) de recordar y usar contraseñas de forma automatizada para acceder a redes, aplicaciones, sitios web, etc. Si alguien tuviera acceso al dispositivo no necesitaría disponer de las credenciales de usuario para acceder a la información.

Esta política de uso seguro de los dispositivos personales para el trabajo, debe ponerse en conocimiento de los empleados antes de que utilicen sus dispositivos para acceder a aplicaciones o tratar con información de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.

El objetivo de este documento es establecer las normas que garanticen la seguridad de la información en el uso de los dispositivos personales en el ámbito corporativo.

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.

[SEG.05.A]	NORMAS Y PROCEDIMIENTOS BYOD
Únicamente se permiten el uso de dispositivos no corporativos si disponen de antivirus y sistemas operativos actualizados, tienen configuraciones de seguridad, no tienen instalado software sin licencia y están debidamente encriptados. No obstante, se debe disponer de autorización específica por parte del personal responsable.	
	En los casos en que no se cumpla esta política no se podrá consultar el mail corporativo desde el dispositivo.

[SEG.05.B]	PROHIBICIÓN DE USO DE DISPOSITIVOS MANIPULADOS
Se prohíbe el uso de dispositivos rooteados o a los que se ha realizado jailbreak.	
	Se prohíbe el uso de dispositivos rooteados o a los que se les ha hecho jailbreak ya que permiten la instalación de aplicaciones de repositorios no oficiales.

[SEG.05.C]	CONCIENCIACIÓN DE LOS EMPLEADOS
El personal deberá estar concienciado del posible robo de sus dispositivos móviles	
	Los dispositivos como el teléfono móvil o el portátil son susceptibles de robo. Por ello es importante que los usuarios sean responsables en la protección de sus propios dispositivos y de los datos que contiene.

[SEG.05.D] FORMACIÓN DE LOS EMPLEADOS

El personal deberá de estar formado para un uso seguro de los dispositivos móviles.

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL proporciona a los empleados formación suficiente para un uso seguro de los dispositivos. Por ejemplo, han de saber:

- *Configurar los parámetros de seguridad de los dispositivos;*
- *Actualizar tanto el sistema operativo como las aplicaciones periódicamente (en especial el antivirus);*
- *No instalar aplicaciones que exijan permisos que pongan en riesgo la información confidencial (acceso a la agenda, geolocalización, etc.);*
- *Bloquear los dispositivos con contraseña y activar el bloqueo automático tras un periodo corto de inactividad;*
- *No desatender los dispositivos al viajar en transporte público.*

[SEG.05.E] LÍMITE DE ACCESO A REDES EXTERNAS

Se prohíbe el uso de redes inalámbricas externas no corporativas para el acceso a los sistemas de la entidad mediante equipos no corporativos. Solo se permiten accesos de redes 3G/4G/5G.

Los usuarios conocen que es preferible optar por la conexión de datos de su móvil 3G/4G/5G cuando las redes inalámbricas disponibles sean desconocidas. Estas redes WiFi deben considerarse inseguras.

[SEG.05.F] LISTA DE APLICACIONES NO PERMITIDAS

Antes de instalar una aplicación en un dispositivo no corporativo para el uso de los datos de la entidad, se debe solicitar autorización al personal responsable.

Existen aplicaciones que no se podrán instalar en estos dispositivos por el peligro que suponen para la información corporativa. Estas aplicaciones pueden requerir para su instalación acceso a datos confidenciales de la organización (datos de la agenda, geolocalización del terminal, etc.). Ante dudas en la revisión de las aplicaciones instaladas diríjase a su responsable o escriba a rgpd@auratechlegal.es

[SEG.05.G] CONTROL DE ALMACENAMIENTO EN LA NUBE DE LOS DATOS CORPORATIVOS

No está permitido el uso de aplicaciones de almacenamiento de datos corporativos en la nube no corporativa.

Las aplicaciones personales en los dispositivos móviles para el tratamiento de datos en la nube no son tan seguras como las empresariales por lo que hay que prestar especial atención a este intercambio de archivos. Se puede permitir la consulta de información en la nube, pero se recomienda no actualizarla desde estos dispositivos personales.

[SEG.05.H] PROCESO DE BORRADO DE LA INFORMACIÓN

Cuando un dispositivo no corporativo deja de usarse para usos corporativos o el empleado que lo usaba abandona la empresa, previamente deben formatearse para evitar la recuperación de datos.

Estableceremos el proceso a seguir para entregar/eliminar la información en estos dispositivos cuando el empleado abandone Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.

[SEG.05.I] CONTROL DE ACCESO A LA RED

Sólo está permitido el acceso a la red corporativa con equipos no corporativos mediante el uso de conexiones VPN.

El acceso a la red corporativa a través de dispositivos personales debe estar integrado en el sistema de control de accesos (autenticación, doble factor...). De esta forma el empleado debe acreditar su identidad antes de acceder a los servicios de la red corporativa. Para mayor seguridad y en caso de ser necesario Servicios Centrales FUNDACION ESCOLAPIAS MONTAL proporcionará a sus empleados acceso mediante red privada virtual (VPN) que cifra las comunicaciones.

[SEG.05.J] CONTROL DE USUARIOS Y DISPOSITIVOS

Debes asegurarte que tú y tu dispositivo está registrado en el listado de usuarios y dispositivos autorizados. Solicita información a tu supervisor.

Mantenemos un registro de usuarios y dispositivos que tienen acceso a los datos y aplicaciones de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL, detallando los privilegios de seguridad asignados para autorizar el acceso tanto a esos usuarios como a los dispositivos.

Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos. Por ejemplo:

- *Implementaremos en los dispositivos mecanismos de cifrado de la documentación además de los de autenticación de usuarios.*
- *Impediremos guardar de forma automática las credenciales de usuarios asociadas a las herramientas corporativas.*

[SEG.05.K] ENCRIPTADO DE DISPOSITIVOS

El uso de dispositivos no corporativos debe ser cifrado y las carpetas con datos corporativos protegidas con contraseñas.

Se deberá de utilizar las opciones de cifrado del dispositivo disponibles. De esta forma, los datos del dispositivo estarán inaccesibles en caso de robo.

[SEG.05.L] BLOQUEO PROGRAMADO

Se debe configurar el bloqueo automático del dispositivo no corporativo tras un periodo de inactividad.

- *Configuraremos el dispositivo para que se bloquee automáticamente tras un periodo de inactividad. Para ello, haremos uso de la funcionalidad de protecctor de pantalla del sistema operativo.*
- *Los periodos de inactividad deben ser tiempos cortos, normalmente 10 minutos.*

[SEG.05.M] EXTRAVÍO DE DISPOSITIVOS

Los dispositivos no corporativos deben ser configurados con medidas de seguridad para proteger la información corporativa (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas) en caso de extravío.

Ante la posibilidad de pérdida o extravío de este tipo de dispositivos, estableceremos las siguientes medidas:

- *Localización mediante GPS, WiFi o la información de la antena de telefonía con la que esté conectado el dispositivo. Una vez marcado como «perdido», el Smartphone empieza a enviar los datos de su ubicación de manera constante a una cuenta previamente configurada (correo, SMS, central de control...).*
- *Tener siempre activado el bloqueo de pantalla del terminal. En caso contrario se bloqueará de manera remota.*
- *Borrado remoto de datos: esta opción permite que los datos contenidos en el dispositivo se borren de manera remota, impidiendo su utilización por un usuario no legítimo.*
- *Vigilar las aplicaciones que se ejecutan. El seguimiento de las llamadas efectuadas y las redes sociales accedidas entre otros, suelen ser datos suficientes para obtener nombres, apellidos y hasta direcciones de un posible delincuente.*

[SEG.05.N] DESCONEXIÓN WIFI Y BLUETOOTH

Se debe desactivar la búsqueda de redes WiFi y de dispositivos vía Bluetooth cuando no sean necesarios.

Se desactivará en el teléfono la búsqueda de redes WiFi y de dispositivos vía Bluetooth cuando no sean necesarios.

[SEG.05.O] CUMPLIMIENTO DE LA NORMATIVA

El personal de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL deberá comprometerse y cumplir la normativa referente a uso de dispositivos móviles no corporativos

Nos aseguraremos que esta información le llega a todos los empleados y se comprometen a cumplirla antes de la incorporación de sus dispositivos personales al entorno de trabajo.

	POLÍTICA DE SEGURIDAD **APLICACIONES PERMITIDAS(v2.0)**
Servicios Centrales FUNDACION ESCOLAPIAS MONTAL	

1.- PROPÓSITO

La normativa de propiedad intelectual obliga a Servicios Centrales FUNDACION ESCOLAPIAS MONTAL a usar en todo momento software legal. El uso de software pirata o adquirido de forma fraudulenta podría conllevar sanciones económicas y penales. Además, la instalación y uso de software ilegal en algún dispositivo incrementa los riesgos de infección por malware.

Por otra parte, para evitar fugas de información y garantizar la privacidad de los datos de carácter personal, Servicios Centrales FUNDACION ESCOLAPIAS MONTAL determina y controla el software que está autorizado para el tratamiento de la información dentro de la empresa.

Cualquier incidente de seguridad puede repercutir en la imagen de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.

Para hacer cumplir esta política Servicios Centrales FUNDACION ESCOLAPIAS MONTAL cuenta con:

- un listado de software autorizado;
- un repositorio del software autorizado y un registro de licencias;
- las sanciones disciplinarias derivadas del incumplimiento de la política.

Y debe identificar a los responsables para realizar las actualizaciones del software y las auditorías.

El objetivo es controlar que siempre se usa software autorizado en la empresa, y que ha sido adquirido de forma legal.

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

[SEG.07.A]	REGISTRO DE LICENCIAS
Existe un registro actualizado de licencias disponibles del software autorizado.	
	Si queremos saber de qué software dispone Servicios Centrales FUNDACION ESCOLAPIAS MONTAL podemos consultar el registro actualizado de licencias. En dicho registro se almacenará al menos la siguiente información: • *nombre y versión del producto* • *autor* • *usuarios permitidos* • *vigencia de la licencia*

[SEG.07.B]	COMPETENCIA DE INSTALACIÓN, ACTUALIZACIÓN Y BORRADO
Únicamente el personal técnico está autorizado para encargarse de la instalación, actualización y eliminación de software en los equipos corporativos.	
	Para asegurarnos una configuración óptima en nuestros equipos sólo el personal técnico aitorizado podrá instalar, actualizar y eliminar software. En los casos en los que no se disponga de dicho personal técnico o este sea externo, se debe avisar a la gerencia o a rgpd@auratechlegal.es para revisar la operativa para instalar, actualizar, revisar y eliminar software legal de forma autónoma, para ello se deberá utilizar una cuenta de administrador diferente a la del usuario habitual. En ningún caso debe permitirse la instalación ni la actualización de software a través de enlaces de webs o correos cuyo origen no sea completamente seguro. Por último, remarcar que además de ser legal, el software instalado en los equipos debe estar correctamente actualizado.

[SEG.07.C]	SANCIONES POR USOS NO AUTORIZADOS
Servicios Centrales FUNDACION ESCOLAPIAS MONTAL pudiera establecer una política de sanciones por uso no autorizado de software. Consulta a tu responsable o a Rgpd@auratechlegal.es	
	Servicios Centrales FUNDACION ESCOLAPIAS MONTAL tiene documentadas las posibles sanciones disciplinarias por el uso de software ilegal o no autorizado. Además, se notificará la posibilidad de acarrear responsabilidad civil y penal según la legislación vigente en cada momento en materia de propiedad intelectual.

