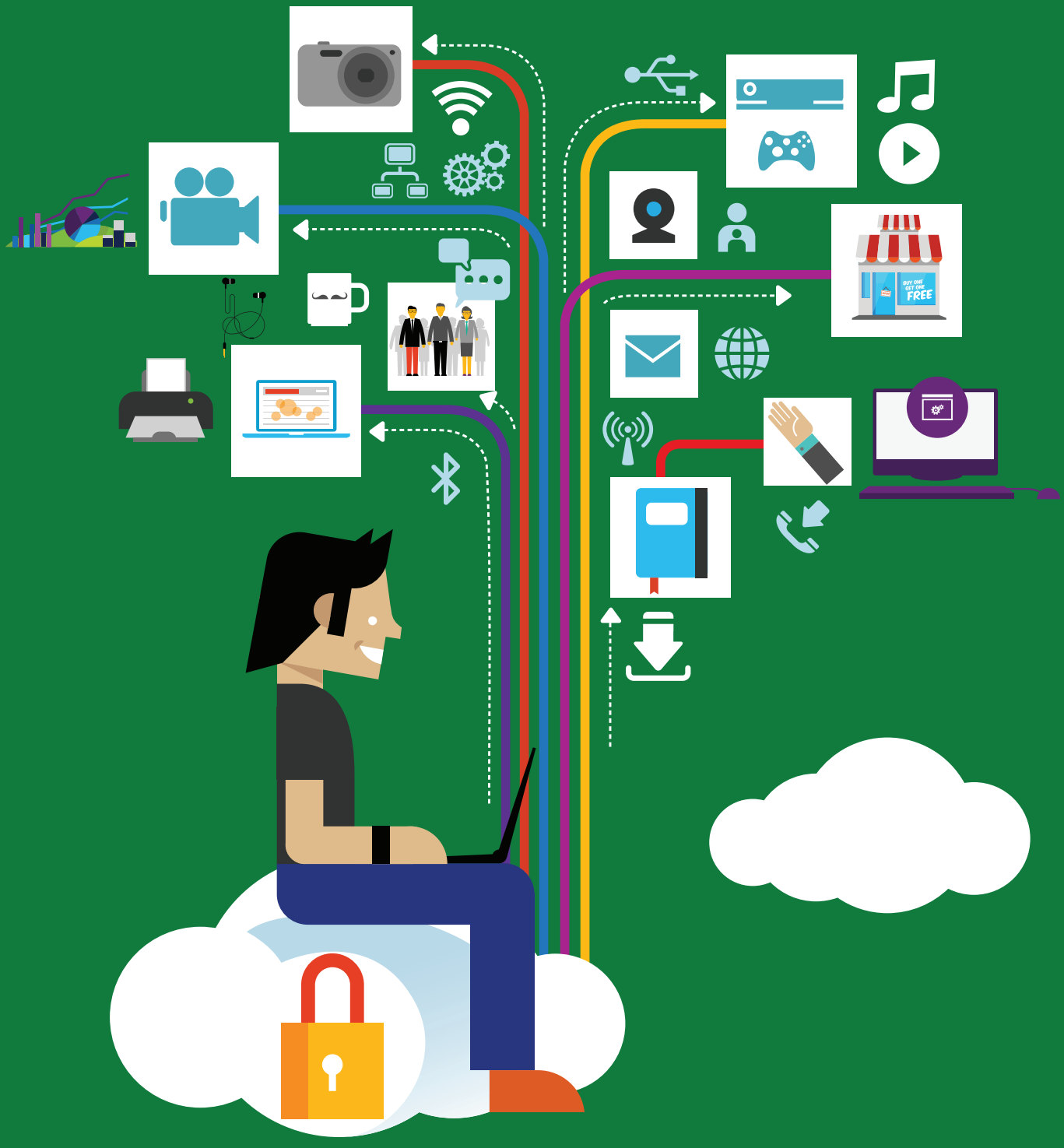
Microsoft



Manual en materia de seguridad de los datos personales y otra información basada en un entorno Microsoft® para MiPyMEs y organizaciones pequeñas mexicanas

Publicado por:
Microsoft México, S. de R.L. de C.V.
Ave. Vasco de Quiroga 1700, Centro de Ciudad Santa Fe, México D.F. 01210
www.microsoft.com/es-mx/default.aspx

Noviembre de 2015

Agradecimiento: Microsoft México agradece a Miguel Recio Gayo su colaboración en esta publicación.

Distribución gratuita

Aviso Legal:
Los autores de esta publicación no son responsables de que lo contenido en la misma garantice el cumplimiento de los requisitos establecidos en la normatividad mexicana sobre protección de datos personales, de manera que corresponde al destinatario de la misma adoptar las medidas necesarias en cada caso para garantizar dicho cumplimiento. Esta publicación tiene un objeto meramente informativo en relación con la normatividad mexicana sobre protección de datos personales, lo que no exime que el destinatario tenga que buscar, en su caso, ayuda legal y/o tecnológica para el cumplimiento de sus obligaciones en materia de protección de datos personales y seguridad.

La implementación de las medidas de seguridad en el entorno Microsoft a que hace referencia este Manual, no garantizan el cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento u otra normatividad aplicable, el cual es responsabilidad exclusiva de los sujetos obligados bajo dichas disposiciones. El presente Manual es únicamente un instrumento de referencia para coadyuvar con los responsables a cumplir su deber de seguridad.

Contenido

Prólogo

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se congratula de que una empresa como Microsoft México haya preparado una publicación como la presente, dirigida a las MiPyMEs y organizaciones pequeñas mexicanas, para ayudarlas en la adopción e implementación de medidas de seguridad en un entorno Microsoft. Más aún, el hecho de que Microsoft haya tenido como referencia el Manual en materia de seguridad de datos personales para MiPyMEs y organizaciones pequeñas que fue publicado por el INAI, es una buena muestra de que la colaboración público-privada es posible de muy diferentes formas y siempre en beneficio de las organizaciones que tratan datos personales. Es así que este Manual, el primero que se publica teniendo como referencia el del INAI, servirá a quienes tratan datos personales para conocer cómo la tecnología de Microsoft puede ayudar a adoptar controles de seguridad, incluidas las últimas versiones como Windows 10 y el cómputo en la nube.

La seguridad de los datos personales, a través del uso de la tecnología e implementación de medidas de seguridad, es uno de los deberes torales previstos en la normatividad sobre protección de datos personales para proteger a la persona, titular de los datos y del derecho humano a la protección de datos personales. Al guiar a las MiPyMES, casi paso a paso en diversos parámetros de configuración de varias funcionalidades de Windows, desde Windows 7 hasta Windows 10, y explicar las características de seguridad de servicios de cómputo en la nube, como OneDrive, Office 365 y Azure, Microsoft ayuda a los responsables del tratamiento a cumplir con su deber de seguridad así como a los encargados del tratamiento; además de facilitar la labor del INAI de proporcionar apoyo técnico a quienes tratan datos personales al poder contar con este Manual.

