POLÍTICA DE SEGURIDAD

CENTRO ASOCIADO A LA UNED EN MADRID

Este documento debe ser entregado a todas las personas que tratan datos personales en la entidad. Las sucesivas versiones deben ser notificadas a dichas personas a través de correo electrónico con acuse de recibo.

Los usuarios deben verificar periódicamente que disponen de la versión más actualizada del documento, según la numeración que consta al pie del mismo.

CONTROL DE VERSIONES		
EDICION	**FECHA**	**DESCRIPCIÓN**
Cuarta	Diciembre 2020	Se mantiene actualizado el presente Documento a las necesidades derivadas 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y se aplican novedades introducidas por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Principales Modificaciones: Las contraseñas deben tener al menos 10 caracteres, mayúsculas, minúsculas, números y un símbolo. - Nuevo modelo de formulario de registro de brechas de seguridad. - Se incluyen en la Política de Seguridad procedimientos que regulan los siguientes aspectos: o Gestión de recursos y gestión de los cambios o Plan de continuidad de negocio o Formación del personal o Monitorización y registro o Seudonimización/cifrado o Actualizaciones software. o No desactivación de antivirus ni instalación de determinadas aplicaciones o Seguridad de las comunicaciones: instalación de cortafuegos, sistemas de detección de intrusión,

		segregación de redes y la utilización de mecanismos de cifrado. o Borrado de la información: políticas de borrado automático o Medidas de seguridad físicas: acceso físico no autorizado mediante sistemas de identificación del personal, definición de áreas de acceso restringido, sistemas de detección de intrusos o la instalación de barreras perimetrales o Obligación de poner certificado SSL en la web si se recaban datos a través de ella

Política de Seguridad:

PARTE GENERAL

Esta Parte General de la Política de Seguridad debe ser entregada a todas las personas que tratan datos personales en la entidad, así como al personal de empresas externas que tengan acceso a datos y presten sus servicios presencialmente en las instalaciones de la Entidad o mediante conexión remota.

No obstante, el Capítulo 7 sólo deberá entregarse a aquellos empleados que traten datos personales en régimen de movilidad o teletrabajo.

Capítulo 1.- Conceptos básicos

1.1. Objeto

La presente Política de Seguridad describe las medidas que deben aplicarse en CENTRO ASOCIADO A LA UNED EN MADRID (en adelante, la Entidad) para evitar la alteración o pérdida de los datos personales o su tratamiento o acceso no autorizados.

El cumplimiento de esta Política de Seguridad es obligatorio para todas las personas que tratan datos personales en la Entidad, así como para el personal de empresas externas que tengan acceso a datos y presten sus servicios presencialmente en las instalaciones de la Entidad o mediante conexión remota.

Las medidas de seguridad definidas en este documento son resultado del Análisis de Riesgos efectuado al efecto.

1.2. Definición de datos personales

Dato personal es cualquier información concerniente a personas físicas, identificadas o identificables. Por tanto, no son datos personales los datos de personas jurídicas (sociedades mercantiles, instituciones, etc.).

1.3. Relación del Personal

Responsable del Tratamiento de los Datos:

Es quien decide sobre los fines y los medios del tratamiento de los datos. A efectos de esta Política, es Responsable del Tratamiento:

Identificación		NIF
CENTRO ASOCIADO A LA UNED EN MADRID		Q-2802102-J
Domicilio	C/ Tribulete 14 28012-Madrid (España)	

Asimismo, existen las siguientes sedes CAMA:

- Madrid Capital

  Gregorio Marañón

  Jacinto Verdaguer

  Las Tablas

- Madrid Periferia

  Las Rozas

Arganda del Rey

Rivas Vaciamadrid

San Martín de Valdeiglesias

Colmenar Viejo

San Sebastián de los Reyes

Coslada

Torrejón de Ardoz

Collado Villaba

Pozuelo de Alarcón

Contacto de Seguridad:

Es la persona que, dentro de la entidad, tiene la función de coordinar y controlar la aplicación y efectividad de las medidas técnicas y organizativas establecidas para el cumplimiento de la normativa sobre protección de datos personales. El Contacto de Seguridad es:

Identificación del Contacto de Seguridad
D. Antonio Crespo León
E-mail del Contacto de Seguridad
subdirector.cyt@madrid.uned.es

Usuarios:

Personas autorizadas para acceder a datos personales de la Entidad o responsabilidad de sus clientes.