[SEG.07.D]	AUDITORÍAS DE SOFTWARE INSTALADO
El personal técnico o autorizados realizarán auditorías periódicas para analizar que el software instalado en cada uno de los equipos de los usuarios está autorizado, actualizado y tiene licencia.	
	Servicios Centrales FUNDACION ESCOLAPIAS MONTAL *debe reservarse el derecho de auditar o inspeccionar en cualquier momento los equipos de los usuarios para verificar que se cumple esta política.*

[SEG.07.E]	AUTORIZACIÓN Y LICENCIA DEL SOFTWARE
Se debe utilizar en todos los dispositivos software autorizado y que dispone de las correspondientes licencias de uso.	
	Debemos garantizar en todo momento que los programas instalados en cualquier dispositivo corporativo (se incluyen los dispositivos BYOD) están debidamente autorizados y que disponen de las licencias necesarias. Es aconsejable además que los empleados lean y comprendan los términos y condiciones de uso de dichas licencias de este modo podremos cumplir con la Ley de Propiedad Intelectual.

[SEG.07.F]	POLÍTICA DE COPIAS DE SOFTWARE
No se debe realizar copias del software puesto a disposición del empleado sin el debido consentimiento del personal responsable.	
	Para garantizar lo especificado en las licencias de uso no se permite que los empleados realicen copias del software disponible sin la debida comunicación al responsable.

POLÍTICA DE SEGURIDAD
RESPUESTA A INCIDENTES (v2.1)

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

1.- PROPÓSITO

Es un hecho que a pesar de las medidas que implantemos, siempre existe el riesgo de que ocurra un incidente de ciberseguridad. Por ello en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL hemos preparardo un plan de acción que nos indique cómo actuar de la manera más eficaz posible en estos casos.

Existen muchos tipos de incidentes de ciberseguridad, algunos son más habituales que otros que podrían encajar en una de las siguientes tipologías:

- incidentes no intencionados o involuntarios;
- daños físicos;
- incumplimiento o violación de requisitos y regulaciones legales;
- fallos en las configuraciones;
- denegación de servicio;
- acceso no autorizado, espionaje y robo de información;
- borrado o pérdida de información;
- infección por código malicioso.

Para ejecutar correctamente el plan y evitar que el daño se extienda se han detallado las acciones a realizar en cada momento, la lista de las personas involucradas y sus responsabilidades, los canales de comunicación oportunos, etc.

Tras un incidente, si hemos aplicado el plan, tendremos una valiosa información para conocer y valorar los riesgos existentes, y así evitar incidentes similares en el futuro.

En caso de que ocurran incidentes graves o desastres que paralicen nuestra actividad principal, aplicaremos el plan de contingencia y continuidad del negocio.

El objetivo es asegurarnos de que todos los miembros de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de las instalaciones de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

[SEG.14.A]	EQUIPO RESPONSABLE
En Servicios Centrales FUNDACION ESCOLAPIAS MONTAL existe un equipo abogado experto que se encarga de gestionar los incidentes de seguridad. Consulta con tu supervisor	
	Para garantizar una respuesta eficaz durante el tratamiento de incidentes de ciberseguridad, debe escribir a nuestro abogado responsable de su gestión a mdelapena@auratechlegal.es.

[SEG.14.B]	MEJORA CONTINUA
Es importante aportar toda la información posible ante los incidentes, con el objetivo de documentarlo y disponer de una mejora continua.	
	Analizaremos la utilidad de usar la información recogida en la gestión de los incidentes para medir y evaluar la posibilidad de modificar procedimientos o añadir nuevas mejoras o controles para limitar futuros daños. Podemos realizar acciones preventivas con el fin de entrenar a la plantilla ante la aparición de un posible incidente.

[SEG.14.C]	DETECCIÓN DEL INCIDENTE
Cualquier incidente debe ser comunicado inmediatamente a mdelapena@auratechlegal.es	
	Debemos concretar las situaciones que se considerarán incidentes.

[SEG.14.D]	EVALUACIÓN DEL INCIDENTE
El equipo de Auratech Legal se ocupará de gestionar el incidente, lo categorizará convenientemente y le otorgará la criticidad correspondiente.	
	Una vez detectado el incidente debemos categorizarlo convenientemente y establecer la gravedad y la prioridad en su tratamiento.

[SEG.14.E]	NOTIFICACIÓN DE INCIDENTES
El procedimiento para la notificación de un incidente es de primera mano, es decir, comunicado personalmente a mdelapena@auratechlegal.es	
	Hemos establecido un punto de contacto único donde los empleados deben notificar los posibles incidentes o puntos débiles detectados. Asimismo, se debe indicar la información a recabar y las acciones inmediatas a seguir en el momento de la notificación. Conviene tener un listado de contactos para actuar con rapidez en caso de incidente.

[SEG.14.F]	RESOLUCIÓN DE INCIDENTE
El equipo de gestión de incidentes ha desarrollado procedimientos detallados de actuación para dar respuesta a cada tipología de incidente de seguridad.	
	Hemos desarrollado y documentado procedimientos de respuesta para cada uno de los tipos de incidentes definidos previamente, poniendo especial énfasis en aquellos incidentes más habituales y peligrosos: • *recogida de evidencias tan pronto como sea posible tras la aparición del incidente, con cuidado de mantener la cadena de custodia, la integridad de las evidencias (cifrándolas si es necesario), soportes, etc.;* • *estimación del tiempo de resolución;* • *realización de un análisis forense en los supuestos requeridos;* • *escalado conveniente del incidente en caso de no poder ser solventado;* • *ejecución de acciones concretas para intentar reparar, mitigar o contener los daños causados por el incidente.*

[SEG.14.G]	TRATAMIENTO DEL REGISTRO DEL INCIDENTE
Se lleva un registro de forma conveniente de toda la información relativa a la gestión del incidente.	
	Para disponer de toda la información acerca del incidente se registrarán convenientemente, almacenándose, entre otra, la información relativa a: • *fecha y hora de aparición del incidente;* • *tipología y gravedad del mismo;* • *recursos afectados;* • *posibles orígenes;* • *estado actual del incidente;* • *acciones realizadas para solventarlo y quienes las ejecutaron;* • *fecha y hora de resolución y cierre del incidente.*

POLÍTICA DE SEGURIDAD
POLÍTICA DE TELETRABAJO (v2.1)

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

1.- PROPÓSITO

Esta política surge como respuesta a los riesgos derivados del teletrabajo, los cuales muchas veces no son tenidos en suficiente consideración.

Si bien aplica a cualquier tipo de teletrabajo, también se centra en la creciente tendencia a trabajar esporádicamente desde casa con equipos propios o a la necesidad durante periodos vacacionales de conectar con el entorno laboral, ya sea para llevar el seguimiento de tareas o proyectos, como para solventar temas urgentes cuando por la distancia no es posible trasladarse físicamente al lugar habitual de trabajo.

Se hace especial hincapié en los riesgos derivados de la utilización de dispositivos personales en el entorno corporativo (también conocido como Bring Your Own Device - BYOD), así como a usuarios que conecten de continuo desde casa o remotamente desde otras ubicaciones (como puede ser la oficina del cliente).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL, se implanta esta política de protección en teletrabajo. A continuación, se facilita una serie de obligaciones y buenas prácticas en materia de seguridad que aplican al Teletrabajo en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL, con el objetivo es garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de Teletrabajo.

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

[SEG.26.A]	MARCO NORMATIVO INTERNO
Servicios Centrales FUNDACION ESCOLAPIAS MONTAL establece un marco normativo interno con el fin de procedimentar y estandarizar el modo y las condiciones bajo las cuales la dirección desea que se desarrolle el teletrabajo.	
	Servicios Centrales FUNDACION ESCOLAPIAS MONTAL ha definido normativas y pautas que abarcan los siguientes puntos: • *Perfiles de usuarios que dispondrán de modalidad de teletrabajo y los permisos de acceso remoto de que dispondrán.* • *Servicios Centrales FUNDACION ESCOLAPIAS MONTAL tiene un procedimiento para solicitud y autorización del teletrabajo cuando no se haya regulado ya en el contrato laboral.* • *Procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales.* • *Posible utilización de equipos personales para el teletrabajo así como las medidas de seguridad aplicables a los mismos.* • *Criterios para la conexión de equipos no confiables al entorno corporativo, ya sea remota o localmente* • *Medidas de seguridad extraordinarias aplicables a los dispositivos utilizados para el teletrabajo* • *Normativas referentes al almacenamiento de información de negocio fuera de las instalaciones, ya sea en equipos de la organización, equipos personales de empleados o dispositivos extraíbles* • *Cualquier otra que se considere necesaria por Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.*

[SEG.26.B]	APROBACIÓN FORMAL POR DIRECCIÓN
Cualquier cambio en la forma de teletrabajo debería estar aprobada formalmente por la dirección.La dirección lleva un control de los empleados que utilizan esta modalidad.	
	Esta modalidad permite, entre otras ventajas, llevar un control del equipamiento que el empleado utiliza y saca de las instalaciones, permite la localización del empleado en caso de incidentes, facilita la justificación de ausencia de la oficina en caso de accidentes personales durante la jornada laboral, pero lo más importante es que permite implantar y aplicar a quien corresponda las diferentes medidas técnicas y organizativas dependiendo del perfil del usuario, la información que maneja, y los riesgos a los que está expuesto.

[SEG.26.D]	CONTROLES GENERALES
Son aquellos que Servicios Centrales FUNDACION ESCOLAPIAS MONTAL cumple para con sus empleados independientemente del tipo de trabajo, y que sin un correcto seguimiento pueden quedar sin implantar ya sea por utilizar equipos propios del empleado, por el desconocimiento o por las diferencias tecnológicas en los entornos de trabajo.	
	Algunos ejemplos serán actualizaciones automáticas de software, ejecución y actualización periódica del antivirus, tiempos de bloqueo de equipos por inactividad, control de accesos de usuarios, o similares, los cuales no siempre están correctamente configurados o tenidos en cuenta en una instalación personal o doméstica.

[SEG.26.D]	CONTROLES ADICIONALES
Aquellos de los que no siempre se dispone de forma genérica ya sea en el lugar de trabajo o en el entorno organizativo.	
	Hablamos de capas de cifrado de información, cláusulas de responsabilidad adicionales, cumplimiento de procedimientos específicos, contraseña en BIOS, software para asistencia remota y localización de equipos en caso de pérdida o robo, inventario de información del dispositivo, procedimientos de emergencia para revocar los permisos del usuario (también en caso de pérdida), o herramientas de borrado remoto de dispositivos.

[SEG.26.E]	EQUIPO Y SISTEMA OPERATIVO
Cualquier equipo que vaya a conectarse a los entornos corporativos, ya sea propiedad de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL, de sus proveedoores o del empleado, debe cumplir con unos mínimos de seguridad.	
	Entre los estándares mínimos de seguridad se encuentran: • *Instalación del sistema operativo y software desde fuente original o fiable.* • *Sistema operativo y aplicaciones actualizadas.* • *Software antivirus.* • *Cuentas de usuario sin permisos para instalar software.* • *Control de acceso robusto.* • *Configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.)* • *Bloqueo automático por inactividad* • *Software antirookits* • *Control de software original* • *Cifrado de disco (lo recgmendable sería no trabajar en local nunca).* • *Comprobación periódica de la adecuación de las salvaguardas.*

[SEG.26.F]	EQUIPOS NO CONFIABLES
Si la información a tratar en los equipos de teletrabajo es considerada importante o crítica, pero no se considera el equipo lo suficientemente confiable en los términos mencionado en el apartado anterior, es posible aplicar medidas compensatorias para conseguir niveles aceptables de seguridad y se deberá comunicar al responsable de la empresa.	
	Entre las diferentes opciones para conseguir niveles aceptables de seguridad se encuentran: • **Diferentes cuentas de usuario:** Se trata simplemente de tener diferentes cuentas de usuario en el mismo equipo donde se utilizará una para entornos confiables (teletrabajo) y otra para asuntos personales. Se recomienda almacenar la información de forma cifrada. • **Arranque dual:** Consiste en instalar en un mismo equipo dos sistemas operativos, iguales o diferentes, de los cuales cada uno se utilizará para un entorno (teletrabajo o personal). Se recomienda almacenar la información de forma cifrada. • **Distribuciones "live":** Se trata de instalaciones completas de sistemas operativos que son totalmente independientes de lo que haya en el PC ya que se cargan antes de que el sistema operativo del equipo arranque. De esta forma, se utilizaría el sistema operativo del PC para temas personales y la distribución "live" para el teletrabajo.