El Manual en materia de seguridad que Microsoft México ha elaborado pretende ser también un instrumento de referencia y utilidad en el día a día de las MiPyMEs que utilizan entornos tecnológicos Microsoft, ya que la seguridad implica, de manera continua, revisar las medidas ya adoptadas e implementadas, identificar, en su caso, las faltantes, así como actualizarlas y mejorarlas en lo posible. Para ello, el Manual incluye también listas de comprobación (check lists), consejos prácticos y otra información, en forma de anexos, para que quien haga uso del mismo pueda encontrar más detalles disponibles tanto en sitios y páginas web de Microsoft como del propio INAI.

En definitiva, se trata de una publicación que es bienvenida por el INAI y que será de utilidad para los sujetos obligados, ayudándoles así en la adopción de medidas de seguridad que sirvan para proteger los datos personales y fomentar al mismo tiempo el respeto al derecho humano a la protección de datos personales. Finalmente, es destacable que Microsoft México distribuya este Manual de forma gratuita, ayudando así a que los interesados puedan acceder al mismo y promoviendo también con ello la seguridad de los datos personales y la información en nuestro país.

Mtro. Luis Gustavo Parra Noriega
Coordinador de Protección de Datos Personales
Instituto Nacional de Transparencia, Acceso a la Información y
Protección de Datos Personales (INAI)

Abreviaturas

Art(s).	Artículo(s)
CURP	Clave Única de Registro de Población
DOF	Diario Oficial de la Federación
etc.	Etcétera
GB	Gigabyte (1 GB= 1,024 MB)
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Manual del INAI	Manual en materia de seguridad de datos personales para MiPyYMEs y organizaciones pequeñas (Julio 2014)
MiPyMEs	Microempresa, pequeña y mediana empresa
N/A	No Aplicable
PC	Personal Computer (equipo de cómputo)
Reglamento de la LFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

1. ¿Por qué y cómo usar este manual en materia de seguridad?

Sin seguridad no hay privacidad y la protección de datos personales se basa en ambas. Es por ello que Microsoft, líder mundial en el desarrollo de software y servicios tecnológicos, como el cómputo en la nube, ha desarrollado este manual de seguridad basada en un entorno Microsoft para MiPyMEs mexicanas, teniendo en consideración el Manual en materia de seguridad de datos personales para MiPyMEs y organizaciones pequeñas publicado por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos (en adelante, INAI), en julio de 2014.

Se trata, por tanto, de un manual de seguridad dirigido a MiPyMEs sujetas a la normatividad sobre protección de datos personales en México, ya sean éstas responsables o encargadas del tratamiento.

El manual de seguridad para MiPyMEs tiene por objeto ofrecerles una guía que, atendiendo a las posibilidades que les facilitan tanto los productos de Microsoft como su configuración, les permitan adoptar medidas para proteger los datos personales y otra información corporativa que requiere de protección.

A tal fin, el manual se divide en varios apartados, que a su vez contienen en su caso varias secciones, cada uno de los cuales tiene por objeto ofrecer información sobre la seguridad y las medidas a adoptar para proteger los datos personales y otra información a través del uso de software y tecnología de Microsoft.

Es así que, en primer lugar, se presenta este manual en materia de seguridad basada en un entorno Microsoft para MiPyMEs mexicanas, poniendo el foco especialmente en algunos pasos clave en la adopción y mantenimiento de medidas de seguridad, los productos o servicios que Microsoft ofrece para tal fin y que ayudarán a proteger su equipo de cómputo, dispositivo electrónico y los datos personales u otra información, así como, por su relevancia, los productos antivirus y antimalware que Microsoft ofrece gratuitamente y que son Microsoft Security Essentials (para Windows 7 y Windows Vista) y Microsoft Defender (para Windows 8, Windows RT, Windows 8.1, Windows RT 8.1 y Windows 10).

Este primer apartado se completa también con una relación más detallada sobre las herramientas o funciones que ofrece Windows, en sus diferentes versiones del sistema operativo; la correspondiente medida de seguridad; la referencia al Manual del INAI, ya mencionado, y la descripción aplicable en su caso.

A continuación, el apartado más extenso del manual está dedicado a presentar las medidas de seguridad más relevantes que todo responsable o, en su caso, encargado del tratamiento tiene que cumplir conforme a la normatividad aplicable en México y cómo, a través del uso de productos o servicios de Microsoft, es posible cumplir con las mismas. En la elaboración de este apartado se han tenido en consideración, en particular, las medidas de seguridad en el entorno de trabajo digital descritas en el Manual del INAI al que ya se ha hecho referencia.

En su caso, el cómputo en la nube (en inglés, *cloud computing*) es una oportunidad para las empresas y las MiPyMEs, por lo que no deben ignorarlo. En este sentido, Microsoft pone a su alcance la posibilidad de hacer uso del mismo, y por tanto de beneficiarse de las ventajas que éste representa, a través de productos como OneDrive, Microsoft Office 365 y Microsoft Azure.

Además, el cómputo en la nube permite a las MiPyMEs encomendar a proveedores como Microsoft, el tratamiento de sus datos personales haciendo uso de un servicio que, en el caso de Microsoft, cumple con altos estándares en seguridad, privacidad y protección de datos personales, transparencia y cumplimiento continuo.

Además, con la lista de comprobación o *checklist* Microsoft quiere ayudar a las MiPyMEs y otras organizaciones a que puedan revisar o, en su caso, considerar la adopción de algunas medidas de seguridad importantes para proteger el derecho humano a la protección de datos personales. En concreto, se incluye una lista de comprobación para que quien lo considere oportuno auto-verifique si ha implementado algunas medidas de seguridad relevantes y, en su caso, evalúe la posibilidad de mejorarlas, así como una lista de comprobación genérica de medidas de seguridad en función de las posibilidades que ofrecen Windows 8.1, Windows RT 8.1 y Windows 10.

También se proporcionan algunos consejos prácticos para proteger equipos de cómputo o dispositivos contra virus y otras amenazas a la privacidad y la protección de datos personales.

En el último apartado se incluyen varios anexos que tienen por objeto, por una parte, presentar algunos conceptos básicos tanto en materia de protección de datos personales, siguiendo a tal fin las definiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento, así como otras definiciones técnicas, como por ejemplo las de *botnet*, muro de protección *(firewall)* o robo (o suplantación) de identidad. Por otra parte, se incluye también una referencia a otros sitios, del INAI, del Diario Oficial de la Federación (DOF) o de Microsoft, dónde se puede encontrar más información sobre protección de datos personales y seguridad en caso de que los destinatarios de este manual quieran ampliar sus conocimientos en la materia o encontrar más recursos de información y/o herramientas para adoptar medidas de seguridad adicionales que permitan aumentar el nivel de seguridad aplicable a los datos personales y otra información.

En definitiva, con esta publicación, Microsoft México quiere facilitar a responsables y encargados del tratamiento de datos personales un documento de referencia que pueda serles de utilidad en la práctica para la implementación de las medidas de seguridad para el entorno digital a las que hace referencia el Manual en materia de seguridad de datos personales para MiPyMEs y organizaciones pequeñas, del INAI. Por tanto, Microsoft México quiere ayudar a quienes día a día tienen que implementar medidas de seguridad facilitando su labor a la hora de asegurar el derecho humano a la protección de datos personales y, de esta manera, contribuir también al desarrollo de una cultura en materia de protección de datos personales, seguridad y ciberseguridad.

