COMITÉ OLÍMPICO
ESPAÑOL

POLÍTICA DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS

Código: PL007
Versión: 1.0
Fecha de emisión: 18/06/2019

HOJA DE CONTROL

REGISTRO DE CAMBIOS:

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión inicial	JM TORO - Abogados	11/07/2018

REVISIÓN Y APROBACIÓN:

Realizado por:	Revisado por:	Aprobado por:
JM TORO - Abogados	Secretaría General	Comité Ejecutivo
Fecha: 11/07/2018	Fecha: 31/05/2019	Fecha: 18/06/2019

CONTENIDO

1 OBJETO

Conforme a lo establecido en la legislación de Protección de Datos de Carácter Personal, (Reglamento UE 2016/679 y L.O. 3/2018) el COE informa al empleado de la política de seguridad implantada en la empresa con el fin de cumplir con las medidas de seguridad que le son exigidas por la referida legislación y que el incumplimiento de las mismas puede suponer a la empresa una sanción económica por lo que cuando dicho incumplimiento se asocie a un individuo concreto será sancionado a nivel interno disciplinariamente según lo acuerde el Responsable del Fichero.

El trabajador declara conocer las normas y política de seguridad que a continuación se establece, así como que el incumplimiento de cualquiera de las obligaciones o prohibiciones establecidas en la totalidad de este documento será considerado como una falta muy grave imponiéndose las sanciones previstas para este tipo de faltas especificadas en la normativa laboral respecto al Convenio Colectivo de aplicación, pudiendo ser sancionado incluso con el despido disciplinario. En este sentido:

2 OBLIGACIONES DE CARACTER GENERAL

Confidencialidad / deber de secreto

Por el art 5.1 f Reglamento UE 2016/679 se comunica a todo el personal de COE que todas las personas que intervengan en cualquier fase del tratamiento de datos e información de cualquier tipo están obligadas al deber de confidencialidad y de secreto y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con COE del tratamiento o, en su caso, con el responsable del mismo.

El personal deberá acceder a la información para la que ha sido autorizado atendiendo a las necesidades para el desempeño de su puesto de trabajo.

Se deberá guardar todos los soportes físicos y/o documentos que contengan información en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

En el supuesto de existir traslado o distribución de soportes y documentos fuera de las instalaciones deberá ser por razones de la actividad propia de la empresa y dentro de las funciones del usuario según su puesto de trabajo, poniendo los medios necesarios para evitar el acceso o manipulación de la información por terceros como es el uso de contraseñas y custodiar la información en todo momento.

Ficheros de carácter temporal o copias de documentos son aquellos en los que se almacenan datos, generados para el cumplimiento de una necesidad determinada o trabajos temporales y auxiliares. Estos ficheros de carácter temporal o copias de documentos deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán cumplir con los niveles de seguridad asignados.

Únicamente las personas autorizadas podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de acceso de los usuarios son

concedidos por el Administrador del Sistema. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del responsable correspondiente.

Si el trabajador tiene conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema (responsable de informática), o en su caso del registro de la misma en el sistema de registro de incidencias.

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 ese usuario.

Respetar las normas establecidas con respecto a la seguridad de los sistemas de información y a la información que en ellos se trata.

Aquellos medios que sean reutilizables, y que hayan contenido copias de información, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

Mantener seguros la información que deba utilizarse fuera del lugar habitual de trabajo (clientes, otras instalaciones, domicilio particular…).

Tienen el carácter de información especialmente reservada los datos personales, datos de carácter financiero, contable o comercial de COE en los que se incluyen, sin carácter limitativo, los procedimientos, metodologías, código fuente, algoritmos, bases de datos de clientes, planes de marketing, y cualquier otro material que forma parte de la estrategia de negocio de COE.

Los soportes que contengan información deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para su uso.

3 OBLIGACIONES RESPECTO A LA INFORMACIÓN CONTENIDA EN SISTEMAS INFORMÁTICOS

Cada puesto de trabajo estará bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestra no pueda ser visible por personas no autorizadas.

Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esta confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlos 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. En el caso de las impresoras, deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengas datos o información protegidos. Si las impresoras son compartidas con otros usuarios

no autorizados para acceder a los datos de fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Cada una de las personas autorizadas accederá al sistema de información o bien al fichero mediante la clave/contraseña asignada.

El usuario debe mantener la confidencialidad de las contraseñas y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlos como incidencia y proceder a su cambio.

El usuario debe evitar la escritura de las contraseñas en papel, salvo si existe una forma segura de guardarlo.

El usuario debe cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad o de la del sistema.

Los usuarios deben cambiar las contraseñas a intervalos de tiempo regulares, cada 75 días, evitando utilizar contraseñas antiguas o cíclicas, el entorno de Windows prohíbe repetir las tres últimas contraseñas.

Los usuarios deben cambiar las contraseñas temporales asignadas para inicio, la primera vez que se acceda al sistema. (El sistema lo requiere).

El usuario no debe incluir contraseñas en ningún procedimiento automático de conexión, que, por ejemplo, las almacene en una macro, o en ventanas de acceso donde aparezca "Recordar contraseña".

Los usuarios no deben compartir contraseñas de usuario individuales (cada usuario debe conocer exclusivamente la suya).

No usar la misma contraseña para propósitos profesionales que para no profesionales.

El usuario debe seleccionar contraseñas de buena calidad, con una longitud mínima de 7 caracteres, que sean:

- Fáciles de recordar.
- No estén basadas en algo que cualquiera pueda adivinar u obtener usando información relacionada con el usuario, por ejemplo, con nombres, fechas de nacimiento, números de teléfono, etc.
- Estén carentes de caracteres consecutivos repetidos o que sean todos números o todas letras. (en algunos casos, el sistema requiere un mínimo de complejidad).
- No contengan caracteres consecutivos, idénticos, todos numéricos o alfanuméricos.

Cerrar o bloquear todas las sesiones al término de la jornada laboral y en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

No copiar la información al ordenador personal, disquetes, portátil o a cualquier otro soporte sin autorización expresa de la empresa.

Asegurarse de la existencia de una autorización antes de sacar un soporte o un equipo portátil con datos fuera de su ubicación habitual.

Queda prohibido:

- Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.
- Intentar modificar el registro de acceso habilitado.
- Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.

Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos, que solo podrá ser cambiada bajo la autorización del responsable de seguridad o por administradores autorizados.

Cuando la salida de información se realice por medio de correo electrónico los envíos se realizarán, siempre y únicamente, desde una dirección de correo controlada por el administrador de seguridad, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de registro de salidas que permita conocer en cualquier momento los envíos realizados, a quien iban dirigidos y la información enviada.

La referida política será de aplicación a todos los usuarios que traten datos a través del ordenador portátil o teléfono móvil de empresa, por medio de los cuales pueden tratar información de la empresa, así como datos personales. En referencia al teléfono móvil deberá bloquease la pantalla mediante patrón o contraseña

Por otra parte, el acceso a las instalaciones fuera del horario laboral deberá realizarse por medio de la contraseña que cada usuario tiene de la alarma de las instalaciones siendo está confidencial e intransferible aplicándose las mismas reglas de confidencialidad que con la contraseña de acceso a los sistemas informáticos.

4 OBLIGACIONES RESPECTO DE LA INFORMACIÓN CONTENIDA EN DOCUMENTOS

Por lo que respecta a los ficheros no automatizados tiene las siguientes obligaciones:

- Mantener debidamente custodiadas las llaves de acceso a la organización, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con información, debiendo poner en conocimiento al Administrador del sistema, o jefe de departamento cualquier hecho que pueda haber comprendido esa custodia.
- Cerrar con llave las puertas de los despachos, así como de los armarios, cajones o archivadores, al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
- Asegurarse de que no quedan documentos impresos que contengan datos impresos en la bandeja de salida de la impresora o fax.