La relación de usuarios y los permisos de acceso concedidos a cada uno de ellos figuran en el Directorio Activo de Windows, pudiendo extraerse de este el listado.

Delegado de Protección de Datos (DPD):

Es la persona que tiene la función de supervisar el cumplimiento de la normativa sobre protección de datos personales y actuar como punto de contacto entre la Entidad y los interesados y entre aquella y la autoridad de control (Agencia Española de Protección de Datos).

Todos los usuarios deben contactar con el DPD para atender los asuntos que surjan en relación con la privacidad, así como consultarle antes de realizar cualquier nuevo tratamiento de datos personales o desarrollar productos o servicios nuevos que impliquen dicho tratamiento.

Se incluyen a continuación los datos del Delegado de Protección de Datos de la Entidad:

Identificación del Delegado de Protección de Datos
Picón y Asociados Derecho y Nuevas Tecnologías, S.L.
E-mail de contacto del Delegado de Protección de Datos
dpd@piconyasociados.es

1.4. Tratamientos de datos a los que se aplica la Política de Seguridad

La presente Política de Seguridad se aplica a los tratamientos de datos personales que se realizan en la Entidad, ya informáticamente, ya en papel.

Las medidas de seguridad deben también cumplirse con respecto a los ficheros temporales o copias de documentos creados exclusivamente para realizar trabajos temporales. Los ficheros o documentos temporales han de ser destruidos por el usuario cuando hayan dejado de ser necesarios para los fines que motivaron su creación.

La Entidad realiza, como responsable, los tratamientos de datos personales que constan en el Registro de Actividades del Tratamiento que figura en el **ANEXO** a la **Política de Protección de Datos Personales**.

Adicionalmente, la Entidad, realiza, como encargada del tratamiento de sus clientes (UNED Sede Central), los tratamientos de datos personales que constan en dicho **ANEXO**.

1.5. Descripción del software utilizado en el tratamiento de datos

Se utilizan los siguientes programas:

- **Genéricas de UNED Central**:
  - "Akademos" (aplicación informática de gestión de los datos académicos de estudiantes y de los profesores tutores).
  - "Alma"" (aplicación informática de datos de estudiantes para control de préstamos de libros en bibliotecas).
  - "Valija Virtual" (aplicación informática de gestión de exámenes de alumnos).
  - "Quid" (aplicación informática de desarrollo de actividades relacionadas con el COIE).
  - Webex (aplicación informática destinada a la llevanza de los diversos trámites relativos a la extensión universitaria, los cursos de verano y UNED Senior).
- **Propias del CAMA**:
  - "Biblex": (aplicación de gestión de los usuarios externos de bibliotecas).
  - "Apliman" (aplicación informática en desarrollo - Contabilidad y datos de filiación de Tutores y PAS).
  - "DeltaNómina" (aplicación informática destinada a cálculo de IRPF y deducción).
  - "Verisure" (aplicación informática destinada a la gestión y al tratamiento de las imágenes captadas por el sistema de videovigilancia.

- "Microsoft OFFICE 365": Paquetes de aplicaciones ofimáticas, integrados por procesador de textos (Word), hoja de cálculo (Excel), base de datos (Access) y PowerPoint (Presentaciones) y entorno Cloud.

1.6. Nuevas actividades de tratamiento de datos

Los usuarios deben **consultar previamente al DPD** cuando, en el desempeño de sus funciones, necesiten realizar las siguientes actividades:

- Tratar datos personales distintos de los que figuran en el Registro de Actividades del Tratamiento de la entidad o para finalidades diferentes de las indicadas en él.

- Tratar datos personales en el disco duro del propio ordenador personal del usuario, en un disco duro de un ordenador distinto de los destinados a ello, en otro dispositivo electrónico o mediante computación en nube.

- Instalar una nueva aplicación informática que utilice datos personales o desinstalar o alterar una ya existente.