2. Microsoft le ayuda a cumplir con el deber de seguridad para la protección de los datos personales

2.1. ¿Por qué adoptar y mantener medidas de seguridad?

Los sistemas de tratamiento de datos personales, el equipo de cómputo y otros dispositivos de almacenamiento de información en general, requieren de protección para minimizar distintos riesgos a los que están expuestos.

Estos riesgos consisten en la posibilidad de que se produzcan daños al equipo de cómputo, los dispositivos o los datos personales, o su pérdida, alteración, acceso o uso, destrucción o cualquier tratamiento no autorizado.

Además, el daño puede afectar derechos del titular de los datos personales, que hay que proteger también.

Entre las fuentes de dichos riesgos se encuentran virus u otro software malicioso o personas que buscan un acceso o tratamiento no autorizado, así como eventos naturales tales como inundaciones o terremotos que podrían hacernos perder el equipo de cómputo y/o los datos personales u otra información.

Además, puede haber otras razones para adoptar y mantener medidas de seguridad, de manera que a continuación se presentan algunas de las mismas:

Adoptar y mantener medidas de seguridad para:	
Evitar	• Daño, alteración o modificación, pérdida o destrucción, uso, acceso o cualquier tratamiento no autorizado.
	• Mala reputación frente a clientes, usuarios, empleados socios, accionistas y/o autoridades competentes.
	• Vulneraciones al derecho humano a la protección de datos personales.
	• Sanciones económicas por incumplimiento.
Limitar	• El daño , en caso de que éste se produzca.
Garantizar	• La confidencialidad, la integridad, la autenticación y la trazabilidad.
	• El cumplimiento de la normatividad aplicable en materia de deber de seguridad al negocio o actividad.

La adopción de medidas de seguridad debe llevarse a cabo paso a paso y día a día, manteniéndolas a lo largo del tiempo y a la vista de los riesgos existentes, que pueden cambiar. Es así que a continuación se incluyen algunos pasos que pueden ayudarle a adoptar y mantener medidas de seguridad:

Algunos pasos clave en la adopción y mantenimiento de medidas de seguridad	
1 **Analice qué datos personales trata y/o almacena en equipos de cómputo y/o dispositivos electrónicos**	• Identifique qué datos personales trata, cómo los trata y en qué procesos (obtención, almacenamiento, uso, divulgación y conservación, así como el bloqueo, borrado, eliminación, supresión o destrucción). • Analice si se trata de datos personales sensibles (por ejemplo, estado de salud, creencias religiosas o afiliación sindical) o no.
2 **Identifique y evalúe los riesgos a que están expuestos los datos personales y los daños que podrían causar**	• Evalúe qué riesgos existen, considerando tanto los derivados de acciones humanas, tales como accesos no autorizados, daños o robo, error humano, etc.; o de la naturaleza, tales como inundaciones, terremotos, etc. • Evalúe qué daños podrían producirse para los titulares de los datos personales.
3 **Identifique qué medidas de seguridad tiene y si le falta alguna (análisis de brecha) o si puede mejorar las que tiene**	• Revise qué medidas de seguridad ha adoptado, en su caso, tanto administrativas, como físicas y técnicas. • Identifique si le faltan medidas de seguridad, pudiendo utilizar para ello, por ejemplo, el Manual en materia de seguridad de datos personales para MiPyMEs y organizaciones pequeñas del INAI, la lista de comprobación incluida en este manual u otras guías o instrumentos que considere oportunos.
4 **Analice qué productos o servicios pueden ayudarle a cumplir con las medidas de seguridad o mejorarlas**	• Microsoft le ofrece herramientas, tales como Microsoft Security Essentials y Windows Defender, Windows Update, Firewall de Windows, así como la posibilidad de configurar (activar, modificar y/o desactivar) las características de seguridad del software y las aplicaciones que usa para tratar datos personales. • Combine el uso de herramientas y la configuración de las características de seguridad del software y aplicaciones para aumentar el nivel de seguridad.
5 **Implemente las medidas de seguridad necesarias conforme a un plan de trabajo**	• Elabore un plan de trabajo para implementar las medidas de seguridad necesarias para gestionar el riesgo derivado del tratamiento de los datos personales.
6 **Revise o audite las medidas de seguridad con frecuencia o cada vez que se produzcan cambios relevantes y mantenga actualizado el software**	• Mantenga activadas e implementadas las medidas de seguridad y revise que sean las adecuadas en atención a los riesgos para los datos personales. • Audite las medidas de seguridad implementadas con frecuencia o cuando se lleven a cabo nuevos tratamientos de datos personales, especialmente si son datos sensibles, así como cambios en el sistema de información (equipo de cómputo, dispositivos, uso de servicios de tecnologías de información, etc.). • Compruebe que utiliza versiones de software que cuenten con soporte de actualizaciones de seguridad por parte de su fabricante. Por ejemplo, Windows XP dejó de ser soportado por Microsoft desde abril de 2014, por lo que ya no recibe actualizaciones de seguridad, siendo esto un potencial riesgo que se elimina actualizándose a las últimas versiones del Sistema Operativo (SO) Windows.
7 **Capacite a empleados y/o colaboradores que traten datos personales**	• Brinde capacitación a quienes traten datos personales en su organización sobre qué son las medidas de seguridad y por qué es necesario cumplir con las mismas. • Ofrezca actualizaciones de capacitación a quienes traten datos personales para mantener y ampliar el conocimiento de manera que ello facilite el cumplimiento en materia de protección de datos personales y seguridad.

2.2. Desde Windows 7 hasta Windows 10: Herramientas de Microsoft que le ayudarán a proteger los datos personales en su equipo y dispositivos

Microsoft le ofrece herramientas y otras medidas que tienen por objeto aumentar la seguridad de su equipo de cómputo, dispositivos y los datos personales o la información tratada en los mismos con la finalidad de evitar su acceso no autorizado, daño o pérdida.

A continuación se presenta una lista de once herramientas y otras medidas que, configuradas de manera adecuada, le permitan evitar riesgos que puedan poner en peligro su equipo de cómputo y dispositivos Windows, en los cuales trate información importante:

	Nombre	Función	Aplica a	Categoría
1	**Microsoft Security Essentials** o **Windows Defender**	Antimalware	Windows 7, 8, RT, 8.1 y RT 8.1, Windows 10	**Herramientas**
2	**Firewall de Windows**	Filtro de tráfico	Windows 7, 8 y 8.1, Windows 10	
3	**BitLocker**	Cifrado de disco duro o unidad de memoria USB	Windows 7, 8 y 8.1, Windows 10	
4	**Windows SmartScreen**	Navegación segura	Internet Explorer 11*	**Configuración**
5	**Windows Update**	Actualizaciones de seguridad al Sistema Operativo Windows del equipo de cómputo	Windows 7, 8 y 8.1, RT, Windows 10	
6	**Cuenta de usuario**	Acceso autorizado	Todas las versiones	
7	**Contraseña segura**	Acceso autorizado	Todas las versiones	
8	**Bloqueo de sesión**	Acceso autorizado	Windows 7, 8 y 8.1, RT, Windows 10	
9	**Historial de archivos**	Copia de seguridad	Windows 8 y 8.1, Windows 10	
10	**Configuración de seguridad de Internet**	Navegación segura	Internet Explorer 11 y Microsoft Edge	
11	**Centros de información, recursos y ayuda en línea**	Información, recursos y ayuda	Todas las versiones	**Ayuda**

* **Nota importante:** A partir del 12 de enero de 2016, la única versión de Internet Explorer (IE) que mantendrá soporte será la de IE 11.