[SEG.26.G]	PROTECCIONES ANTIROBO
Para evitar robos de equipos portátiles suele ser suficiente tomar algunas medidas de sentido común como no dejarlo en el coche (aunque no esté a la vista), no dejarlo desatendido, evitar sacarlo de casa si no es necesario, etc.	
	Además, pueden adquirirse candados de seguridad para portátiles, lo cuales sirven para anclar el dispositivo a algún elemento del mobiliario, aunque bien es cierto que no son extremadamente robustos y según su calidad pueden romperse con herramientas simples. *Su utilidad está más enfocada a proteger el equipo del robo fácil por descuido que no de una intrusión en casa o en la oficina.* *Otra solución pasa por adquirir un armario de seguridad donde almacenar el equipo y otros artículos de relativo valor, los cuales evitarán que ante una "intrusión relámpago" en el domicilio se sustraiga el equipo de trabajo.*

[SEG.26.H]	BORRADO REMOTO
Se han implementado aplicaciones tanto para dispositivos móviles como para PC que permiten administrar remotamente los dispositivos extraviado o robados.	
	Entre las funcionalidades típicas de estos programas se encuentran: • *Activar el GPS del dispositivo (si lo tiene) para intentar localizarlo.* • *Lo anterior podría permitir hacer un borrado completo del equipo si no va a ser posible recuperarlo.* • *Instalar aplicaciones que permitan acceder remotamente al equipo para recuperar datos necesarios antes de borrar el disco, monitorizar el uso que se está haciendo del equipo, o incluso activar la webcam para intentar averiguar la identidad del ladrón.* • *Cabe recordar que estas aplicaciones evidentemente deben instalarse antes de que el dispositivo se extravíe ya que por lo general después será demasiado tarde.*

[SEG.26.I] DAÑOS FISICOS

Se implementan mecanismos para evitar el daño físico:

- *Para el transporte entre la oficina y el lugar de teletrabajo es necesario disponer de una **funda o maletín que ofrezca buena resistencia** a caídas, golpes, aplastamiento o incluso líquidos.*
- *Se debe prestar **atención al cableado**. El no estar en la oficina no significa que se puede tener todo desastrado. Un correcto cableado evitará tropiezos que acabarían con el dispositivo e incluso lo que es peor, un accidente laboral.*
- ***Guardar el dispositivo en lugar seguro** mientras no se utiliza. Aunque no es frecuente tener intrusiones en el lugar de teletrabajo, existen otros peligros con los que no contamos en la oficina: mascotas subiendo a las mesas, niños pequeños intentando alcanzar cualquier cosa de la mesa, o sobrinos en busca de algo conectado a internet para consultar una red social. Si no se está utilizando lo más recomendable es retirarlo.*
- *Considerar **cambiar el disco duro** por un SSD. Los discos duros tradicionales funcionan mediante agujas que leen los datos y que nunca deben tocar los discos que giran a gran velocidad. Cualquier vibración o caída en un momento delicado puede conllevar una pérdida total de los datos. Los discos SSD no disponen de partes móviles y son mucho más resistentes. Además, son más rápidos, ligeros y reducen el consumo de recursos.*

[SEG.26.J] TABLETS Y SMARTPHONES

Los dispositivos móviles no se limitan a leer documentos ofimáticos. También se utilizan para recibir correos electrónicos, atender llamadas de trabajo, almacenar información corporativa, tener acceso remoto a documentos en la nube, o incluso tener conversaciones por mensajería instantánea sobre temas laborales.

Entre los consejos más recomendados, se encuentran los siguientes:

- *Limitar el acceso al dispositivo mediante un bloqueo con contraseña, patrón o similar.*
- *Cifrar la memoria del dispositivo o caso de contener información sensible.*
- *Disponer de medidas para localizar el dispositivo o hacer un borrado remoto del dispositivo en caso de pérdida o robo.*
- *Disponer de algún mecanismo lo más automatizado posible para hacer copias de seguridad de la información del dispositivo.*
- *Tomar medidas para prevenir y detectar malware en los dispositivos móviles.*
- *No se deben deshabilitar las medidas de seguridad de las que disponen los dispositivos. Esto incluye, conseguir permisos de administrador, o permitir instalar software de fuentes no fiables.*
- *Instalar siempre las últimas actualizaciones de seguridad de los programas y sistemas operativos.*
- *Desactivar las conexiones inalámbricas que no se utilicen como Bluetooth, Wifi o NFC.*

[SEG.26.K] DISPOSITIVOS BYODS

Si se permite la utilización de dispositivos personales (ordenadores, smartphone, tables, etc. propios del trabajador) Servicios Centrales FUNDACION ESCOLAPIAS MONTAL tiene implementado una política de BYOD para tomar una serie de medidas de seguridad técnicas y organizativas.

- *Si usted puede utilizar equipos personales para el despeño laboral se le habrá entregado también para su aceptación la política 10.05 Uso de dispositivos no corporativos.*

[SEG.26.L] COMUNICACIONES

Se ha establecido una correcta configuración de la estructura de comunicaciones entre los empleados en teletrabajo y Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

Estas son las principales consideraciones a tener en cuenta a la hora de utilizar una conexión a internet para conectar con los recursos corporativos:

- *No utilizar conexiones poco confiables (Wifi abiertas, redes públicas de hoteles, bibliotecas, locutorios, etc.) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por httpS. No basta con tener contraseña para conectar.*
- *Si es posible se recomienda utilizar conexiones 4G o 5G los cuales son bastante más seguras que las redes inalámbricas ajenas.*
- *La administración de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL lleva un seguimiento de las conexiones remotas a los servicios corporativos de teletrabajo, especialmente se presta atención a los intentos de conexión sospechosos.*
- *Se evitarán las soluciones de administración remota gestionadas por terceros como pueden ser LogMeIn o TeamViewer ya que se evaden por completo de cualquier arquitectura de seguridad implantada, además de delegar el acceso a los sistemas a terceros externos a Servicios Centrales FUNDACION ESCOLAPIAS MONTAL.*

[SEG.26.M] VPN (Virtual Private Network)

Estas redes hacen que usted pueda conectarse de forma segura, para ti y para Servicios Centrales FUNDACION ESCOLAPIAS MONTAL, a servicio o servidores que no se encuentran directamente accesibles a Internet.

Entre las ventajas de usar este tipo de conexiones VPN se encuentran:

- *El uso de sistemas de certificados digitales que permiten que el usuario tenga la certeza de que se está comunicando con las aplicaciones correctas (no es posible que le falsifiquen las direcciones de las empresas)*
- *Asegura que todo lo que se envíe y reciba está cifrado y a salvo de intercepciones o robos de información.*
- *Estas redes permiten trabajar desde casa como si fuese desde la propia oficina, teniendo acceso a todos los recursos internos que sean necesarios, pudiendo utilizar programas internos, clientes de correo electrónico, e incluso llegar a imprimir remotamente.*
- *Su uso es relativamente sencillo pues, una vez hecha la configuración inicial, bastará con arrancar un programa e introducir la contraseña para que todo quede configurado.*
- *Facilita la robusted y seguridad ya que pueden configurarse para que utilicen autenticación fuerte de doble factor.*

[SEG.26.N] HERRAMIENTAS DE ADMINISTRACIÓN REMOTA

Se determinará en qué casos está permitida la conexión remota y en cuales no, además de cúales son los procedimientos oficiales y las aplicaciones permitidas para dicho propósito en los casos en que la VPN no esté disponible.

- *En estos casos, la dirección de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL valorará la manera de hacer la conexión y se lo comunica a cada empleado en función del perfil .*
- *Al instalar este tipo de aplicaciones en realidad se está abriendo una puerta trasera al equipo y a la red interna de la organización, que tira por tierra muchas de las medidas de seguridad implantadas, como puede ser el filtrado de conexiones mediante cortafuegos, control de conexiones desde VPN, revisiones de usuarios con teletrabajo, robustez de contraseñas, etc., permitiendo que un atacante pueda probar contraseñas directamente contra un servicio web gestionado por un tercero y sobre el que tenemos poco control.*
- *Además de lo anterior, cabría la posibilidad de que los empleados de estas compañías (LogMeIn, TeamViewer, etc.) pudieran conectarse a los equipos sin permiso, o incluso una intrusión en sus sistemas daría acceso a todos los equipos clientes, por lo que no son soluciones aconsejables.*

[SEG.26.Ñ]	COPIAS DE SEGURIDAD
En el teletrabajo no siempre se siguen las mejores prácticas en lo referente a las copias de seguridad de la información. Se debe ser consciente de que cualquier información que se saca de las instalaciones, especialmente en equipo portátiles, corre peligro de ser robada junto con el dispositivo, sufrir accidente doméstico que inutilice el acceso que se pierda por una subida de tensión en el lugar de teletrabajo.	
	El cómo operar dependerá principalmente de la modalidad de teletrabajo: • **Escritorios remotos:** Este viene a ser el único caso donde generalmente se gestionan correctamente las copias de seguridad de los datos del usuario ya que éste conecta directamente contra un servidor del entorno corporativo del cual se hacen copias de seguridad completas. • ***Perfil móvil, o sincronización automática:*** *En estos casos periódicamente se sincroniza de forma automática el contenido del PC del usuario con el entrono corporativo.* • ***Sincronización manual:*** *No es otra cosa que copiar periódicamente los ficheros actualizados contra algún servidor de la plataforma corporativa. Los principales problemas de esta solución son que no se hagan las copias con la frecuencia establecida por dejadez, o que la criticidad de la información y su volumen no hagan viable el hacer sincronizaciones manuales.* • ***Copias de seguridad offline:*** *Para este tipo de copias se recomienda utilizar un dispositivo externo con el fin de evitar un fallo físico, o que algún tipo de código malicioso corrompa la información almacenada en todo el equipo. Debería tenerse en cuenta también la posible necesidad de cifrar el soporte donde se almacenen las copias, almacenar el dispositivo bajo llave, o guardarlo en un lugar a salvo de peligros domésticos (fuego, agua, hijos pequeños, etc.)*

[SEG.26.O]	GESTIÓN Y TRASLADO DE CONTRASEÑAS
El robo de contraseñas en entornos de teletrabajo puede ser especialmente crítico ya que con una contraseña se podría acceder remotamente a los sistemas.	