Capítulo 2.- Controles de Acceso a la Información y Confidencialidad

2.1. Objeto

Este Apartado describe los controles existentes para que cada usuario acceda únicamente a los datos y recursos que necesite para el desempeño de sus funciones.

2.2. Reglas generales

Se debe evitar el acceso de personas no autorizadas a los datos personales.

A tal fin, se evitará dejar los datos expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), incluyendo las pantallas que se utilicen para la visualización de imágenes captadas por las cámaras.

No se comunicarán datos personales a terceros, prestando especial atención en no divulgar datos personales durante las conversaciones telefónicas, en correos electrónicos, etc.

Los deberes de confidencialidad y secreto subsisten aún después de finalizada la relación entre el usuario y la empresa.

2.3. Contraseñas

El mecanismo de identificación y autenticación utilizado en el tratamiento automatizado de los datos personales es el de usuario y contraseña.

La generación inicial de una contraseña la hará el Contacto de Seguridad, quien la comunicará confidencialmente a cada usuario. El cambio de contraseñas será realizado por el propio usuario, cada vez que el sistema lo exija.

Las contraseñas tendrán un mínimo de 10 caracteres y estarán integradas por números, letras (mayúsculas y minúsculas) y símbolos.

Cada identificador y contraseña debe ser tratado por los usuarios como información **confidencial, personal e intransferible** y no podrán ser revelados a terceros, ni siquiera a compañeros de trabajo.

Si un usuario necesita acceder a datos o correos electrónicos a los que no tenga acceso, debe comunicarlo al Contacto de Seguridad, quien, si lo considera justificado, podrá facilitarle el acceso. En ningún caso dos usuarios podrán compartir sus contraseñas para acceder de manera conjunta a los datos personales.

En caso de que la confidencialidad de una contraseña pudiera verse comprometida, se deberá poner inmediatamente en conocimiento del Contacto de Seguridad.

No está permitido apuntar los identificadores y contraseñas, ni en papel, ni en soporte electrónico.

Cuando un usuario se ausente del puesto de trabajo, procederá al bloqueo de la pantalla o al cierre de la sesión.

No está permitido utilizar los ordenadores del trabajo para fines personales. En caso de que, excepcionalmente, sea necesario, se deberá disponer de perfiles de usuario distintos para cada una de las finalidades.

2.4. Accesos en remoto

En caso de que existan accesos al sistema de tratamiento de datos a través de redes de comunicaciones electrónicas o en remoto, se deberán aplicar en ellos las mismas medidas de seguridad que en los accesos locales.

2.5. Controles de acceso a la información en papel

A los documentos en papel que contengan datos personales únicamente podrán acceder los usuarios que lo necesiten para desempeñar sus funciones, de conformidad con los permisos que cada uno tenga autorizados. El resto de usuarios tienen prohibido el acceso a estos documentos.

Si un usuario necesita tratar documentos con datos personales, pero no tiene permiso para ello, debe solicitar la autorización previa del Contacto de Seguridad.

2.6. Control de acceso físico

Las medidas de seguridad físicas juegan un papel tan importante como las medidas técnicas, en tanto que protegen los sistemas de un acceso físico no autorizado.

En este sentido, la empresa valorará la conveniencia de establecer sistemas de identificación del personal, definición de áreas de acceso restringido, sistemas de detección de intrusos o la instalación de barreras perimetrales, debiendo los usuarios respetar dichas medidas, en su caso.

Sólo el personal de informática podrá acceder a los lugares donde se encuentren ubicados los equipos físicos que dan soporte al sistema informático con el que se tratan dichos datos. El acceso a dicho lugar se encuentra limitado mediante llave, huella dactilar o mecanismo equivalente. El acceso a dichos locales por personas distintas debe efectuarse siempre bajo el control del Contacto de Seguridad.

Capítulo 3: Gestión de soportes informáticos y documentos

3.1. Objeto

Este Apartado describe las condiciones en las que pueden utilizarse soportes informáticos portátiles – CDs, memorias portátiles, discos duros externos, ordenadores portátiles, etc. – y documentos en papel que contengan datos personales.