- Evitar (cuando se produzcan copias o reproducción de documentos) que puedan acceder a las copias personas no autorizadas a ello.

5 OBLIGACIÓN A HACER BUEN USO DEL CORREO ELECTRÓNICO

5.1 POLÍTICA

El correo electrónico (e-mail) es una herramienta valiosa para enviar y recibir mensajes, obtener y enviar información y hacer negocios. Sin embargo, a menos que sean usados apropiadamente, pueden ser también una fuente de problemas de seguridad y responsabilidad legal para COE y los individuos que lo usan.

COE ha establecido esta Política de correo electrónico para proteger los activos de la entidad y reducir su posible responsabilidad legal.

Esta Política debe ser cumplida por todos los usuarios del sistema de correo electrónico de COE.

El acceso a los recursos del servicio de correo electrónico es un privilegio que está condicionado a la aceptación de la Política de utilización de estos recursos.

La calidad de estos servicios depende en gran medida de la responsabilidad individual de los usuarios.

5.2 PROPIEDAD DEL CORREO ELECTRÓNICO

El Correo Electrónico es una herramienta de productividad que COE pone a disposición de sus empleados, como una herramienta de trabajo más, para el desarrollo de las funciones qué les tiene encomendadas. Por lo tanto, debe utilizarse únicamente para su uso laboral.

Los usos ajenos a estos fines son por tanto considerados inapropiados y están totalmente prohibidos.

5.3 NORMAS

5.3.1 REGLAS DE USO

El sistema de correo electrónico de la entidad debe ser usado para aquellas comunicaciones requeridas como consecuencia del desarrollo de la actividad propia de COE con otras entidades o con otros usuarios.

Así el acceso y uso de este servicio por parte de los usuarios, así como los privilegios asociados a dicho acceso deben limitarse a los necesarios para realizar su actividad, es decir, destinados a

su uso estrictamente laboral, por lo que queda totalmente prohibido su uso para fines privados o particulares ajenos a los estrictamente laborales.

Los usuarios son responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la empresa COE.

Es una falta muy grave facilitar y/o permitir la utilización de la cuenta y/o el correspondiente buzón a personas no autorizadas.

Está prohibida la utilización en los equipos informáticos provistos por COE de buzones de correo electrónico de otros proveedores de Internet, salvo autorización expresa del Administrador del Sistema, o su responsable directo o superior inmediato.

La violación de la seguridad de los sistemas puede generar responsabilidades civiles y/o criminales. COE colaborará al máximo de sus posibilidades en cualquier eventual investigación contra este tipo de actos o cualquier otra utilización ilegal, incluyendo la cooperación con la Justicia.

El sistema informático de COE se encuentra protegido contra virus informáticos por un antivirus. La responsabilidad sobre la comunicación a los responsables del sistema de cualquier anomalía suscitada en este sentido depende de cada usuario, así como la apertura de un correo sobre el que se tengan dudas o la emisión de un mensaje de virus por parte del antivirus.

No es correcto enviar correos electrónicos a personas que no desean recibirlo. En caso de reunir determinadas características, estos envíos podrían llegar a enrolarse dentro del concepto de spam, lo que configura una conducta prohibida por la legislación vigente en nuestro país. Si COE llegara a recibir reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.

Además, está completamente prohibido realizar cualquiera de las siguientes actividades:

- Enviar mensajes que comprometan la reputación de COE a foros de discusión, listas de distribución y/o newsgroups.
- Enviar información confidencial, privada o propiedad de COE o información sobre clientes y/o proveedores.
- Enviar materiales externos con derechos de propiedad intelectual, de marca comercial registrada patentados, incluyendo artículos o software, que no sean propiedad de COE o que no hayan sido autorizados para ser enviados, reenviados, almacenados por el propietario de los mismos.
- Además, el usuario debe usar discreción al enviar correo electrónico a ¨todos los usuarios¨ del sistema, o a cualquier otra lista grande de destinatarios, ya sea interna o externa, utilizando la copia oculta.