	• *En caso de disponer de una conexión VPN que dé acceso a todos los demás servicios, se debe custodiar con extremo cuidado esta contraseña y seguir las mejores prácticas posibles: caducidad, complejidad, bloqueo por intentos fallidos, bloqueo por inactividad, revisiones de acceso, etc.*
	• *Si se trata de diferentes servicios (generalmente web) de los cuales cada uno dispone de una contraseña diferente la situación se complica ya que nunca se debe utilizar una única contraseña para todo.*
	• *Para poder mantener las diferentes contraseñas y garantizar que no se van a olvidar, es muy recomendable almacenarlas en un gestor de contraseñas, el cual garantizará que están a salvo de robos además de permitir transportarlas, por ejemplo, en una memoria USB o incluso online en caso de necesitar movilidad.*
	• *Algunos de los gestores de contraseñas más utilizados son:*
	  • *Keepass (http://keepass.info)*
	  • *Teampass (http://teampass.net)*
	  • *OnePassword (https://agilebits.com/onepassword)*
	  • *1Password (https://1password.com/)*
	  • *LastPass (https://www.lastpass.com/es)*
	  • *Dashlane (https://www.dashlane.com/es)*
	  • *Enpass (https://www.enpass.io/)*
	  • *Keeper (https://keepersecurity.com/es_ES/)*
	  • *Bitwarden (https://bitwarden.com/)*
	  • *PasswordSafe (https://pwsafe.org/)*
	  • *Roboform (https://www.roboform.com/)*

[SEG.26.P] CIFRADO DEL DISCO DURO Y SOPORTES

Proteger la información que se almacena fuera de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL será una de las mayores prioridades de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL a la hora de disponer de trabajadores en modalidad de teletrabajo, porque el robo o pérdida de un dispositivo portátil es algo que puede ocurrir con relativa facilidad. Es por ello que cifra la información

Existen diferentes soluciones de cifrado:

- ***Cifrar una carpeta o el disco completo mediante el propio sistema operativo:*** *Los principales sistemas operativos disponen de herramientas de cifrado, ya sea para cifrar las carpetas personales del usuario llegando algunos incluso a permitir cifrar todo el disco duro.*
- ***Crear un volumen de cifrado:*** *Existen herramientas que permiten, en lugar de cifrar una carpeta o un disco duro, crear un único fichero que contendrá la información cifrada.*

[SEG.26.Q] PAPEL

En entornos de teletrabajo la información en papel es menos susceptible de sufrir ataques deliberados (siempre y cuando no haya un trasiego habitual de documentación), pero el no estar en un ambiente laboral puede hacer que documentación relevante acabe junto con el papel y cartón para reciclar, se utilice para dibujar por detrás o que sufra algún accidente doméstico como que se derramen bebidas sobre él.

Es por ello que se deben tomar una serie de medidas de sentido común muy similares a las que se siguen en la oficina:

- *Almacenar los documentos en lugar seguro mientras no se estén utilizando. Las medidas de seguridad se establecerán en base a los requisitos que su clasificación marque.*
- *Se tomarán medidas de seguridad que se consideren oportunas para el transporte de la documentación, las cuales pueden ir desde no dejar la documentación desatendida, hasta utilizar contenedores especialmente preparados para ello.*
- *Se debe estudiar a fondo el método de destruir la información en papel evitando tirarla directamente al contenedor de reciclaje (habitual en la mayoría de hogares), o peor aún, que se reutilice para labores domésticas (dibujar por detrás, hacer la lista de la compra, etc.)*
- *Se deben aplicar el resto de buenas prácticas en cuanto a la gestión del papel, como pueden ser no dejar copias impresas desatendidas en la bandeja de la impresora.*

[SEG.26.R] SISTEMAS DE ALMACENAMIENTO ONLINE

El almacenamiento de datos en sistemas online conlleva una serie de riesgos que deben delimitarse y que Servicios Centrales FUNDACION ESCOLAPIAS MONTAL ha revisado.

Se han valorado:

- *El nivel de seguridad de la información que se vaya a cargar en este tipo de servicios online ya que ante un ataque a la plataforma sería posible acceder a toda la información del usuario.*
- *Dependiendo de la criticidad de la información puede ser necesario tomar medidas adicionales como el cifrado previo de la información, o el uso de medidas de protección de la propia plataforma, generalmente de pago, que aporten capas adicionales de seguridad.*
- *También existen plugins y complementos que se encargan de cifrar la información de estos servicios online, pero dependiendo de la aplicación, una vez más pasamos a delegar la seguridad de los datos en un tercero, por lo que la situación final no siempre es un incremento de la seguridad.*
- *Se debe considerar que, dependiendo de la naturaleza de los datos, se puede incurrir en el incumplimiento de normativas y leyes de protección de datos ya que en muchas ocasiones estos servicios se alojan en grupos de servidores repartidos por todo el planeta por lo que es muy difícil saber dónde está realmente la información, así como saber qué legislación le aplica.*
- *Tampoco deben descuidarse otros temas como los contratos de prestación de servicio que ofrecen estas plataformas ya que no siempre se comprometen a garantizar la disponibilidad de la información, pudiendo tener fallos técnicos que les dejen sin conectividad durante días, o pudiendo llegar al extremo de cerrar de un día para otro (o ser confiscados los servidores, como ya le sucedió a Megaupload) dejando al usuario sin posibilidad de recuperar sus datos.*

[SEG.26.S] CONCIENCIACIÓN Y FORMACIÓN DEL USUARIO DE TELETRABAJO

Como eslabón más débil en la cadena de seguridad, el usuario es el que más expuesto está a los riesgos tecnológicos, pudiendo ser víctima de ataques de ingeniería social (engaños), robos, agresiones físicas, extorsión, etc.

Por desgracia, existen pocas medidas de seguridad que aplicar sobre las personas más allá del sentido común y la formación, por lo que es precisamente en estos puntos donde más esfuerzos debe invertir.

Cualquier usuario que realice su actividad mediante teletrabajo debe estar familiarizado con todos los conceptos que aparecen en esta política, debe entender los riesgos a los que se enfrenta por no utilizar una arquitectura tradicional, y se le debe informar de las responsabilidades adicionales con respecto a la información y servicios de que disponga en comparación con un puesto de trabajo presencial. Si tiene cualquier duda o consulta puede acudir a su responsable o escribir a mdelapena@auratechlegal.es.

[SEG.26.T] ENGAÑOS MEDIANTE INGENIERIA SOCIAL

Se conocen como ataques de ingeniería social aquellos que tratan de conseguir información mediante engaños a los usuarios.

- Los ataques de ingeniería social más frecuentes son: Correos electrónicos o llamadas telefónicas suplantando a algún compañero, proveedor o cliente y solicitando cualquier tipo de información, o llegando incluso a suplantar al soporte técnico y pedir al usuario que ejecute comandos en su equipo o que comparta las contraseñas de acceso.
- Para evitar este tipo de ataques se forma a los empleados para que sepan en todo momento la información que pueden dar por teléfono y la que no, como por ejemplo configuraciones de red, contraseñas o ficheros con información sensible.
- Por otro lado, se debería establecer un protocolo para identificar al interlocutor en las llamadas telefónicas que vayan a requerir intercambiar información sensible, especialmente si los usuarios no se conocen. Puede ser algo tan sencillo como disponer de un listado de número de teléfonos autorizados, intercambiar verbalmente contraseñas pre-pactadas mediante métodos seguros, o sencillamente ser el propio usuario que haga la llamada hacia la sede de la organización y que sea la centralita quien redirija las conversaciones.
- Cabe destacar que este tipo de ataques pueden llegar a ser muy elaborados pudiendo desde crearse perfiles falsos en redes sociales profesionales como Linkedin y hacerse pasar por alguien de la empresa, hasta llegar a entablar una relación amistosa en redes más generalistas para, con el tiempo, obtener información sensible.

[SEG.26.U] AL FINALIZAR EL TRABAJO

En un entorno de teletrabajo donde es posible que el equipo se pierda, lo utilicen otros miembros de la familia, o incluso se utilize un equipo que no es del propio usuario (jamás se debería trabajar desde un cibercafé u ordenador de un hotel/aeropuerto,), Se recomienda ante situaciones como las descritas se le comunique al responsable de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL Nunca debemos olvidar seguir los siguientes consejos para proteger adecuadamente la información y las comunicaciones.

Aunque algunos puedan parecer excesivos, se deberán aplicar según la criticidad del equipo :

- *Cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción "desconectar" o "cerrar sesión".*
- *Eliminar información temporal prestando especial atención a la carpeta de descargas, papelera de reciclaje, o posibles carpetas perdidas que se dejen en "Mis documentos".*
- *Utilizar herramientas de borrado seguro para eliminar los ficheros en caso de información sensible o especialmente confidencial.*
- *Si se han utilizado certificados digitales, estos deben ser borrados de forma segura.*
- *Asegurarse de retirar cualquier memoria USB, CD o DVD que se haya utilizado en el quipo.*
- *Borrar el histórico de navegación, así como las cookies, y otros datos del navegador web, prestando especial atención a las contraseñas recordadas.*

POLÍTICA CUMPLIMIENTO NORMATIVO

[VID.01] VIDEOVIGILANCIA (v2.1)

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

1.- PROPÓSITO

El uso de cámaras de Video Vigilancia se está extendiendo de forma notable en los últimos años con el objetivo de garantizar la seguridad de las personas y la seguridad de los bienes. No cabe duda, que el uso de cámaras de Video Vigilancia ofrece unas óptimas garantías de seguridad para aquel que las utilice. Sin embargo, se ha de tener presente que la grabación de imágenes supone en la mayoría de casos grabación de personas, por lo que el uso de cámaras de Video Vigilancia constituye un tratamiento de datos personales (la imagen es un dato personal), lo que hace que dicha grabación este dentro del ámbito del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales su Instrucción 1/2006 de Video Vigilancia.

La Organización que hace uso de estos sistemas de Video Vigilancia ha de ser consciente de que esta tecnología supone asimismo una fuerte intrusión a la privacidad e intimidad de las personas, por lo que se establece un choque entre la Seguridad y la Intimidad.

El objetivo de esta política es mantener un justo equilibrio entre estos dos derechos se ha procedido ha realizar una política de uso de cámaras de Video Vigilancia con el objeto de minimizar al máximo la intrusión a la intimidad de estos sistemas de Video Vigilancia

2.- ALCANCE

La presente política es aplicable a:

- Todos los USUARIOS que intervengan en los sistemas de procesamiento de datos personales de la organización Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

[VID.01.A]	PRINCIPIO DE PROPORCIONALIDAD
la instalación de las cámaras en Servicios Centrales FUNDACION ESCOLAPIAS MONTAL es proporcional, es decir, adecuado, pertinente y no excesivo con el objetivo que se persigue con la Videovigilancia de tal forma que no ataca al derecho a la intimidad.	
	Las cámaras se instalarán únicamente en aquellas zonas que necesite cumplir con el objetivo de seguridad (zonas como los accesos a las instalaciones, zonas sensibles de agresiones a la seguridad, etc.). Queda prohibida la instalación de cámaras de seguridad en zonas donde el derecho a la intimidad se hace más patente como zonas de descanso, baños, vestuarios, etc.
	Si se utilizan cámaras orientables y/o con zoom será necesaria la instalación de máscaras de privacidad para evitar captar imágenes de la vía pública, terrenos, viviendas o cualquier otro espacio ajeno

[VID.01.B]	PRINCIPIO DE INFORMACIÓN
Los carteles con distintivos informativos de videovigilancia son claramente visibles, tanto en espacios abiertos como cerrados.	
	El hecho de que los carteles de videovigilancia estén visibles no implica que estos deban estar ubicados necesiariamente en las mismas localizaciones que las cámaras.
	Es súmamente importante que los carteles de videovigilancia están colocados en lugares estratégicos de modo que son visibles y permiten advertir de la zona videovigilanda ANTES de que el individuo es captado por las cámaras de videovigilancia.