Sin perjuicio de lo anterior, hay que atender a que Microsoft ha desarrollado un nuevo sistema operativo, Windows 10. Se trata de un sistema operativo para dispositivos, incluyendo equipos (PCs) tabletas, Windows Phone u otros, que ha sido diseñado considerando el escenario actual, en el que la movilidad es primordial y los riesgos o amenazas para la seguridad cambian constantemente. Además, Windows 10 es la apuesta de Windows por su sistema operativo como un servicio (en inglés, "Windows as a service"), lo que le permitirá contar siempre con un sistema operativo actualizado tanto en temas de seguridad como de nuevas funcionalidades.

En el caso de dispositivos calificados con Windows 7, Windows 8.1 y Windows Phone 8.1 que cumplan los requisitos necesarios, Microsoft ofrece una versión completa de Windows 10 como **actualización** de manera gratuita únicamente durante el primer año a partir del lanzamiento de Windows 10 (los términos y condiciones aplicables pueden verse en el vínculo electrónico https://www.microsoft.com/es-mx/windows/features). En el caso de clientes empresariales que cuenten con el Software Assurance de Windows activo en sus contratos de licencias por volumen, éstos tienen la ventaja de actualizar a la versión Windows 10 Enterprise fuera de esta oferta de actualización gratuita.

Entre otras novedades, cabe señalar que Windows 10 incorpora un nuevo navegador, llamado Microsoft Edge, y un asistente digital, Cortana[1]. Microsoft Edge permite, entre otras cosas, hacer anotaciones directamente sobre las páginas web y compartirlas.

2.2.1. Características de seguridad de Windows 10.

En cuanto a los riesgos o amenazas para la seguridad, que evolucionan a diario, Windows 10 proporciona un amplio conjunto de protecciones que incluyen características de seguridad, despliegue y gestión. Windows 10 introduce novedades que ayudan a proteger los datos mediante el cifrado de los archivos y el disco así como autenticación biométrica. A continuación, se presentan las principales características de Windows 10:

Características de seguridad de Windows 10		
Aspecto	**Característica**	**Función**
Protección de la identidad	Microsoft Passport	Se trata de autenticación de dos factores para el entorno empresarial.
	Microsoft Hello	Autenticación biométrica (lo que requiere tener hardware específico) para acceder a su dispositivo, Microsoft Passport, apps, datos y otros recursos en línea.
	Microsoft Azure Active Directory	Proporciona una solución completa de gestión de identidad y acceso para la nube.

[1] Esta funcionalidad pudiera ser liberada en meses posteriores al lanzamiento de Windows 10. Para conocer los detalles sobre Cortana y su disponibilidad, pueden consultar la página web www.windows.com

Características de seguridad de Windows 10		
Aspecto	**Característica**	**Función**
Protección de datos	BitLocker	Ha sido mejorado, es altamente manejable y puede ser provisionado automáticamente en la mayoría de nuevos dispositivos.
	Enterprise Data Protection	Aborda las necesidades de prevención de pérdida de datos (en inglés, Data Loss Prevention, DLP) y proporciona una solución de cifrado a nivel de archivo. Está integrado con Azure Active Directory y Rights Management Services.
Resistencia a amenazas	Device Guard	Permite a las organizaciones bloquear dispositivos para brindar protección avanzada contra malware nuevo y desconocido.
Seguridad de dispositivos	Seguridad basada en el hardware	Ayuda a mantener y validar la integridad del hardware y el sistema
	UEFI Secure Boot	Ayuda a prevenir que el malware se integre en el hardware o arranque antes que el sistema operativo. Secure Boot es parte del proceso denominado Trusted Boost, que ayuda a mantener la integridad del resto del sistema operativo.

En función del tipo de usuario, hay varias versiones de Windows 10. Por lo que se refiere a la seguridad y algunas de las principales características de Windows 10 en cada versión, es posible presentarlas en la siguiente tabla[2]:

Windows 10	Home	Pro	Empresa	Educación
Seguridad				
Microsoft Passport	✓	✓	✓	✓
Enterprise Data Protection (disponible próximamente)	—	✓	✓	✓
Credential Guard (requiere UEFI 2.3.1 o superior y otros requisitos aplican)	—	—	✓	✓
Device Guard (requiere UEFI 2.3.1 o superior y otros requisitos aplican)	—	—	✓	✓
Windows Hello (requiere hardware específico)				
Reconocimiento de huella digital	✓	✓	✓	✓
Reconocimiento facial y de iris	✓	✓	✓	✓
Seguridad a nivel de empresa	✓	✓	✓	✓
Otras características				
Windows Defender & Windows Firewall	✓	✓	✓	✓
Windows Update	✓	✓	✓	✓
Encriptación de dispositivo (requiere InstantGo o un dispositivo que cumpla con el "Device Encription Requirements Test")	✓	✓	✓	✓
BitLocker (requiere TPM 1.2 o superior)	—	✓	✓	✓

Es necesario tener en consideración que la seguridad en el entorno digital depende del uso de herramientas y de su configuración, debiendo mantenerlas de manera adecuada en todo momento

[2] Las funcionalidades y versiones disponibles de Windows 10 y/o sus características, como Windows Hello, Microsoft Edge, Cortana u otras, pueden variar, por lo que se deberá consultar la página oficial de Windows en www.windows.com, para tener la información oficial actualizada y completa.

para reducir los riesgos derivados de virus, software malicioso o intentos de acceso o tratamientos no autorizados.

Es decir, la seguridad es una cuestión que nos involucra a todos y que requiere de atención constante. No adoptar medidas de seguridad o no mantenerlas supone arriesgarse a perder activos e incluso puede dar lugar a vulnerar el derecho humano a la protección de datos de las personas cuyos datos personales son tratados.

2.3. Protección para su PC, dispositivo e información: antivirus y antimalware

Ayuda para proteger fácilmente y gratis en tiempo real el equipo de su MiPyME contra virus, software espía (spyware) y otros tipos de software o aplicaciones potencialmente no deseados:

Sistema operativo			
		Windows 7, Windows Vista	**Windows 8, Windows RT, Windows 8.1, Windows RT 8.1 y Windows 10**
Producto		**Microsoft Security Essentials**	**Windows Defender**
Protección	Protección en tiempo real contra spyware, virus, rootkits y otro software malicioso.	✓	✓
	Análisis online y limpieza del sistema.	✓	✓
	Servicio dinámico de firmas.	✓	✓
	Análisis sin conexión y limpieza del sistema.	✓	✓
	Protección mejorada contra rootkits y bootkits.	—	✓

En el caso de Windows 10, como ya se ha indicado (véanse las tablas en el apartado anterior), incluye nuevas características de seguridad relativas a la protección de identidad, protección de datos, resistencia a amenazas y protección de dispositivos a través, entre otros, de Microsoft Passport, Microsoft Hello, Enterprise Data Protection, Seguridad basada en el hardware o UEFI Secure Boot.