3.2. Medidas aplicables a todos los soportes y documentos

Las medidas de seguridad contenidas en este apartado deben aplicarse tanto a soportes informáticos como a documentos en papel, siempre que contengan datos personales.

3.2.1. Almacenamiento de soportes y documentos

Mientras no se esté trabajando con ellos, los usuarios deben guardar los soportes y documentos con datos personales en estancias, armarios, cajones u otros dispositivos que dispongan de cerradura con llave o mecanismo equivalente, de modo que sólo él o, en su caso, el resto de personas autorizadas, puedan acceder a ellos.

3.2.2. Borrado de datos. Desechado de documentos y soportes

El fin último en la destrucción o retirada de los dispositivos y soportes que contienen datos personales debe ser un borrado irreversible de los datos, para que no puedan ser recuperados.

Quien vaya a desechar documentos o soportes que contengan datos personales, debe, previamente, destruirlos o borrarlos, cumpliendo las siguientes premisas:

1. El usuario guardará reservadamente el documento o soporte hasta que lleve a cabo el borrado o destrucción.

2. La destrucción o borrado deben tener como resultado necesario la imposibilidad de acceder o reconstruir, siquiera parcialmente, la información.

3. Siempre que se cumpla el objetivo anterior, la destrucción se podrá hacer por medios manuales o, en su caso, por los medios mecánicos que la Entidad ponga a disposición de los usuarios.

4. Queda terminantemente prohibido depositar soportes o documentos no destruidos o borrados en la vía pública o lugares accesibles a personas no autorizadas.

Se recomienda seguir los siguientes procedimientos de destrucción o borrado, conforme a los estándares internacionales generalmente reconocidos:

SOPORTE	PROCEDIMIENTO	
Papel o microfilm	Destruir	Trituradora en tiras o cuadrados de 2mm
Móviles y PDAs	Borrar manualmente	Agenda, mensajes, llamadas y resetear a la configuración de fábrica
Routers	Borrar manualmente	Tablas de encaminamiento, registros de actividad, cuentas de administración y resetear a la configuración de fábrica
Impresoras y faxes	Borrar manualmente	Resetear a la configuración de fábrica
Discos reescribibles	Formatear	Formateo de bajo nivel
Discos de solo lectura	Destruir	Trituradora: 5mm
Discos virtuales cifrados	Además de lo anterior	Destruir las claves

El usuario que tenga conocimiento de la existencia de soportes o documentos que, debiendo ser destruidos o borrados, no lo hayan sido, lo comunicará de inmediato al Contacto de Seguridad, para que adopte las medidas oportunas para la destrucción.

3.3. Medidas especiales aplicables a documentos en papel

Además de las medidas previstas en el Apartado 3.2 anterior, cuando se traten documentos en papel que contengan datos personales, deben cumplirse las siguientes:

3.3.1. Documentos en tramitación o revisión

Durante el tiempo en que, por estar en revisión o tramitación, anterior o posterior a su archivo, los documentos con datos personales no se encuentren almacenados en las condiciones previstas en el Apartado 3.2.1, la persona que esté a su cargo los mantendrá permanentemente en su poder y bajo su vigilancia y control, impidiendo a terceros no autorizados acceder a ellos. El resto del tiempo, los documentos permanecerán guardados en los lugares mencionados en el apartado 3.2.1

Siempre que un usuario haya de imprimir documentos que incluyan datos personales, debe tener en cuenta las siguientes medidas:

- Supervisará el proceso, con el fin de impedir que personas no autorizadas puedan visualizar los datos mientras se realiza la impresión.
- Retirará los documentos de la impresora en cuanto sea posible y los guardará en un lugar seguro.

3.3.2. Ubicación de archivadores con datos de riesgo elevado

Los archivadores en los que se almacenen los documentos con datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento) deben ubicarse en un área que disponga de puerta con llave propia o sistema equivalente. Dicha área debe permanecer cerrada mientras no sea necesario acceder a los documentos.

3.3.3. Copias o reproducciones de documentos con datos de riesgo elevado

Las copias o reproducciones de los documentos con datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento) deben realizarse siempre con autorización del Contacto de Seguridad.