[VID.01.C]	EXISTENCIA DE IMPRESOS INFORMATIVOS
Tenemos a disposición de los interesados suficientes impresos en los que se detalla la información prevista en los artículos, 12 y 13 del Reglamento General de Protección de Datos. Deben solcitarlo a rgpd@auratechlegal.es	
	__Artículo 12__. Respecto a las posibles personas objeto de videovigilancia se debe: • *Informar de forma concisa, transparente, inteligible y de fácil acceso* • *Facilitar el ejercicio de los derechos que le amparan* • *Atender las solicitudes de ejercicio de derechos en un plazo máximo de 30 días* • *Informar al interesado que ejerce sus derechos incluso si no se disponen de imágenes suyas.* • *Se podrá solicitar una fotografía reciente para identificar al individuo en las imágnes de videovigilancia* • *Informar mediante carteles distintivos de videovigilancia*
	__Artículo 13__. Se debe informar al interesado de: • *La identidad y los dtos de contacto del responsable de la videovigilancia* • *Los datos de contacto del Delegado de Protección de Datos, si lo hubiere* • *Los fines del tratamientos a que se destinan los datos captados por los sistemas de videovigilancia y las bases jurídicas que legitiman el tratamiento de las imágenes captadas.* • *Si la base jurídica sea "interés legítimo del resoposable del tratamiento", se deberán detallar dichos intereses legítimos.* • *Los posibles destinatarios o categorías de destinatarios a los que se comunican las imágenes de videovigilancia.* *Además de lo anterior, se deberá informar de:* • *El plazo de conservación de las imágenes (no superior a un mes) o los criterios utilizados para determinar dicho plazo* • *Los derechos que asisten al interesado (persona captada por los sistemas de videovigilancia)* • *Derecho del interesado a presentar una reclamación ante la AEPD en caso de que considere que el tratamiento no es conforme a lo establecido en el RGPD.* • *Si se realizara o estuviese prevista la realización de decisiones automatizadas o elaboración de perfiles, se debe informar previamente al interesado.*

[VID.01.D]	CONTROL DE ACCESO FÍSICO
Los sistemas de videovigilancia se ubican en un lugar vigilado y de acceso restringido, considerando las siguientes directrices.	

[VID.01.E]	CONTROL DE ACCESO LÓGICO
El acceso a las imágenes de grabación del sistema de videovigilancia será restringido a personal autorizado.	
	Únicamente tienen acceso a las imágenes personal autorizado específicamente para ello y el personal de servicio de vigilancia de la organización si estuviera contratado. Dicho personal deberá garantizar la confidencialidad de las imágenes capturadas.
	Se prohíbe la ubicación de pantallas donde se puedan visualizar las imágenes de los sistemas de grabación en lugares donde puedan ser visualizadas por personal interno o externo no autorizado.
	Las imágenes que queden registradas en los soportes de grabación únicamente serán visionadas en el monitor si previamente se hubiese recibido constancia de alguna agresión a la seguridad, como robo, acceso indebido por la noche, etc. no pudiendo ser utilizada con ninguna otra finalidad, que no esté legitimada.

[VID.01.F]	AUDIO
Las videograbaciones no registrarán conversaciones de audio privadas.	

[VID.01.G]	PLAZO DE CONSERVACION
Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación	
	Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten contra la integridad de fisica de personas o bienes de las instalaciones.

[VID.01.H]	CONTROL LABORAL

Su imagen será captada mediante las cámaras de Videovigilancia sitas en en PLAZA DE SANTA PAULA MONTAL, 3. 28044, Madrid (Madrid), España **las instalaciones propias de** Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

Las finalidades principales de estas grabaciones son:

1. **Garantizar la seguridad y protección de las personas y los bienes de la empresa** Servicios Centrales FUNDACION ESCOLAPIAS MONTAL
2. **Basándonos en el art. 20.3 del Estatuto de los Trabajadores, realizar un control laboral de los empleados de la empresa** Servicios Centrales FUNDACION ESCOLAPIAS MONTAL **al proclamar que el gerente de la mencionada empresa desea adoptar esta medida de videovigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales,**

La administración de Servicios Centrales FUNDACION ESCOLAPIAS MONTAL **está facultada para poder revisar las grabaciones captadas por las cámaras en cualquier momento de la jornada laboral. Dichas grabaciones se conservarán en poder de la administración de la empresa durante un periodo de cómo máximo 30 días salvo que se haya producido algún incidente y las grabaciones hayan sido puestas a disposición de la autoridad judicial competente o de los cuerpos y fuerzas de seguridad del estado.**

[VID.01.I]	EJERCICIO DE DERECHOS
Se garantiza el ejercicio de los derechos de acceso de los interesados a las videograbaciones.	
	Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.
	No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

CÓDIGO CONDUCTA COMPLIANCE

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

¿QUE ES EL COMPLIANCE?

El ***COMPLIANCE*** es un "conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos".

En la reforma del Código Penal de 2015 se destacaba especialmente la regulación de la posibilidad de exoneración de responsabilidad penal de la persona jurídica por la existencia previa de "un modelo de organización y gestión que incluya las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza (del que se haya producido) o para reducir de forma significativa el riesgo de su comisión".

Aun cuando puede resultar cierto que el nivel de riesgo de nuestros centros a incurrir en una responsabilidad penal puede ser bajo, esto no debe llevarnos a la relajación, porque hay determinados tipos que efectivamente podrían producirse dadas las actividades habituales en un centro, y además del riesgo penal, debe valorarse también el riesgo reputacional y la afectación a la imagen del centro o de su titularidad. La mera posibilidad de que pueda darse un supuesto de responsabilidad penal, hace recomendable realizar el esfuerzo de tener un modelo de prevención y cumplimiento.

MAPA DE RIESGOS

Este análisis, parte de un marco de Escuelas Católicas, se ciñe a los centros y a las actividades educativas de las diferentes instituciones. En nuestro caso el borrador lo realizaron las Directoras Generales de las tres Fundaciones, luego pasó a trabajarlo y la redacción definitiva el Equipo Institucional (las mismas, más la madre General y Provincial) y ha sido aprobado por el patronato de la Fundación Escolapia Montal, en la reunión del 22 de junio de 2020.

PROPUESTA DE MAPA DE RIESGOS FUNDACIONES ESCOLAPIAS DE ESPAÑA

El análisis de probabilidad de riesgos se va a estructurar en los siguientes niveles, ordenados de menor a mayor en función de las posibilidades de que ocurran:

GRADO 1	GRADO 2	GRADO 3	GRADO 4	GRADO 5
Probabilidad mínima	Hay alguna probabilidad	Puede ocurrir	Es bastante probable	Casi seguro que ocurre

DELITOS POR BLOQUES	EJEMPLOS O CASOS	PROBABILIDAD	CONSECUENCIAS
Delitos relativos a la prostitución y corrupción de menores	Abuso	Grado 2, alguna probabilidad	Graves
	Acoso	Grado 2, alguna probabilidad	Graves
	Difusión pornografía infantil	Grado 1, poca probabilidad	Graves
Delitos contra la intimidad y el allanamiento informático	Castigos que transgredan los derechos del menor	Grado 1, poca probabilidad	Grave
	Difusión de teléfonos o mails	Grado 4, bastante probable	Graves
	Difusión de datos bancarios	Grado 4, bastante probable	Graves
	Difusión de imágenes	Grado 4, bastante probable	Graves
Estafas y fraudes	Falsificación documental para conseguir beneficio.	Grado 2, alguna probabilidad	Graves
Insolvencias punibles	Doble contabilidad	Grado 2, alguna probabilidad	Graves
	Incumplimiento de régimen de concierto	Grado 1, poco probable	Graves

DELITOS POR BLOQUES	EJEMPLOS O CASOS	PROBABILIDAD	CONSECUENCIAS
Daños Informáticos	Introducción de virus o datos falsos en el sistema informático	Grado 3, bastante probable	Leves
	Suplantación de identidad informática	Grado 3, bastante probable	Leves
	Apropiación de contraseñas	Grado 3, bastante probable	Leves
	Entrar en wifis privadas	Grado 3, bastante probable	Leves
Delitos contra la propiedad intelectual…	Copiar trabajos de otras personas sin autorización.	Grado 4, muy probable	Leves
	Piratear programas	Grado 4, muy probable	Leves
	Uso de materiales protegidos (PI)	Grado 3, bastante probable	Leves o graves
Delitos contra la Hacienda pública y la SS	Eludir pagos de tributos, o cuotas de SS de los trabajadores	Grado 1, poco probable	Graves
	Obtener subvenciones falsificando datos de solicitud	Grado 1, poco probable	Graves
	Malversación de fondos públicos	Grado 1, poco probable	Graves
Delito de Prevención de Riesgos laborales	Incumplir la Normativa al respecto.	Grado 3, bastante probable	Muy graves
	Contratación de espacios y servicios sin cumplir normativa	Grado 3, bastante probable	Graves
Delitos contra trabajadores extranjeros	Recibir servicios sin contrato legal	Grado 2, probable	Graves
Delitos de construcción o edificación ilegal	Edificar sin la licencia correspondiente.	Grado 2, probable	Leves
Delitos contra el medio ambiente	Emisiones o vertidos de sustancias altamente contaminantes.	Grado 2, probable	Leves
Delitos contra la salud pública	Trapicheo, tráfico y consumo de drogas	Grado 2, probable	Leves
	Administración de medicamentos sin autorización	Grado 1, poco probable	Leves
	Intoxicación en el comedor por alimentos o agua	Grado 1, poco probable	Graves
	Intoxicación en el comedor por negligencia alergógenos.	Grado 1, poco probable	Graves
Tráfico de influencias	Clases particulares a alumnos del centro por parte de trabajadores.	Grado 2, probable	Leves
	Contrataciones que no siguen el protocolo establecido.	Grado 2, probable	Leves
	Falsificación de notas	Grado 2, probable	Graves
	Sustracción de pruebas y exámenes	Grado 1, poco probable	Graves
Cohecho	Soborno	Grado 1, poco probable	Graves
Incitación al odio y a la violencia	Discriminaciones diversas	Grado 2, probable	Graves

CÓDIGO DE CONDUCTA

INTRODUCCIÓN

La Fundación Escolapias Montal es una entidad religiosa de la Iglesia Católica con una misión educadora que se basa en la pedagogía de Santa Paula Montal y San José de Calasanz, que concibe a la persona como un ser singular, social y trascendente, en continuo proceso de crecimiento y maduración, expresado en El Estilo Educativo. Los Centros educativos de la Fundación Escolapias Montal ofrecen una educación integral y armónica para construir una sociedad más fraterna y solidaria, en un mundo que exige una ecología ambiental, económica y social al servicio del bien común.

Por lo señalado, en los Centros de la Fundación los educadores desarrollan una misión de gran responsabilidad para los educandos -normalmente menores de edad- sus familias y para la sociedad en su conjunto, con un alto grado de exigencia.

Las familias que escogen nuestros centros educativos para la educación de sus hijas e hijos esperan que nuestra acción educadora sea congruente con el Carácter Propio (Nuestro Estilo Educativo) que les ofrecemos y que sus hijos encuentren en el Centro elegido un ambiente propicio para su formación integral, que los acoja, respete, les ayude en su maduración, les proteja, y les forme para vivir en sociedad y poner sus capacidades al servicio de la comunidad humana.

La Fundación y los centros, autorizados por la Administración Educativa, tienen también la responsabilidad pública y social de actuar con profesionalidad, objetividad y transparencia, asegurando en su seno comportamientos éticos y, por supuesto, lícitos.

Toda la acción educadora tiene como objetivo el interés superior de los alumnos, especialmente de los menores de edad; su derecho a la educación, una educación integral e inclusiva que promueva todas las dimensiones, las capacidades e inteligencias del alumno; que les capacite para su vida personal, familiar, profesional y para vivir en entornos sociales democráticos.