En el caso de Windows XP, recuerde que después de 12 años, desde el 8 de abril de 2014, el soporte técnico y las actualizaciones para éste dejaron de estar disponibles, de manera que si Usted sigue usando Windows XP, al no tener soporte técnico ni estar cubierto por Microsoft Security Essentials, ¡podría estar exponiendo su equipo, los datos personales e información a nuevos riesgos y amenazas!

2.4. Cumplir con las medidas de seguridad tecnológicas con Microsoft

A continuación se incluye información sobre las principales herramientas que le ofrece Microsoft para adoptar medidas de seguridad en el entorno de trabajo digital, a la vista del Manual del INAI para MiPyMEs y pequeñas organizaciones.

Herramienta o función de Windows	Medida de seguridad	Manual del INAI	Descripción
BitLocker	Cifrado	C.3.1. Uso de contraseñas y/o cifrado	Permite cifrar el contenido del equipo con la finalidad de evitar accesos no autorizados.
Comprobador de contraseñas	Accesos autorizados	C.3.2. Uso de contraseñas sólidas	Ayuda a los usuarios a validar qué tan robusta es su contraseña.
Microsoft Passport y Windows Hello (Windows 10)	Accesos autorizados	C.3.2. Uso de contraseñas sólidas	Evita que terceros no autorizados puedan tener acceso al equipo.
Control de cuentas de usuario	Administración de usuarios	C.3.4. Administrar usuarios y accesos	Permite administrar usuarios así como evitar cambios no autorizados en la configuración de Windows.
Cuentas de usuario	Administración de usuarios	C.3.4. Administrar usuarios y contraseñas	Permite administrar usuarios así como evitar cambios no autorizados en la configuración de Windows.
Firewall de Windows	Antimalware y filtrado de tráfico	C.5.1. Instalar herramientas antimalware y de filtrado de tráfico (firewall o muro de protección)	Su activación evita que cuando Usted está conectado o navegando por Internet su equipo sufra ataques o intentos de acceso no autorizado.
Historial de archivos	Copia de seguridad y restauración de archivos	A.5. Respaldos de los datos personales	Permite realizar copias de seguridad de los datos personales tratados en archivos y, en caso de que sea necesario, restaurarlos si se produce alguna incidencia de seguridad.
Microsoft Security Essentials (Windows 7 y Vista)	Antimalware	C.5.1. Instalar herramientas antimalware y de filtrado de tráfico (firewall o muro de protección)	Su instalación y uso permite detectar y, en su caso, remover virus y otro software malicioso (malware), que podría dañar o borrar datos personales y otra información.

Herramienta o función de Windows	Medida de seguridad	Manual del INAI	Descripción
Microsoft Defender (Windows 8, RT, 8.1 RT 8.1 y Windows 10)	Antimalware	C.5.1. Instalar herramientas antimalware y de filtrado de tráfico (firewall o muro de protección)	Su instalación y uso permite detectar y, en su caso, remover virus y otro software malicioso (malware), que podría dañar o borrar datos personales y otra información.
UEFI Secure Boot (Windows 10)	Antimalware	C.5.1. Instalar herramientas antimalware y de filtrado de tráfico (firewall o muro de protección)	Ayuda a prevenir que el malware se integre en el hardware o arranque antes que el sistema operativo.
Protector de pantalla	Acceso	C.3.3. Bloqueo y cierre de sesiones	Junto con la contraseña, el bloqueo de sesión, permite, en casos de ausencia, evitar que los terceros no autorizados puedan acceder al equipo y a la información o los datos personales al ser necesaria una contraseña para reiniciar la sesión.
Windows SmartScreen	Navegación segura	C.5.2. Reglas de navegación segura	Permite filtrar sitios web maliciosos y otros riesgos para la privacidad y la seguridad.
Windows Update	Actualizaciones al equipo de cómputo	C.1. Actualizaciones al equipo de cómputo y C.2. Revisar periódicamente el software instalado en el equipo de cómputo	Permite mantener actualizado, de manera automática y/o manual, el software de Microsoft instalado en el equipo, de manera que facilita que se hayan instalado también los parches y actualizaciones de seguridad para evitar riesgos contra virus, software malicioso (malware) y otras amenazas.
Panel de control y Centro de actividades	Configuración de seguridad del equipo de cómputo	C.4. Revisar la configuración de seguridad del equipo de cómputo	Permiten revisar y administrar (activar, modificar y/o desactivar) la configuración de seguridad del equipo de cómputo a través del uso de herramientas y productos de Microsoft.
Internet Explorer	Conexiones seguras	C.5.4. Uso de conexiones seguras	Permite configurar un nivel de seguridad de manera que se eviten riesgos al navegar por sitios y páginas web que podrían poner en riesgo la seguridad del equipo de cómputo debido a virus, software malicioso y otras amenazas.

Herramienta o función de Windows	Medida de seguridad	Manual del INAI	Descripción
Outlook	Cuidar el movimiento de la información	C.6.1. Validación del destinatario de una comunicación y C.6.2. Seguridad de la información enviada y recibida.	A través de su Centro de confianza, permite configurar varias características que sirven para proteger la privacidad y seguridad de las comunicaciones hechas por correo electrónico, evitando por ejemplo descargar imágenes que podrían poner en peligro a la privacidad o facilitando la comprobación de los nombres de los destinatarios de correos electrónicos.
Configuración de Windows	Reglas para la divulgación de información	C.5.3. Reglas para la divulgación de información	Facilita el control sobre la divulgación de información de manera que ello permita proteger la privacidad y la seguridad en el entorno digital.
Rights Management Services	Cifrado, Accesos autorizados Cuidar el movimiento de la información y Reglas para la divulgación de información	C.3.1. Uso de contraseñas y/o cifrado; C.6.2. Seguridad de la información enviada y recibida, y C.5.3. Reglas para la divulgación de información	Sirve para proteger la información de una organización a través del uso de políticas de encriptación o cifrado, identidad y autorización que ayudan a asegurar sus archivos y correo electrónico.

3. Implementación de medidas de seguridad con Microsoft

3.1. Acceso autorizado: la cuenta de usuario

¿Qué y por qué?

☑ Garantizar que sólo quien está autorizado tenga acceso al PC o dispositivo así como a los datos personales o la información que se tratan en los mismos.

Gracias a la activación y configuración de cuentas de usuario es posible aumentar la seguridad ya que ello permite controlar qué usuario y a qué accede, gestionando así el acceso en cada caso.

Referencia al Manual del INAI

Ver el apartado *C.3.4. – Administrar usuarios y contraseñas* (pág. 31).

¿Cómo con Microsoft?

☑ **Solución propuesta:** Microsoft le permite activar una o varias cuentas de usuario, según las necesidades, y administrarlas:

— **Diferentes tipos de cuenta:** ya sea estándar, Administrador o invitado, de manera que Usted puede asignar derechos en cuanto al acceso y cambios en el equipo y la información o los datos personales.