Cuando este tipo de documentos se trasladen, deben adoptarse las medidas necesarias para impedir el acceso indebido o la manipulación de la información.

En todo caso, si un usuario tuviera conocimiento de la existencia de documentos en papel con datos personales con respecto a los que no se cumplan las medidas de seguridad previstas en este Apartado 3.3 lo comunicará de inmediato al Contacto de Seguridad, para que adopte las medidas oportunas.

3.4. Medidas especiales aplicables a soportes informáticos

3.4.1. Usos permitidos de soportes informáticos

Como regla general, no está permitida a los usuarios la grabación de datos personales en soportes físicos o informáticos portátiles – CDs, memorias portátiles, discos duros externos, ordenadores portátiles, etc. –. Únicamente podrán tratar dichos datos en soporte papel y sólo si ello es necesario para el desempeño de sus funciones.

Excepcionalmente, se permite la grabación o utilización de datos personales en soportes informáticos portátiles cuando el usuario, necesitándolo para desempeñar sus funciones, solicite y obtenga una autorización del Contacto de Seguridad.

Adicionalmente, se podrán grabar datos personales en soportes informáticos portátiles en los siguientes supuestos:

a) Para la realización de copias de seguridad, por las personas encargadas de hacerlo.
b) La grabación de datos mediante las cámaras del sistema de videovigilancia.
c) Los usuarios que hayan sido autorizados para utilizar ordenadores portátiles, agendas electrónicas, tablets o dispositivos análogos.
d) Para hacer entrega a los clientes de datos personales de estos tratados en la prestación de servicios por la Entidad.
e) Cuando el soporte informático haya sido entregado por los clientes y se mantenga el tiempo mínimo imprescindible para realizar el trabajo para el que fue entregado.

3.4.2. Cifrado de los datos

La salida de soportes – CDs, memorias portátiles, discos duros externos, ordenadores portátiles, etc. – que contengan datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento) se realizará cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada.

El tratamiento de datos cuyo tratamiento implique un riesgo elevado mediante soportes portátiles fuera de las instalaciones de la Entidad debe hacerse también cifrando los datos.

No se podrán enviar datos cuyo tratamiento implique un riesgo elevado por medios telemáticos (e-mail, Internet, etc.) sin autorización expresa del Contacto de Seguridad. Además, antes de efectuar cualquier comunicación de dichos datos mediante redes de telecomunicaciones, también deberá cifrarse la información.

En todo caso, se valorará la posibilidad de proceder al cifrado de datos personales con carácter previo a que salgan de las instalaciones de la entidad en soporte informático, aun cuando, por la naturaleza de los datos personales enviados y resto de circunstancias concurrentes, no exista un riesgo elevado.

Capítulo 4: Gestión de brechas de seguridad

4.1. Objeto

Este apartado describe la forma de actuar en caso de que se produzca una brecha de la seguridad que afecte o pueda afectar a los datos personales.

Una brecha de seguridad es todo quebranto de la seguridad que ocasione o pueda ocasionar la destrucción, pérdida o alteración accidental o ilícita de datos personales tratados o la comunicación o acceso no autorizados a dichos datos. Por ejemplo, si se produjese una incidencia informática (virus, hacker, etc.) que pusiese en peligro la confidencialidad, integridad o disponibilidad de los datos personales.

4.2. Desarrollo

Todos los usuarios tienen la obligación de comunicar al Contacto de Seguridad, lo antes posible, cualquier anomalía o evento que observen y que en su ejecución o desarrollo pueda afectar a la seguridad de los datos personales, cualquiera que sea el soporte en que estos se encuentren, informático o en papel.

A tal fin, cuando un usuario detecte una brecha de seguridad de los datos personales (potencial o consumada), debe comunicarlo de modo inmediato al Contacto de Seguridad, con toda la información que conozca hasta ese momento.

Salvo que, excepcionalmente, las circunstancias lo impidan, la comunicación al Contacto de Seguridad se efectuará por correo electrónico con acuse de recibo, incluyendo la siguiente información:

- Nombre, apellidos y puesto de la persona que efectúa la notificación.
- En qué ha consistido la posible brecha de seguridad.
- Fecha y hora en la que fue detectada.
- Cuáles han sido sus efectos, potenciales o consumados.
- Toda la información complementaria que se considere de interés.