A lo largo de la historia, también de la historia de la Entidad Titular y de cada Centro, se han ido gestando una serie de normas que conforman el "buen ser" de las/los educadoras y que se encuentran recogidas en instrumentos de muy diversa naturaleza (documentos institucionales, normas, convenios colectivos, reglamentos de régimen interior, protocolos, etc.), o forman parte de los usos profesionales, o institucionales.

1. NATURALEZA Y ÁMBITO DE APLICACIÓN DEL CÓDIGO

El propósito del presente Código de conducta no es el de generar normas -pues la mayoría de las que se contemplan ya existen con anterioridad; ni el de recoger en un solo instrumento todas las normas que han de conocer y cumplir los educadores -pues eso excedería su pretensión haciéndolo excesivamente minucioso y prolijo, siendo así, que hay numerosas normas que no tienen una plasmación escrita; sino, más bien, explicitar en un único documento aquellas que conforman el núcleo fundamental de los comportamientos que se esperan y son exigibles a los educadores de la Fundación.

La interpretación de las normas contenidas en el presente Código ha de hacerse respetando los derechos y libertades reconocidos a los educadores de centros educativos privados con carácter propio católico, así como el tipo de relación que une a cada uno de los educadores con la Fundación.

Objeto y finalidad.

El presente Código de conducta (en adelante, Código) contiene las normas de conducta de carácter positivo (hacer) y negativo (no hacer) que han de seguir los educadores de la Fundación… en cuanto tales educadores, todo ello en consonancia con la naturaleza de la actividad educativa, de Nuestro Estilo Educativo, de la elección del Centro por parte de las familias y del profundo respeto debido a cada alumno y a su proceso de maduración. El Código pretende el desarrollo de la actividad educativa en un ambiente positivo de convivencia, confianza y libertad en el que los educadores desplieguen su vocación y se sientan reconocidos.

El Código no afecta a las conductas de los educadores en su esfera privada, salvo que guarden relación con los alumnos del Centro, o tengan una repercusión pública en el seno de la comunidad educativa y sean objetiva y gravemente contrarias a la identidad del Centro, o a la buena fe.

Destinatarios.

El Código afecta a todas las personas que desarrollen su actividad para la Fundación, con independencia de su relación jurídica con la misma: directivos, personal docente, personal no docente, otros empleados, voluntarios, religiosas, profesionales, capellanes, catequistas, monitores, etc. (en adelante, educadores).

Asimismo, será de aplicación a las empresas de servicios con las que contrate la Fundación y cuyo personal desarrolle actividades para la Fundación y/o sus centros educativos. A tal efecto, se incluirá esta obligación en los contratos que suscriban la Fundación y sus centros con dichas empresas.

Todos los educadores, y el personal de empresas de servicios que tenga contacto habitual con alumnos de los centros, deberán acreditar que no han sido condenados por sentencia firme por algún delito contra la libertad e indemnidad sexual, mediante la aportación de una certificación negativa del Registro Central de delincuentes sexuales. Esta certificación será revisada por la Dirección general cada cuatro años.

2.-COMPORTAMIENTOS

De modo general, los Colegios regentados por las Escolapias en España y quienes trabajan en ellos, de cualquier modo que sea, han de proceder de modo positivamente coherente con el fin institucional pretendido, procurando en todo, el bien integral de las personas a las que sirven, y evitando todo lo que de cualquier forma pueda oponerse a él.

En particular, se observarán los comportamientos siguientes:

A.-De la Institución Educativa

I) Respecto de sí misma

Deberá, como primera obligación, realizar su misión, preservar, mantener y robustecer su propia identidad y manifestarla claramente a sus destinatarios y a cuantos trabajan en ella; hacerla visible al público en general por todos los medios apropiados. Esto implica en la práctica la formulación periódica y la actuación permanente de acciones estratégicas eficaces, encaminadas a esa finalidad.

II) Con la Iglesia

Los Colegios desarrollarán sus actividades en comunión con la Iglesia y cooperarán en sus planes e iniciativas en su entorno, siendo al mismo tiempo solidarios con las iniciativas de carácter universal de la misma; harán todo lo posible para mantener relaciones cordiales con las autoridades y organismos de las iglesias locales y con otras Instituciones semejantes de su mismo ámbito.

III) Con la sociedad en general

Desarrollarán sus actividades sin interferencias políticas de ninguna clase. Cualquier relación con gobiernos, autoridades, instituciones y organismos públicos se llevarán a cabo de forma lícita, ética y respetuosa.

Al mismo tiempo, los Colegios han de ser consciente del deber general de cooperar, según su propia naturaleza y posibilidades, al bien común del medio en que están implantados.

De modo particular,

1. Cumplirán fielmente y, en su ámbito, harán cumplir todas las obligaciones que legalmente les corresponden.
2. Se comprometerán a actuar de modo respetuoso con el medio ambiente, observando los procedimientos y prácticas generalmente aceptadas en la materia. Ofrecerán oportunamente, a quienes trabajan en ellos y a sus destinatarios, orientaciones sobre perspectivas, recursos y prácticas compartidas de índole ecológica y sostenibilidad medioambiental; les pedirán comportamientos concretos coherentes con ellas.

IV) Con los destinatarios de la actividad

Los destinatarios y beneficiarios de la actividad de los Colegios de la Fundación deben ser considerados el centro al que converjan sus esfuerzos. Los Centros se esforzarán por ofrecer a todos un nivel de excelencia y calidad en sus servicios y formas de gestión.

Este horizonte de excelencia debe ser explícitamente orientado al servicio desinteresado a los demás, especialmente a los más necesitados.

Los Colegios trabajarán por sensibilizar a sus destinatarios en las necesidades de los demás y por suscitar en ellos un compromiso efectivo de solidaridad.

V) Con sus empleados y colaboradores

Sin perjuicio de aquellos otros deberes que les incumban en razón a su relación con la misma y en consonancia con su Estilo Educativo y Proyecto Educativo, se tendrá:

1. **Trato digno y respetuoso con las personas**

- El respeto y el trato digno a las personas, así como el rechazo de cualquier actitud vejatoria o discriminatoria, constituyen un principio básico e irrenunciable de actuación.
- Nadie será discriminado, desfavorecido o beneficiado por su ideología, religión o creencias; su pertenencia a una etnia, raza o nación; su sexo, orientación sexual, enfermedad o discapacidad física o psíquica; por ostentar la representación legal o sindical de los trabajadores; o por el uso de cualquier lengua que sea oficial dentro de cada Comunidad Autónoma, según la legislación establecida, atendidas las circunstancias de cada caso.

2. **Garantía de la seguridad y la salud en el trabajo**

- Se establecerán condiciones de trabajo que garanticen la seguridad y protejan la salud de quienes trabajan en los Colegios y de sus destinatarios o beneficiarios.
- A estos efectos se aplicará la normativa sobre seguridad y salud en el trabajo y protección medioambiental; se proporcionará instrucción y formación regular en este ámbito y se llevarán a cabo la vigilancia y el mantenimiento regular de las instalaciones, bienes y equipos.

3. **Respeto de las condiciones laborales y de Seguridad Social**

- Se respetarán, en todo momento, las condiciones laborales y de Seguridad Social establecidas por las disposiciones legales, convenios colectivos y contratos suscritos, así como los derechos que los empleados tengan reconocidos por los mismos.
- Las políticas de contratación y promoción interna se basarán en criterios de mérito, capacidad y calidad profesional, así como en la sintonía personal de los empleados con la propuesta institucional o ideario de los Colegios.
- Además de la igualdad de oportunidades, se cuidará el desarrollo integral de los empleados y colaboradores, tanto en el aspecto profesional como en el personal, ofreciéndoles la formación y las herramientas necesarias para el desempeño de su actividad.
- Como ayuda a sus empleados y colaboradores, para el mejor desempeño de sus funciones, los Colegios les darán a conocer los documentos básicos que definen su misión, les ayudarán a familiarizarse con ellos y a asimilar su contenido, mediante informaciones y reflexiones periódicas, a fin de que inspiren sus comportamientos.

4. **Garantía de libertad sindical.**

Se garantizará a los empleados, sin excepción, los derechos de asociación, sindicación y negociación colectiva.

5. **Fomento de la vida de familia.**

Los Colegios promoverán la vida de familia de los empleados y colaboradores. En la medida de lo posible, se habilitarán los cauces necesarios para facilitar la ayuda adecuada (horarios, días festivos, reducciones de jornada o cualquier otra medida de análogo efecto) a quienes tengan a su cargo hijos menores o familiares de primer grado con discapacidad o enfermedades graves.

6. **Participación en otras actividades y asociaciones**

- Se respetará el derecho de los empleados y colaboradores a participar en cualquier actividad no profesional, siempre que no interfiera en el ejercicio de sus funciones o pueda resultar comprometida la imagen pública de la Institución.
- Asimismo, se reconocerá el derecho de los empleados y colaboradores a participar en asociaciones o partidos políticos u otras instituciones económicas, sociales o culturales, siempre que ello no interfiera el adecuado desempeño de su actividad en el Colegio.

VI) Responsables del cumplimiento de estas obligaciones

1. Son responsables del cumplimiento de estas obligaciones, las Escolapias, los que desempeñan cargos de dirección en los Colegios y, en el ámbito que les corresponde, todos los que trabajan o colaboran en éstos.

B.-Los empleados y colaboradores con la Institución

1.-Comprometidos con la institución.

Quienes trabajan y colaboran en los Colegios de Escolapias, conscientes de la importancia de la misión educativo-evangelizadora y de la función social que llevan a cabo, se han de sentir comprometidos con ella. Mantendrán siempre un comportamiento coherente con los valores e ideales que tratan de educar, expresados en su Estilo educativo, respetando los principios y los medios para realizarlos.

- a.-Todos los que trabajan o colaboren en los Colegios deben mostrar con sus actuaciones un comportamiento recto, íntegro e intachable con los directivos, compañeros, subordinados y con los destinatarios y beneficiarios de su misión y evitar cualquier conducta que pueda dañar la reputación de los mismos.
- b.-Deben también esforzarse por mejorar en su persona y en su actividad profesional para promover la excelencia educativa en todos los ámbitos y prestar el mejor servicio a la Institución, a sus compañeros y destinatarios, así como a la Iglesia y a la sociedad.
- c.-Los educadores de la Fundación, especialmente, deben conocer el Reglamento de Régimen Interior donde se contemplan sus derechos, deberes y funciones.

2. -Vida privada y conflicto de intereses

- a.-La Fundación respeta la vida privada de cada persona y, por lo tanto, el ámbito privado de sus decisiones, sin perjuicio de la deseable coherencia de vida con su ideario y carácter propio, particularmente, por parte de quienes ocupen puestos de responsabilidad.
- b.-Los empleados no podrán desarrollar actividades profesionales ajenas a la Institución que puedan entrar en concurrencia directa con la actividad de la misma, salvo que cuenten con autorización especial del Equipo de Titularidad, ni por sí mismo ni a través de derivaciones a familiares.

3.-Actuaciones públicas.

Cuando las personas que trabajan o colaboran en los Colegios de la Fundación, comparezcan en nombre de la Institución en conferencias, jornadas o en cualquier otro acto que pueda tener difusión pública, en particular ante los medios de comunicación, deben ser especialmente cuidadosas en sus manifestaciones, de modo que no se vea menoscabado el carácter propio de la Institución que representan.