— **Configuración de Control de cuentas de usuario:** a través del control de cuentas de usuario Usted puede recibir notificaciones cuando un programa o aplicación intente realizar cambios en el equipo o en Windows.

Cuenta de usuario en la práctica

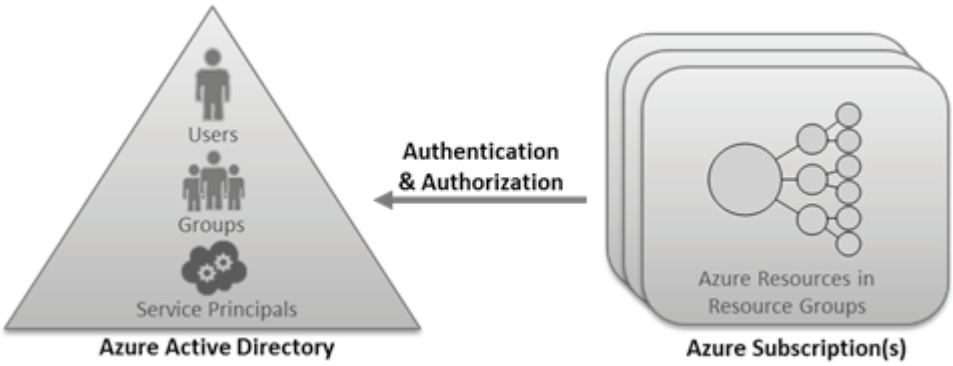
Administrar Cuentas de usuario
Configuración > Panel de control > Cuentas de usuario y protección infantil > Cuentas de usuario > Realizar cambios en la cuenta de usuario.

Ventajas de utilizar una Cuenta de usuario
— Evitar accesos no autorizados al PC o dispositivo en el que se tratan los datos y cambios en la información o datos personales y protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.
— Gestionar los derechos que tiene cada usuario en virtud de su perfil (estándar, Administrador o invitado).
— Impedir cambios no autorizados en el equipo por programas o aplicaciones perjudiciales.

Acción recomendada
Gestionar la cuenta de usuario como medida que contribuye a aumentar la seguridad de los datos personales y de la información que se trata en el PC o dispositivo.

Control de acceso basado en el rol (*Role-based access control*) en Azure

En el caso de Azure, Microsoft facilita a las organizaciones que puedan satisfacer sus requisitos de administración de acceso haciéndolo compatible con el control de acceso basado en roles (en inglés, *Role-based access control*, RBAC) ya que cada una de las suscripciones de Azure está asociada a un Azure Active Directory (en adelante, Azure AD). Gráficamente, puede representarse de la siguiente manera:



El RBAC permite, mediante la asignación de roles, conceder el nivel de acceso apropiado a usuarios, grupos y servicios:

- Usuarios**:** los roles se pueden asignar a usuarios de la organización que están en el Azure AD al que está asociada la suscripción de Azure.
- Grupos**:** los roles se pueden asignar a grupos de seguridad de Azure AD. Si un usuario pasa a pertenecer a un grupo que tiene acceso, ese usuario dispondrá automáticamente de acceso a un recurso. Del mismo modo, si el usuario se sale del grupo, pierde automáticamente el acceso al recurso. En lugar de asignar roles directamente a los usuarios, lo más recomendable es administrar el acceso por grupos mediante la asignación de roles a grupos y la adición de usuarios a esos grupos. RBAC de Azure no permite la asignación de roles a listas de distribución.
- Entidades del servicio**:** las identidades de servicio se representan como entidades de seguridad en el directorio. Se autentican con Azure AD y se comunican entre ellas de forma segura.

Para más información al respecto en español, favor de consultar: https://azure.microsoft.com/es-es/documentation/articles/role-based-access-control-configure/ Y en inglés: https://azure.microsoft.com/en-us/documentation/articles/role-based-access-control-configure/

3.1.1. Comprobador de contraseñas

¿Qué y por qué?

☑ El uso de una contraseña es una medida de seguridad que tiene por objeto evitar que terceros no autorizados tengan acceso al PC o dispositivo y a los datos personales o información.

Es así que el uso de una **contraseña segura** permite aumentar la seguridad del equipo o dispositivo y de los datos personales tratados. Se intenta, por lo tanto, proteger los datos personales y la información contra daño, pérdida, alteración, uso, acceso o cualquier tratamiento no autorizado.

Referencia al Manual del INAI

Ver el apartado *C.3.1. – Uso de contraseñas y/o cifrado* (pág. 30).

¿Cómo con Microsoft?

☑ **Solución propuesta:** Microsoft le da algunas recomendaciones para que Usted pueda elegir una contraseña y mantenerla segura:

— **Claves para elegir una contraseña segura:** están en su longitud y complejidad, además de que es necesario guardarla de forma segura, preferiblemente lejos del equipo o dispositivo, para evitar así que un tercero no autorizado la obtenga y pueda hacer mal uso de la misma. Además, es importante cambiarla con regularidad.

— **Comprobador de contraseñas**: Microsoft le ofrece un comprobador de contraseñas (en inglés, *password checker*) para que Usted pueda comprobar si su contraseña es segura en términos de tipo de caracteres, longitud y si se puede encontrar en un diccionario de cualquier idioma.

Recomendaciones para generar una contraseña segura

Al generar o elegir una contraseña segura, Usted puede considerar las siguientes recomendaciones:

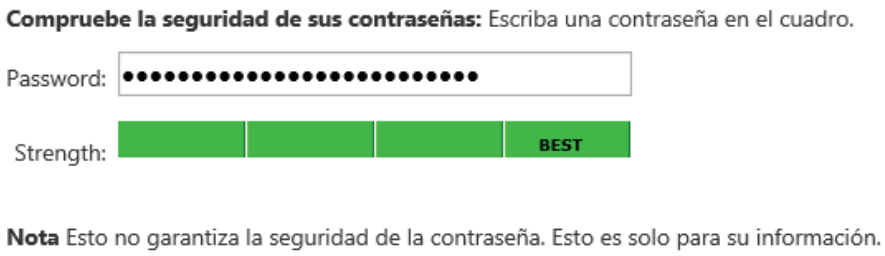
No recomendado		Recomendado	
✗	No use palabras que aparezcan en diccionarios en cualquier idioma.	✓	Use diferentes tipos de caracteres (letras mayúsculas y minúsculas, números, caracteres especiales).
✗	No utilice secuencias o caracteres repetidos, por ejemplo, 12345678, 22222222, abcdefg o letras adyacentes en el teclado (qwerty).	✓	Longitud: use como mínimo ocho (8) caracteres.
✗	No utilice información personal, por ejemplo, fecha de nacimiento, número de pasaporte, etc.	✓	Cambie la contraseña con regularidad.
✗	No utilice la misma contraseña para todo (redes sociales, banca electrónica, etc.).	✓	Guárdela de manera segura lejos de su PC o dispositivo.