5.3.2 CONSIDERACIONES DE PRIVACIDAD

Todas las comunicaciones enviadas, recibidas o almacenadas mediante la mensajería electrónica de COE se consideran propiedad de ésta.

Al objeto de garantizar el cumplimiento de la presente política, el trabajador consiente que COE pueda llevar a cabo un control aleatorio de los medios informáticos que la empresa pone a su disposición como instrumento de trabajo, así como poder supervisar/auditar las comunicaciones y archivos remitidos por los usuarios por medio de los recursos y sistemas de la entidad de que se está haciendo un uso indebido de los recursos de COE, incumpliéndose los aspectos descritos en esta política, ya que el uso debe ser estrictamente profesional. La supervisión/auditoria o el acceso respetarán en todo momento los derechos de privacidad de los usuarios, incluyendo el cumplimiento de la legislación autonómica, nacional e internacional.

La utilización del correo electrónico para fines ajenos a los laborales se considerará una infracción del deber de buena fe contractual, con independencia de que le conlleve o no un lucro personal o perjuicio cuantificable para la empresa. La citada infracción podrá ser causa de sanción disciplinaria, muy grave, incluyendo, en su caso, el despido disciplinario.

6 OBLIGACIÓN AL ACCESO A INTERNET CON FINES RELACIONADOS CON EL LUGAR DE TRABAJO

6.1 POLÍTICA

El acceso a la red Internet es un privilegio y COE lo pone a disposición de sus empleados, como una herramienta de trabajo más, por lo tanto, debe utilizarse únicamente para uso laboral y por el tiempo estrictamente necesario. Los usuarios de ordenadores dispuestos en red deben concienciarse de que se trabaja compartiendo recursos con otras personas de forma permanente. La utilización de los mismos en forma incorrecta, puede obstaculizar el trabajo del resto de los usuarios, llegando a interferir en la normal prestación de los diferentes servicios informáticos privando a otras personas de los medios necesarios para realizar su trabajo, a parte de los riesgos de virus informático.

Esta Política debe ser cumplida por todos los usuarios de ordenadores dispuestos en red con el fin de garantizar el buen aprovechamiento del sistema, así como la seguridad del mismo, por lo que se fijan las siguientes normas de uso de obligado cumplimiento.

6.2 NORMAS

6.2.1 REGLAS DE USO

Los usuarios son únicos responsables de las sesiones iniciadas en la red Internet desde sus terminales de trabajo. En la empresa, la red de internet tiene carácter laboral y no debe ser utilizada con fines distintos.

Está completamente prohibido modificar las configuraciones de los navegadores (opciones de Internet) del equipo ni la activación de servidores o puertos sin autorización de los responsables de seguridad.

Se recomienda, que se proceda evitar la utilización de imágenes (como los formatos GIF, JPG, BMP o TIFF entre otros), sonido (formatos WAV y MP3 principalmente) y video (MPG, DivX;-), AVI, RAW o similares) para fines ajenos a la actividad laboral de la empresa, debido a que el tamaño de estos archivos satura los canales de comunicación y disminuye la velocidad de transmisión perjudicando al funcionamiento de la red en su conjunto.

Está completamente prohibido el acceso, la descarga y/o el almacenamiento en cualquier soporte, (a modo de ejemplo, Pen Drive, tarjetas de memoria, MP3… etc), de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres; de virus y códigos maliciosos y, en general, de todo tipo de programas y/o plugin sin la expresa autorización del coordinador de seguridad de COE. La empresa colaborará al máximo de sus posibilidades en cualquier eventual investigación contra este tipo de actos o cualquier otra utilización ilegal, incluyendo la cooperación con la Justicia.

Está completamente prohibido la utilización ajena a las actividades de la empresa de los servicios de IRC (canales de chat) ya sea mediante el acceso a páginas que los brinden como desde aplicaciones instaladas en los equipos (como MS Messenger, TOM, Yahoo, ICQ o similares), salvo que sean destinadas a su uso estrictamente laboral por ser necesarias (a modo de ejemplo el Skype), para la actividad y se esté expresamente autorizado para ello por parte de la empresa. Tampoco se permite el acceso a páginas de juegos en línea o la descarga de cualquier dispositivo similar.