4.-Información confidencial

- a.-Todos los que trabajan o colaboran en un Colegio de la Fundación se abstendrán de utilizar en su propio beneficio o de comunicar, de cualquier manera, datos, documentos, o, información de carácter estratégico o confidencial, obtenidos durante el ejercicio de su actividad en la Institución.
- b.-El carácter de confidencialidad permanecerá una vez concluida la actividad en el Colegio. El empleado o colaborador tendrá la obligación de devolver cualquier material confidencial en el momento del cese de su trabajo.

5.-Acceso a documentación, datos y sistemas informáticos

- a.-Las personas que trabajan y colaboran en el Colegio no tienen derecho a acceder a información ajena a sus funciones, excepto en su calidad de directivo o persona autorizada para ello. Ningún empleado podrá sacar copias de documentos del Centro o de archivos informáticos, salvo que se requieran por motivos de trabajo.
- b.-Todos los datos y archivos informáticos deberán mantenerse de tal forma que cualquier empleado pueda sustituir a otro en todo momento. Por consiguiente, los archivos deberán estar completos, ordenados y su comprensión deberá resultar sencilla.
- c.-No está permitido, por ningún medio o procedimiento, acceder sin autorización a datos o programas informáticos contenidos en un sistema, o, en parte del mismo, o, mantenerse en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
- d.-Los documentos y soportes de almacenamiento de datos utilizados en el lugar de trabajo no podrán ser accesibles a personas no autorizadas y, por consiguiente, se guardarán bajo llave. Los ordenadores deberán protegerse mediante la utilización

- de contraseñas que deberán ser cambiadas con frecuencia.

6.-Administración de bienes

- a.-Los directores y responsables de los Colegios deben administrar los bienes temporales con gran diligencia y fidelidad, no como dueños que puedan disponer a su arbitrio de sus propios bienes, sino como mandatarios que deben administrar, conforme a las leyes de la Iglesia y de las Escolapias, los bienes que les han sido confiados.
- b.-Asimismo, todos los directores y responsables de los Colegios deben vigilar cuidadosamente para que en la administración de los bienes y, especialmente, en las inversiones de capital, se cuide la calidad ética, no se falte a la justicia social y se ponga el debido cuidado en promoverla.
- c.-Los administradores de los Colegios cumplirán fielmente con las obligaciones contables. No les está permitido llevar contabilidades distintas que, referidas a una misma actividad y ejercicio económico, oculten o simulen la verdadera situación del Colegio; ni dejar de anotar en los libros obligatorios, actos, operaciones o, en general, transacciones económicas; ni anotarlos con cifras distintas a las verdaderas; ni practicar en los libros obligatorios anotaciones ficticias.
- d.-Todos los registros contables deberán estar a disposición de los auditores internos y externos.

7.-Blanqueo de capitales

- a.-No está permitido adquirir, poseer, utilizar, convertir o transmitir bienes sabiendo que tienen su origen en una actividad delictiva, así como realizar cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona, que haya participado en la infracción o infracciones, a eludir las consecuencias legales de sus actos.
- b.-Asimismo tampoco está permitida la ocultación o encubrimiento de la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes o propiedad de los mismos, a sabiendas de que proceden de alguna actividad ilícita o de un acto de participación en ella.

8.-Utilización de instalaciones, equipos y servicios

- a.-Los bienes de los Colegios de la Fundación están destinados al cumplimiento de sus fines. En consecuencia, sus instalaciones, equipos y servicios se utilizarán exclusivamente para las funciones que les han sido asignadas. Ningún empleado o colaborador podrá hacer uso de ellos para fines personales, sin la autorización expresa del superior correspondiente.
- b.-Respecto a los equipos informáticos, queda prohibido el acceso a páginas pornográficas, la generación o transmisión de virus, la copia ilegal de software, la descarga de contenidos sujetos a derechos de autor o la distribución de correos electrónicos con fines políticos o comerciales.
- c.-En los medios informáticos se permitirá un moderado uso personal de los mismos que quedará sometido al control de la Institución. El correo institucional se utilizará exclusivamente para la actividad profesional.
- d.-Todos los que hayan trabajado o colaborado en los Colegios tienen la obligación de devolver cualquier equipo o material, que tengan en su poder relacionado con su trabajo o colaboración, en el momento del cese de su relación con la Institución; así como el compromiso de no hacer uso del correo electrónico o firma digital institucional, salvo autorización especial para ello.

C.-Los empleados y colaboradores con los destinatarios de la actividad de los Colegios y la sociedad en general

1.-Relaciones de respeto a cada persona:

- a.-Las personas afectadas por este código de conducta están obligadas a actuar, en sus relaciones, conforme a criterios de respeto, cordialidad, dignidad y justicia, no permitiéndose ninguna forma de violencia, intimidación, hostilidad, humillación, acoso o abuso, ya sea en el orden sexual o meramente personal, ni discriminaciones por razón de ideología, religión o creencias, etnia, raza o nación, sexo, orientación sexual, enfermedad o discapacidad física o psíquica.
- b.-Especial respeto merecen el desarrollo y la dignidad de los menores; han de quedar preservados de cualquier conducta que pueda significar frente a ellos violencia, intimidación, hostilidad, humillación, acoso o abuso, ya sea en el orden sexual o escolar (*bullying*).
- c.-Asimismo, evitarán totalmente contactar con menores a través de Internet, teléfono o cualquier otra tecnología de la información y la comunicación, para proponer o concertar con ellos encuentros con fines sexuales (on-line grooming).

2.-Actuación íntegra, veraz y transparente:

- a.-Todos los que trabajan o colaboran en los Colegios de la Fundación se relacionarán con sus destinatarios y, en general, con cualquier persona física o jurídica con la que traten, de forma íntegra y transparente, facilitando siempre información cierta, clara y veraz, evitando toda conducta engañosa, fraudulenta y falsa que pueda perjudicar a otro.
- b..-Evitarán toda conducta que implique alterar o simular documentos o contratos, suponer la intervención de personas en un acto que no la han participado o atribuir a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hayan realizado, así como faltar a la verdad en la narración de los hechos.
- c.-Respetarán las obligaciones que derivan de la propiedad intelectual ajena.
- d.-Todas las personas responsables de recopilar información del Centro y de transmitirla a las autoridades eclesiásticas y organismos, o de plasmarla en forma de anuncios públicos deberán comunicarla, oportunamente, en su totalidad, de manera veraz, abierta, puntual y comprensible.

3.-Relaciones con proveedores de bienes y servicios

- a.-Todos los que trabajen y colaboren en los Colegios de la Fundación se relacionarán con los proveedores de bienes y servicios de forma lícita, ética e íntegra.
- b.-La selección de los proveedores de bienes y servicios se regirá por criterios de objetividad y transparencia, conciliando el interés de obtener las mejores condiciones en el suministro, con la conveniencia de mantener relaciones estables con proveedores éticos y responsables. En ninguna circunstancia las relaciones o intereses personales influirán en la adjudicación de un contrato.
- c.-Ninguno de los que trabajen y colaboren en los Colegios podrán, por sí o por persona interpuesta, prometer, ofrecer, conceder, solicitar o aceptar, directa o indirectamente, regalos, favores, beneficios, ventajas o compensaciones, en metálico o en especie, cualquiera que sea su naturaleza, que puedan influir en el proceso de toma de decisiones relacionado con el desempeño de las funciones derivadas de su cargo. Se exceptúan de esta prohibición los regalos simbólicos habituales que tengan un valor intrínseco mínimo o sean material publicitario o promocional.
- e.-Si se hace una oferta de este tipo a un responsable, empleado o colaborador, éste deberá notificarlo inmediatamente a su superior.
- f.-Cualquier regalo recibido contraviniendo el presente Código deberá ser inmediatamente devuelto y esta circunstancia, será puesta en conocimiento del superior o responsable inmediato. De no ser razonablemente posible su devolución, el regalo se entregará al superior o responsable del Centro, quien lo destinará a fines de interés social.

4.-Relaciones de respeto a cada persona:

- **Relaciones con autoridades y organismos públicos**. En las relaciones con las Administraciones Públicas, ninguno de los que trabajan y colaboran en los Colegios podrá influir de modo indebido sobre una autoridad, funcionario público o persona que participe en el ejercicio de la función pública, para obtener de ellos decisiones favorables a la Fundación.

D.-Relaciones personales dentro del Colegio

1.-Desempeño del trabajo en un ambiente de confianza y libertad

- a.-Todos los empleados y colaboradores contribuirán a generar en el Centro un ambiente de trabajo gratificante y estimulante, en el que sea reconocido el mérito individual y donde se promuevan el respeto mutuo, el intercambio de ideas, la igualdad, el compañerismo e incluso la amistad, favoreciendo así el desarrollo del Proyecto común.
- b.-Se evitará, por tanto, cualquier forma de violencia, intimidación, hostilidad o humillación y acoso o abuso, tanto de orden laboral como sexual, debiéndose prestar especial atención a la integración laboral de las personas con discapacidad.

2.-Comportamiento respetuoso

- a.-El respeto debido a los demás obliga a presentarse en el trabajo correctamente vestido, de acuerdo con las normas establecidas, y sin la influencia de alcohol o drogas.
- b.-Han de evitarse las palabras soeces o irrespetuosas para los demás.
- c.-No está permitido nada relacionado con el cultivo, el tráfico, el consumo de drogas en el Colegio.
- d.-Está prohibido introducir, vender, exhibir, ofrecer, facilitar o poseer material pornográfico de cualquier tipo en el Centro y/o fuera del mismo.

3.-Descubrimiento y revelación de secretos

- No está permitido apoderarse, sin consentimiento de la persona, para descubrir sus secretos o vulnerar su intimidad, de papeles, cartas, mensajes de correo electrónico u otros documentos o efectos personales, o interceptar sus telecomunicaciones, utilizar artificios técnicos de escucha, transmisión, grabación, reproducción del sonido o de la imagen, o cualquier otra señal de comunicación.

3.-MEDIDAS PARA EL CUMPLIMIENTO DEL CÓDIGO

1.-Difusión y comunicación.

Este Código se hará llegar a todos los que trabajan y colaboran en los Colegios de la Fundación, permanecerá publicado en las páginas webs de éstos y será objeto de las adecuadas acciones de comunicación, formación y sensibilización para su oportuna comprensión y puesta en práctica.

2.-Las personas afectadas por el presente Código firmarán un reconocimiento de que han recibido un ejemplar del mismo, manifestando que comprenden su contenido y están de acuerdo en su cumplimiento.

3.-Cumplimiento de las disposiciones de este Código forma parte esencial de las obligaciones contractuales de los empleados de las Fundaciones Escolapias

El incumplimiento de las normas y pautas de actuación contenidas en este código, sin perjuicio de cualquier otra responsabilidad administrativa o penal a que pudiera dar lugar, puede motivar la adopción de sanciones disciplinarias conforme a lo previsto en la correspondiente legislación laboral.

Nadie podrá solicitar de cualquier persona, a la que sea de aplicación este Código que contravenga lo dispuesto en él.