El e-mail se remitirá con acuse de recibo, que deberá ser confirmado por el destinatario y conservado por el remitente como prueba del envío.

Capítulo 5: Protección de las comunicaciones

5.1. Uso del correo electrónico

El uso del correo electrónico queda limitado, estrictamente, al cumplimiento de las tareas laborales o profesionales que el usuario tenga asignadas, no pudiendo utilizarse para fines privados.

Se utilizará el correo electrónico corporativo, evitando, salvo que resulte imprescindible, el uso de otras cuentas de correo distintas.

5.2. Confidencialidad de los destinatarios del correo electrónico

Cuando se envíe un e-mail a varios destinatarios simultáneamente, para evitar que las direcciones de correo electrónico de cada uno de ellos sean visibles para los demás, dichas direcciones se incluirán siempre en el campo "CCO" (con copia oculta) del programa gestor de correo y nunca en el campo "Para", ni en el campo "CC" (con copia).

5.3. Limpieza de los documentos

Cuando un documento electrónico deba ser enviado fuera de las instalaciones de la empresa, previamente, se debe retirar de él toda la información contenida en campos ocultos, meta-datos, comentarios, revisiones anteriores, etc. salvo cuando dicha información sea pertinente para el receptor del documento. En los siguientes links se explica cómo eliminar esta información:

- Documentos Office: https://support.office.com/es-es/article/quitar-datos-ocultos-e-informaci%C3%B3n-personal-mediante-la-inspecci%C3%B3n-de-documentos-presentaciones-o-libros-356b7b5d-77af-44fe-a07f-9aa4d085966f
- Documentos Adobe: https://helpx.adobe.com/es/acrobat/using/pdf-properties-metadata.html#edit_document_metadata

Esta medida es especialmente relevante cuando el documento vaya a difundirse ampliamente o entre varias personas.

5.4. Cifrado de datos

Cuando se envíen datos personales a través de redes de telecomunicaciones (por ejemplo, a través del correo electrónico), el usuario deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información. En caso de que valore que es conveniente cifrar los datos, procederá al cifrado por sí mismo o con la asistencia del Contacto de Seguridad.

El servidor en el que se aloja la página web debe tener instalado un certificado SSL (Secure Sockets Layer). Ello asegura que la comunicación de datos personales a través de la web se hace de forma fiable, garantizando a los usuarios la identidad del sitio web y cifrando la información transmitida.

En todo caso, será obligatorio el previo cifrado de los datos cuyo tratamiento implique un riesgo elevado (conforme a lo previsto en el Registro de Actividades de Tratamiento).

Capítulo 6. Protección frente a código dañino y phishing

Se considera **código dañino** los virus, los gusanos, los troyanos, los programas espías, «spyware» y, en general, todo lo conocido como «**malware**».

El **phishing** es una técnica engañosa utilizada por los delincuentes para obtener información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por una comunicación confiable y legítima.

Para prevenir estos ataques, antes de abrir correos electrónicos, ejecutar archivos informáticos o pulsar hipervínculos, los usuarios se asegurarán de los siguientes extremos:

- Que dichas acciones estén relacionadas con el ejercicio de sus funciones laborales.
- Que se identifique correctamente al remitente.

Los usuarios deben estar atentos a cualquier indicio de que en el sistema informático haya podido instalarse código dañino. Ante dicha sospecha, el usuario, como primera medida de prevención, desconectará el equipo de la red y lo apagará, comunicando inmediatamente la situación al Contacto de Seguridad para que se adopten las actuaciones oportunas.

Capítulo 7: Tratamiento de datos personales en régimen de movilidad o teletrabajo

Los Usuarios que traten datos personales fuera de la oficina, en situación de movilidad o teletrabajo,[1] además de observar las medidas generales descritas en esta Política de Seguridad, deberán cumplir las siguientes:

a) <u>Protección de los dispositivos y del acceso a ellos:</u>

- Se deben utilizar contraseñas de acceso diferentes a las utilizadas para acceder a cuentas de correo personal, redes sociales y otro tipo de aplicaciones utilizadas por el Usuario en su vida personal.