Está completamente prohibido cualquier sistema de compartir ficheros con información relacionado con la empresa, clientes, proveedores, como puede ser Emule, Dropbox o google Drive o cualquier otro que pueda existir en el mercado sin una autorización expresa de la dirección de la empresa.

El sistema informático de COE cuenta con los pertinentes programas para detección y protección de los denominados virus informáticos.

6.2.2 CONSIDERACIONES DE PRIVACIDAD

Al objeto de garantizar el cumplimiento de la presente política, el trabajador consiente expresamente que COE se reserva el derecho de cancelar, limitar o supervisar/auditar las conexiones y/o comunicaciones realizadas desde su sistema informático, pudiendo hacer las comprobaciones e indagaciones pertinentes desde todos y cada uno de los puestos informáticos que componen la red interna. En tal caso, se respetarán los derechos de privacidad de los usuarios en cumplimiento de la normativa vigente.

La utilización de Internet para fines ajenos a los laborales se considerará una infracción del deber de buena fe contractual, con independencia de que le conlleve o no un lucro personal o perjuicio cuantificable para la empresa. La citada infracción podrá ser causa de sanción disciplinaria, muy grave, incluyendo, en su caso, el despido disciplinario.

7 OBLIGACIÓN DE BUEN USO DEL SISTEMA INFORMÁTICO

7.1 POLÍTICA

Para garantizar la debida confidencialidad del tratamiento de la información COE ha adoptado las siguientes normas preceptivas de obligado cumplimiento para todos los usuarios y colaboradores que se les haya otorgado un Ordenador personal propiedad de la empresa, debiendo conocer el uso y funcionalidades del terminal, así como los usos que la empresa autoriza.

7.2 NORMAS

7.2.1 REGLAS DE USO

No se permite la instalación de ningún producto informático en el sistema de información de la empresa. Todas las aplicaciones necesarias para el desempeño de su trabajo serán instaladas únicamente por el personal especializado del Departamento sistemas o bajo su supervisión, tras su conocimiento y aprobación.

No deberán utilizarse los recursos del sistema de información de la empresa para uso privado ni para cualquier otra finalidad diferente a las estrictamente laborales.

Se prohíbe la revelación a cualquier persona ajena a la organización, de información a la que se haya tenido acceso en el desempeño de sus funciones, sin la debida autorización, así como de cualquier soporte que contengan datos.

Todo usuario del sistema de COE se encuentra obligado a cumplir la normativa vigente en el desarrollo de sus funciones en la empresa, así como los extremos vertidos en el documento de seguridad, en relación a la protección de datos de carácter personal.

Está totalmente prohibido la utilización de Pen drive o cualquier otro sistema de almacenamiento con el fin de almacenar en soporte informático información relativa a la empresa, clientes o proveedores, salvo expresa autorización de la empresa.

Deberá darse cumplimiento a los compromisos anteriores, incluso después de extinguida la relación laboral con COE. El trabajador será responsable frente a COE y frente a terceros, de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores, debiendo resarcir a la empresa por las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

8 OBLIGACIÓN DE BUEN USO DEL TELÉFONO MÓVIL DE EMPRESA

8.1 POLÍTICA

Para garantizar la debida confidencialidad del tratamiento de la información COE ha adoptado las siguientes normas preceptivas de obligado cumplimiento para todos los usuarios y colaboradores que se les haya otorgado un teléfono móvil propiedad de la empresa, debiendo conocer el uso y funcionalidades del terminal, así como los usos que la empresa autoriza.