Además, Microsoft le ofrece también algunos consejos prácticos para que le sea fácil recordar su contraseña:

Qué hacer	Ejemplo
Comience con una frase o dos.	Las contraseñas complejas son más seguras.
Elimine los espacios entre las palabras de la frase.	Lascontraseñascomplejassonmásseguras.
Abrevie palabras o escriba mal una de ellas intencionadamente.	Lascontraseñascomplejazson+seguras.
Agregue números para que la contraseña sea más larga. Coloque números que signifiquen algo para usted al final de la frase.	Lascontraseñascomplejazson+seguras2011.

Comprobar cómo es su contraseña

Microsoft le ofrece un comprobador de contraseñas para que pueda verificar qué tan segura (robusta) es su contraseña en cuanto al uso de diferentes tipos de caracteres (letras, números y caracteres especiales), su longitud (como mínimo 8 caracteres) y si se puede encontrar en un diccionario de cualquier idioma.



El comprobador de contraseñas está disponible en https://www.microsoft.com/es-es/security/pc-security/password-checker.aspx

Resetear o restablecer la contraseña

Si olvida su contraseña o tiene un problema para iniciar la sesión con su cuenta, puede resetear o restablecer la contraseña siguiendo estos cinco pasos básicos:

1. Ir al vínculo https://account.live.com/resetpassword.aspx
2. Elegir el motivo por el que necesita restablecer la contraseña (contraseña olvidada, problemas con el inicio de sesión aunque sabe cuál es su contraseña o porque piensa que otra persona está utilizando su cuenta de Microsoft).
3. Escriba la dirección de correo electrónico que usó para crear su cuenta de Microsoft.
4. Escriba los caracteres que se le muestran en pantalla y haga clic en siguiente.
5. Utilice el código que se le envíe, al teléfono alternativo o a la dirección de correo electrónico que indique, para restablecer su contraseña.

Puede encontrar más información y ayuda para restablecer su contraseña a través del vínculo electrónico http://windows.microsoft.com/es-419/windows-live/account-reset-password-forgot-faq y para Azure AD, en inglés, en https://msdn.microsoft.com/en-us/library/azure/dn683881.aspx

3.1.2. Administración de usuarios

¿Qué y por qué?	¿Cómo con Microsoft?
☑ La administración de usuarios que pueden tener acceso a un equipo de cómputo y a los datos es necesaria para garantizar la seguridad de los mismos. Al otorgar sólo el acceso necesario para el usuario se mantiene el principio de "necesidad de conocer" (en inglés, "need to know"), con lo cual se evitan accesos no autorizados.	☑ **Solución propuesta:** Microsoft le permite gestionar el acceso por diferentes usuarios: — **Administrar cuentas:** a través de la administración de las Cuentas de usuario puede agregar, cambiar o quitar cuentas de usuario, gestionando así quién y con qué perfil (Administrador, estándar o invitado) accede al equipo de cómputo. — **"Necesidad de conocer":** el tipo de cuenta que se asigne a cada usuario delimita su acceso, de manera que por ejemplo un "invitado" no tendrá acceso a los archivos, carpetas ni configuraciones protegidos con contraseña, lo que ayuda a proteger los datos personales.

Referencia al Manual del INAI

Ver el apartado *C.3.4. – Administrar usuarios y accesos* (pág. 31).

Administración de usuarios en la práctica

Administrar Cuentas de usuario
Panel de control > Cuentas de usuario y protección infantil > Cuentas de usuario > Administrar cuentas.

Ventajas de administrar cuentas de usuario
— Garantizar que los usuarios sólo tienen acceso a los datos necesarios ("necesidad de conocer") para el desarrollo de sus funciones.
— Evitar accesos no autorizados al PC o dispositivo en el que se tratan los datos personales.
— Gestionar varios usuarios en caso de que se hayan activado varias cuentas.
— Facilitar la trazabilidad de las acciones realizadas por los usuarios en caso de que sea necesario determinar quién hizo algo (modificó, borró, envió, etc.).

Acción recomendada
Gestione las cuentas de usuario que son necesarias, creando, cambiando o dando de baja dichas cuentas para así proteger los datos personales y otra información que es tratada en el equipo de cómputo o dispositivo.

Nota general: Sobre la gestión de la identidad y el acceso, puede verse más información, en inglés, en https://www.microsoft.com/en-us/server-cloud/solutions/identity-management.aspx

3.1.3. Bloqueo de sesión

¿Qué y por qué?	¿Cómo con Microsoft?
☑ Si su sesión de usuario está abierta y Usted se ausenta, debe bloquear dicha sesión con la finalidad de evitar que personas no autorizadas puedan tener acceso al equipo y a la información que resguarda el mismo. Se trata de proteger los datos personales y la información contra daño, pérdida, alteración, destrucción o su uso, acceso o cualquier tratamiento no autorizado.	☑ **Solución propuesta:** Microsoft le permite bloquear fácilmente una sesión abierta: — **Bloquear la sesión con tecla del logotipo de Windows + L (o también: Ctrl + Alt + Supr):** si pulsa esta combinación de teclas al mismo tiempo podrá bloquear rápidamente una sesión. También puede cerrar la sesión abierta o cambiar de usuario, si hay varias cuentas de usuario activadas. — **Protector de pantalla:** también puede activar el protector de pantalla lo que, unido a las opciones de inicio de sesión, permite asegurar que sólo el usuario autorizado pueda iniciar o reiniciar la sesión mediante su contraseña.

Referencia al Manual del INAI

Ver el apartado *C.3.3. – Bloqueo y cierre de sesiones* (pág. 31).

Bloqueo de sesión en la práctica

Activar pantalla de bloqueo
Configuración > Cambiar la configuración de PC > PC y dispositivos > Pantalla de bloqueo.

Ventajas de bloquear la sesión
— Evitar accesos no autorizados al PC o dispositivo en el que se tratan los datos personales en casos de inicio o reinicio de una sesión.
— Mantener la confidencialidad de los datos personales y de la información que se trata en el equipo de cómputo o dispositivo.
— Autenticar a los usuarios que intentan acceder al PC, equipo o dispositivo, ya que se requiere la contraseña correspondiente.
— Gestionar varios usuarios en caso de que se hayan activado varias cuentas.

Acción recomendada
Bloquear la sesión mediante el uso de la combinación **tecla del logotipo de Windows + L (o también: Ctrl + Alt + Supr)** y también activar el protector de pantalla de manera que ello evite que en casos de ausencia, un tercero no autorizado pueda acceder.

3.2. Cifrado de los datos personales y de la información

¿Qué y por qué?

☑ Cifrar o encriptar los datos personales y la información es una medida de seguridad técnica que tiene por objeto **evitar accesos no autorizados** a los datos personales.

Al cifrar los datos personales o la información, éstos ya no son accesibles para quien no tiene la clave correspondiente, de manera que sólo la persona autorizada puede acceder a los mismos.

Referencia al Manual del INAI

Ver el apartado *C.3.1. – Uso de contraseñas y/o cifrado* (pág. 30).

¿Cómo con Microsoft?

☑ **Solución propuesta:** Microsoft le ofrece varias soluciones para cifrar o encriptar datos en virtud del sistema operativo que tengas:

— Cifrado de unidad **BitLocker**: permite encriptar o cifrar todos los datos almacenados en el volumen del sistema operativo Windows y volúmenes de datos configurados. Aplica para Windows 8.1 Pro y Windows 8.1 Enterprise.