[1] Algunos de los riesgos derivados de dicha situación son la pérdida o deterioro de los datos por catástrofes físicas (incendio, inundación, derrumbe del edificio, etc.), robo o extravío del dispositivo, limitaciones en la posibilidad de acceder a los datos por la caída de Internet, la falta de sincronización con la plataforma matriz en la que se alojan los datos, los daños en el dispositivo de acceso por la intervención de otras personas que residan con el Usuario o por descuidos (como la caída de bebidas o alimentos), el robo de credenciales o el conocimiento indebido de ellas por terceros, el empleo del dispositivo por personas no autorizadas, el uso de conexiones a internet no seguras (redes wi-fi públicas), la visualización de los datos por personas no autorizadas (otras personas que convivan con el Usuario o terceros, en estaciones de tren o aeropuertos), hacking/cracking o instalación de aplicaciones maliciosas por falta de actualización del sistema operativo o de las aplicaciones, por no instalación o actualización de antivirus o por ausencia de firewall, conexión mediante equipos no autorizados por la compañía, etc. Todos estos riesgos pueden materializarse en incidencias que afecten a la confidencialidad, integridad o disponibilidad de los datos personales, por lo que deben ser prevenidos.

- No se deben descargar ni instalar aplicaciones que no hayan sido previamente autorizadas por la Entidad.
- Se debe evitar la conexión de los dispositivos a la red corporativa desde lugares públicos, así como la conexión a redes WI-FI abiertas no seguras.
- Si se dispone de un equipo corporativo, no se debe utilizar con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
- Si el equipo utilizado es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.
- El antivirus instalado en el equipo debe estar operativo y actualizado.
- Siempre ha de verificarse la legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico del que procede es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal.
- Si pueden ser gestionadas por el Usuario, conviene desactivar las conexiones WI-FI, bluetooth y similares que no estén siendo utilizadas.
- Una vez concluida la jornada de trabajo, debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

b) Protección de la información

- Tanto en lugares públicos como en el entorno doméstico, deben adoptarse las precauciones necesarias para garantizar la confidencialidad de los datos personales.
- Si se genera y trabaja con papel durante situaciones de movilidad, es importante minimizar o evitar la entrada y salida de documentación y extremar las precauciones para evitar accesos no autorizados por parte de terceros.
- La información en soporte papel, incluyendo borradores, no se puede desechar sin garantizar que es adecuadamente destruida. No arrojar papeles con datos personales, enteros o en trozos, en papeleras de hoteles, lugares públicos o en la basura doméstica.
- Hay que extremar las precauciones para evitar el acceso no autorizado a los datos personales, no dejando a la vista ningún soporte que los contenga en el lugar donde se desarrolle el teletrabajo y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos.
- Se debe evitar exponer la pantalla a la mirada de terceros. Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.
- En la medida de lo posible, se debe prevenir que se puedan escuchar conversaciones por parte de terceros, utilizando, por ejemplo, auriculares o retirándose a un espacio en el que el Usuario no esté acompañado.

c) Almacenamiento de la información

- Se evitará almacenar los datos personales de forma local en el dispositivo utilizado, salvo situaciones excepcionales. Se deben utilizar los recursos de almacenamiento compartidos o en la nube proporcionados por la Entidad, que son los siguientes: One Drive.

- No se debe bloquear o deshabilitar la política de copia de seguridad corporativa definida para cada dispositivo.
- Es recomendable revisar y eliminar periódicamente la información residual que pueda quedar almacenada en el dispositivo, como archivos temporales del navegador o descargas de documentos.

Se informa a los Usuarios de que se encuentra instalado un sistema de monitorización de la actividad para identificar patrones anormales de comportamiento en el tráfico de red, con el objetivo de evitar la propagación de malware por la red corporativa y el acceso y uso no autorizado de recursos. Asimismo, dicho sistema es utilizado por la Entidad para supervisar el correcto desempeño por el Usuario de sus tareas y obligaciones, en el marco de las funciones de control previstas en el Estatuto de los Trabajadores, que se ejercerán dentro de las condiciones legales y con los límites inherentes a ellas.