8.2 NORMAS

8.2.1 REGLAS DE USO

Por tanto, el usuario del teléfono móvil corporativo tiene que ser consciente que:

- El terminal es propiedad de la empresa y que una vez acabada la relación laboral deberá devolver el mismo en las mismas condiciones que lo recibió.
- El terminal que se le ha asignado es una herramienta que debe ser utilizada exclusivamente para fines laborales, no permitiéndose su uso privado, por lo que deberá actuar en consecuencia, dándole un uso responsable.
- Las llamadas utilizan una red de telefonía móvil de un tercero, con lo que no son gratuitas. Existiendo además una cuota de "*roaming*" para el caso de las llamadas internacionales (cursadas y recibidas), lo cual supone un coste adicional.
- Al contrario que las conexiones de datos WIFI que son gratuitas, las conexiones de datos móviles (3G-4G) no son gratuitas, sino que tienen coste, tanto a nivel nacional como en otros países.

La Dirección de la empresa:

- No se hace responsable en los casos de "robo".
- No se hace responsable de los datos bancarios que el usuario haya podido incluir en el terminal
- No se hace responsable de las operaciones bancarias que a título personal haya podido realizar a través del terminal de la empresa ni de los datos personales.
- Informa que a día de hoy los Smartphone corporativos no están protegidos por ningún tipo de software antivirus, por lo que recomienda no acceder a cuentas bancarias o de otra naturaleza de carácter personal desde un Smartphone corporativo.
- No se hace responsable de que las aplicaciones descargadas ya sean gratuitas o de pago, tengan el funcionamiento deseado por el usuario, o bien supongan un conflicto con las aplicaciones básicas soportadas (sincronización del correo, calendario, contactos, etc.).

La Dirección de la empresa informa que:

- Se podrá solicitar el terminal en cualquier momento con el fin de poder comprobar que se hace un uso adecuado del mismo y en caso de un problema una vez realizadas las comprobaciones básicas en el terminal, las siguientes acciones serán desinstalar las aplicaciones no corporativas que se detecten, y finalmente restablecer el teléfono a los valores de fábrica (perdiendo por lo tanto toda la configuración, personalización y aplicaciones instaladas).
- Tampoco se hace responsable de la continuidad de un sistema de Smartphone como sistema homologado en la compañía. Esto es importante sobre todo para las aplicaciones de pago (de cualquier manera, no soportada).
- Cuando se envía el terminal a reparar al fabricante/operadora, casi en el 100% de los casos el terminal viene restablecido a los valores de fábrica.
- No está permitido, salvo en casos "emergencias", el uso del teléfono móvil como modem de conexión a Internet desde el PC. Si tiene esta necesidad, por favor solicite un modem USB/PCMCIA.

El usuario del teléfono móvil debe leerse las condiciones y especificaciones técnicas que junto al teléfono móvil se le han dado por parte del fabricante, así como de proceder a bloquear mediante pin el acceso y así tener que introducir de nuevo el pin tras haberse superado el tiempo de apagado automático de la pantalla y querer volver a utilizar el móvil, con el fin de evitar el acceso a la información del teléfono a terceros ajenos a la organización, en caso de robo o pérdida.

9 APROBACIÓN, ENTRADA EN VIGOR Y REVISIÓN DE LA PRESENTE POLÍTICA

El Comité Ejecutivo del COE aprobó la presente Política en su reunión del 18 de junio de 2019, momento en el cual entró en vigor con efectos vinculantes para todos sus destinatarios.

Sin perjuicio de lo anterior, la presente Política será objeto de revisión y, en su caso, actualización, periódica.

10 DOCUMENTOS RELACIONADOS

- PL006: POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS
- NR006: MANUAL DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS
- PC017: PROCESO DE AUTORIZACIÓN DE TRATAMIENTO DE DATOS FUERA DE LOCALES
- PD010: PROCEDIMIENTO PARA AUTORIZAR TRATAMIENTO DE DATOS FUERA DE LOCALES
- FM006: FORMULARIO DE AUTORIZACIÓN DE USO DE ORDENADORES PORTÁTILES
- FM021: FORMULARIO DE AUTORIZACIÓN DE ACCESO REMOTO