4.-Comité de Observancia

- A fin de garantizar el cumplimiento del Código, existirá, como órgano dependiente del Patronato de la Fundación, un Comité de Observancia compuesto por cuatro miembros nombrados por el mismo para un tiempo determinado: Vicepresidenta del Patronato de la Fundación que preside el comité, un asesor, la Directora General del ET y un director general de uno de los colegios de la Fundación.
- Son funciones del Comité de Observancia:
- Estudiar y dar respuesta a las consultas, quejas o comunicaciones que se reciban.
- Tramitar las denuncias que procedan y, en su caso, proponer a la Vicepresidenta del Patronato la adopción de las medidas correctoras procedentes.
- Ordenar la realización de auditorías y evaluaciones del cumplimiento del Código de Conducta, así como elaborar un informe anual que será presentado a la Presidenta del Patronato de la Fundación.
- Promover las adecuadas acciones de comunicación, formación y sensibilización para la oportuna comprensión y puesta en práctica del Código de Conducta en todos los Colegios de la Fundación.
- Proponer a la Presidenta del Patronato las modificaciones convenientes en el Código de Conducta que permitan su adaptación permanente a las nuevas circunstancias y compromisos.
- Este Comité podrá actuar por propia iniciativa y a instancia o por comunicación de cualquier persona que trabaje en los Colegios de la Fundación o se relacione con ella.
- A estos efectos las comunicaciones podrán hacerse llegar al Comité a través de cualquiera de los siguientes medios:

Vicepresidenta del Patronato: M. Amelia Ramírez de Nicolás

Correo postal: C/ Palomeque, 2. 50004 Zaragoza

Correo electrónico: educacion@escolapias.es

5.-Comunicación de infracciones

- Como contribución al bien de los Colegios de la Fundación y de cuantos se relacionan con ella, las personas a las que se aplica este Código deberán informa, en primer lugar, al Director General del Centro y más adelante si es necesario, al Comité de Observancia, de las actuaciones contrarias a sus disposiciones de las que hayan tenido conocimiento, en especial, de las que pudieran representar transgresión de leyes o normas generales de obligado cumplimiento o causar daño a alguien.
- Las personas que se consideren afectadas por actuaciones contrarias a las disposiciones de este Código, deberán informar, en primer lugar, al Director General del Centro y más adelante si es necesario, al Comité de Observancia los hechos que consideren lesivos.
- La comunicación de posibles infracciones que se efectúen quedan amparadas con el correspondiente deber de sigilo y secreto sobre los informantes.

6.-Supervisión

En todo caso los Directores Generales de los Colegios también deberán tomar la iniciativa de supervisar regularmente las actividades de sus subordinados.

7.-Revisión

El Código será revisado siempre que sea necesario para adaptarlo a los futuros cambios legislativos y a las nuevas circunstancias y compromisos que se le planteen a la Provincia.

8.- Vigencia y seguimiento

El Código tiene una vigencia indefinida, si bien podrá ser modificado por la Fundación, en función de la evaluación sobre su ejecución o porque sea necesaria o conveniente su adaptación.

Aprobado en Zaragoza, a 22 de Junio de 2020

PRESIDENTA DEL PATRONATO	VICEPRESIDENTA DEL PATRONATO

CÓDIGO DEONTOLÓGICO

Servicios Centrales FUNDACION ESCOLAPIAS MONTAL

PRINCIPIOS DE LA FUNDACIÓN ESCOLAPIAS MONTAL

La educación Escolapia tiene como objetivo principal, lograr el máximo desarrollo de las facultades intelectuales, físicas, afectivas y espirituales de las nuevas generaciones, tanto a nivel individual como social. Concebimos a la persona como un ser singular, social y trascendente en continuo proceso de crecimiento y maduración. Un ser abierto a todos los valores que lo enriquecen.

Nuestra concepción de educación cristiana exige que la escuela sea una auténtica Comunidad Educativa y que el conjunto de miembros que la forman estén integrados armónicamente a través de la participación, con el objetivo de lograr una educación coherente que favorezca la formación y crecimiento personal del alumnado.

El profesorado asume y hace suya la pedagogía escolapia que se caracteriza por ser abierta y flexible, amplia en contenidos y materias, encarnada en el entorno y capaz de integrar los avances tecnológicos y pedagógicos para su constante actualización.

La familia es la principal responsable de la educación de sus descendientes, siendo el profesorado el principal actor en el centro escolar, complementando con su acción la tarea educativa de la familia.

El personal de administración y servicios colabora en la educación y en la marcha de la escuela, según sus respectivas competencias y responsabilidades.

El personal colaborador participa dando continuidad al estilo propio de la escuela en las actividades complementarias y extraescolares

COMPROMISOS Y OBLIGACIONES DE TODO EL PERSONAL TRABAJADOR DE LA FUNDACIÓN ESCOLAPIAS MONTAL

D./Dña.

Con DNI , es informada de sus compromisos y obligaciones como persona trabajadora de la Fundación Escolapias Montal.

1.Compromisos y deberes con el alumnado

1.1 Contribuir activamente al ejercicio efectivo del principio constitucional del derecho a la educación.

1.2 Ayudar al alumnado a conseguir su propio crecimiento, la aceptación y superación de sí mismo, fomentando la capacidad de autonomía, decisión y sentido crítico con una relación de confianza que contribuya fomentar la autoestima.

1.3 Tratar de manera justa y equitativa al alumnado, sin aceptar ni permitir prácticas discriminatorias de ningún tipo.

1.4 Motivar al alumnado, despertando y manteniendo el interés por los contenidos de las asignaturas. Fomentando la creatividad y la inquietud por adquirir nuevos conocimientos y por la investigación y la búsqueda de la verdad como principio rector del saber.

1.5 Educar en la libertad y para la libertad responsable, para que el alumnado actúe por propia convicción, con rectitud de conciencia, respetando el principio de igualdad y la libertad de los demás.

1.6 Guardar el secreto profesional en relación con los datos personales del alumnado de que se disponga en el ejercicio profesional de la docencia.

2. Compromisos y deberes en relación con las familias y tutores del alumnado

2.1 Favorecer la cooperación entre las familias y el profesorado, compartiendo la responsabilidad educativa en los temas que afecten a ambas partes, propiciando la participación.

2.2 Proporcionar a las familias y tutores toda la información que se precise sobre los proyectos educativos del centro, la programación docente y los criterios de evaluación.

2.3 Proporcionar a las familias y tutores la información acerca del proceso educativo de sus hijos, el grado de consecución de los objetivos y las posibles dificultades que se detecten, así como la orientación adecuada a dichas circunstancias.

2.4 Respetar y guardar secreto profesional sobre las informaciones proporcionadas, en el ejercicio de sus funciones, por familias y tutores.

3. Compromisos y deberes en relación con la Fundación Escolapias Montal

3.1 Promover y participar activamente en el Proyecto Educativo-Pastoral cristiano de la Fundación Escolapias Montal.

3.2 Respetar y hacer respetar las normas de funcionamiento del Centro y colaborar en todo momento con sus órganos de gobierno, con los diversos departamentos, con los servicios de orientación psicopedagógica, las tutorías y cualesquier otro servicio de la Fundación.

3.3 Favorecer la convivencia en el Centro, contribuyendo a mantener un ambiente adecuado para la enseñanza y el aprendizaje.

3.4 Velar por el buen estado de mantenimiento y limpieza de instalaciones y materiales, inculcando al alumnado el respeto por los bienes comunes y públicos.

3.5 Ejercer con dedicación las responsabilidades directivas o de cualquier tipo que se desempeñen, actuando como modelo de conducta ante los compañeros y compañeras.

3.6 Velar en cualquier circunstancia por el prestigio de la Fundación Escolapias Montal, contribuyendo en todo momento a la mejora de su calidad.

3.7 Colaborar con la Fundación Escolapias Montal y con las autoridades educativas en cuantas consultas e informaciones se precise

4. Compromisos y deberes en relación con los compañeros

4.1 Aportar los propios conocimientos, capacidades y aptitudes a fin de que exista un clima de confianza que potencie el trabajo en equipo.

4.2 Colaborar con todo el personal que participa en la educación, para que una actuación colectiva coordinada, redunde en beneficio del alumnado y de la institución.

4.3 Respetar el ejercicio profesional de todo el claustro, sin interferir en su trabajo ni en su relación con el alumnado, familias y tutores.

4.4 Guardar el secreto profesional en relación con los datos personales del personal de que se disponga en el ejercicio de cargos de responsabilidad.

5. Compromisos y deberes en el ejercicio de su profesión

5.1 Conocer que la distribución anual de la jornada de trabajo, se concreta en 38 h. semanales que, en el caso del personal docente será de 37,5 h. y se distribuirán de la siguiente manera:

- 25 horas de carácter lectivo presenciales en el centro
- 5 horas de carácter complementario presenciales en el centro para claustros, reuniones, sesiones de evaluación, sesiones de coordinación, atención tutorial, atención a familias
- 7,5 h. para preparación de clases, corrección de tareas, corrección de exámenes y que no necesariamente deberán ser presenciales.

5.2 En aquellos casos en que el personal no esté contratado a jornada completa, se establecerá una distribución proporcional a las horas contratadas.

5.3 Se establece como horario general del Centro para el personal de administración y servicios de lunes a viernes de 06:00 a 22:00 h. y sábados de 08:00 a 14:30 h.

5.4 Se establece como horario general del Centro para el personal de docente de lunes a viernes de 08:00 a 18:00 h. para la jornada lectiva y hasta las 20:00 h. para horas complementarias. En cualquier caso, lo jornada lectiva podrá modificarse sin previo aviso de acuerdo a la jornada lectiva que para cualquier etapa pudiera autorizar la administración competente en materia educativa.

5.5 En el caso de que un profesor, en un curso escolar, no tenga destino en el aula para todas sus horas lectivas contratadas, quedará a disposición de la Dirección del Centro para realizar aquellas tareas que se le encomienden que siempre obedecerán al interés general del Centro y nunca al particular del docente (corrección de tareas, corrección de exámenes…)

5.6 Conocer y aceptar que además de la jornada lectiva y complementaria, todo el personal del centro deberá realizar al menos 30 h. de formación anuales que se realizarán principalmente, aunque no exclusivamente, durante los primeros quince días de julio.

5.7 Que todos los nuevos educadores, deberán realizar la formación en identidad escolapia programada a tal fin y que con el paso del tiempo deberán realizar el denominado de reciclaje y evolución en el carisma.

5.8 Conocer que, para el personal docente la vigilancia en los patios de recreo del alumnado es obligatoria diariamente, salvo que la Dirección del Centro realice una organización que permita la alternancia de días de vigilancia con días de descanso siempre y cuando aquella quede garantizada.

5.9 Aceptar y respetar el horario asignado para cada curso escolar de buen grado, reconociendo la dificultad que supone realizarlos y anteponiendo el interés general y de los alumnos al suyo propio.

5.10 Participar en todas aquellas actividades y celebraciones que más allá del currículo, vayan alineadas con el carisma fundacional.

5.11 Aceptar de buen grado los cargos de coordinación y directivos que la Entidad Titular le propusiese para su ejercicio.

5.12 Aceptar, en la medida de lo posible, cualquier propuesta de acompañamiento y vigilancia del alumnado en salidas culturales y recreativas aun cuando estas fueren en periodo de vacaciones escolares.

5.13 Colaborar activamente y participar en la elaboración de materiales propios tanto curriculares como extracurriculares.

5.14 Todos los materiales creados por el personal de la Fundación Escolapias Montal en el ejercicio de su profesión y dentro del horario destinado a tal fin, serán propiedad de la Fundación Escolapias Montal y autoría de la persona o personas que lo hayan elaborado.

5.15 El uso de dispositivos TIC, redes, correos electrónicos, así como cualquier otra tecnología, se utilizará con diligencia responsable, única y estrictamente con motivos del desempeño profesional.

COMPROMISO DE CUMPLIMIENTO

Mediante la puesta a disposición de este documento, el usuario reconoce haber leído y entendido todas y cada una de las cláusulas siendo consciente de su responsabilidad y obligado cumplimiento.

Usted acepta y se compromete a cumplir expresamente, incorporando el presente Anexo a su contrato de trabajo en calidad de cláusulas adicionales.

El presente código deontológico ha sido aprobado por el Patronato de la Fundación Escolapias Montal, el 12 de marzo de 2021.,