— **Sistema de cifrado de archivos (EFS)**: también permite almacenar información cifrada o encriptada en el disco duro o en otro dispositivo. Aplica para Windows 7 y Windows Vista.

BitLocker en la práctica

Activar BitLocker
Configuración > Panel de control > Sistema y seguridad > Cifrado de unidad BitLocker > Activar.

Ventajas de utilizar BitLocker
— Evitar accesos no autorizados internos o externos.
— Facilita la comprobación de que se ha mantenido la integridad del archivo de arranque inicial.
— Distribución segura de dispositivos (USB, disco duro externo, etc.).
— Simplifica el proceso de retirada o reciclaje de equipos.
— También permite cifrar memorias USB.

Acción recomendada
Administrar BitLocker tanto para unidades de datos fijas como, en su caso, unidades de datos extraíbles (USB, disco duro externo, etc.).

Nota sobre Azure: Con respecto a las características de seguridad que ofrece Azure, puede verse más información en su Centro de Confianza, en http://azure.microsoft.com/es-es/support/trust-center/security/

3.3. Conexiones seguras: la configuración de seguridad de Internet

¿Qué y por qué?

☑ Cuando Usted se conecta a Internet, especialmente si lo hace a través de redes públicas, y navega por páginas o sitios web de los que no está seguro sobre el contenido, debe adoptar también medidas para evitar descargar software malicioso o permitir que terceros no autorizados puedan interceptar sus comunicaciones.

Gestionar el uso de *cookies* es otra de las cuestiones a considerar a la hora de hacer uso de Internet.

Referencia al Manual del INAI

Ver el apartado *C.5.2. – Reglas de navegación segura* (pág. 32).

¿Cómo con Microsoft?

☑ **Solución propuesta:** Para Microsoft, la seguridad y la privacidad son prioritarias y por ello, le ofrece la posibilidad de configurar un nivel personalizado de seguridad y privacidad para navegar de forma segura:

— **Seguridad:** permite seleccionar un nivel de seguridad para navegar por Internet y también gestionar una lista de sitios web de confianza y restringidos.

— **Privacidad**: a través de la configuración es posible bloquear *cookies* conforme a determinados controles; impedir que un sitio web pueda solicitar su ubicación física, o bloquear elementos emergentes (por ejemplo, ventanas emergentes, etc.). Además, Internet Explorer permite navegar sin almacenar datos de la sesión de exploración (InPrivate).

Conexiones seguras e Internet en la práctica

Configurar Opciones de Internet
Configuración > Panel de control > Redes e Internet > Opciones de Internet > Seguridad.

Ventajas de configurar Opciones de Internet
— Evitar que se pueda descargar software malicioso o se puedan ejecutar programas que podrían ser una amenaza para la seguridad (virus, malware, etc.).
— Gestionar si se aceptan o no *cookies* de sitios o páginas web conforme a los criterios establecidos para cada nivel de seguridad.
— Impedir que un sitio web pueda solicitar su ubicación física.
— A través de InPrivate, configurar el navegador para que no almacene datos de la sesión o historial de navegación.

Acción recomendada
Revisar la configuración de seguridad de Internet para evitar que la seguridad y la privacidad puedan verse comprometidas al navegar por Internet. En el caso de Azure, véase http://azure.microsoft.com/es-es/support/trust-center/security/

3.4. Filtro (SmartScreen)

¿Qué y por qué?

☑ Cuando Usted navega por Internet puede acceder a sitios o páginas web en los que tratan de robar sus datos personales para suplantar su identidad *(phishing)*, así como descargarse software, aplicaciones o archivos que podrían dañar su equipo de cómputo y los datos personales u otra información.

Proteger la seguridad del equipo de cómputo y de los datos personales requiere adoptar medidas de seguridad como los filtros, que permiten evitar riesgos.

Referencia al Manual del INAI

Ver el apartado *C.5.2. – Reglas de navegación segura* (pág. 32).

¿Cómo con Microsoft?

☑ **Solución propuesta:** Con Windows SmartScreen tiene la posibilidad de recibir avisos sobre páginas o sitios web así como software que podrían ser un riesgo para la seguridad:

— **Robo de identidad *(phishing)*:** SmartScreen permite obtener información sobre un sitio web para saber si está en la lista de sitios de robo de datos personales para la suplantación de identidad *(phishing)*.

— **Software malicioso *(malware)***: SmartScreen también cuenta con una lista de software malicioso y, a través de los avisos, si se activan, informa al usuario de que se trata de software desconocido que si se ejecuta, podría causar daños al equipo y a los datos personales.

SmartScreen en la práctica

Configurar Filtro SmartScreen
Configuración > Panel de control > Sistemas y seguridad > Centro de actividades > Cambiar la configuración de Windows SmartScreen.

Ventajas de configurar SmartScreen
— Evitar que pueda producirse el robo de identidad *(phishing)* al navegar por sitios o páginas web identificadas como de riesgo en la lista de SmartScreen.
— Evitar riesgos derivados de la descarga y ejecución de software malicioso *(malware)* que podría dañar al equipo de cómputo, los datos personales y otra información.
— Controlar qué software, aplicaciones o archivos se descargan e instalan, lo que también permite evitar software que no es necesario o sin licencia.

Acción recomendada
Activar y configurar Windows SmartScreen de manera que le permita determinar si quiere recibir avisos o que se requiera su aprobación a la descarga o instalación de software o aplicaciones no reconocidos.

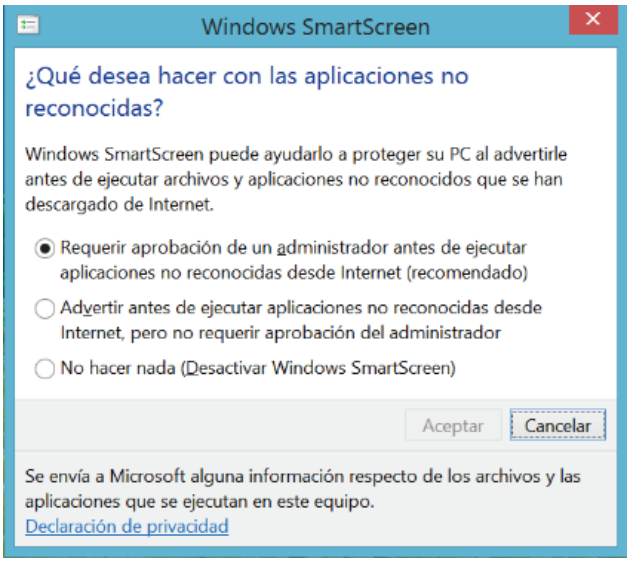
— Protección frente al robo de identidad y software malicioso

Las versiones más recientes de Internet Explorer incluyen el filtro Windows SmartScreen que le ayuda a estar protegido frente a riesgos y amenazas tales como:

Filtro SmartScreen

Riesgo/amenaza	Descripción
Intentos de suplantación de identidad (en inglés, *phishing*).	Advierte sobre las amenazas de sitios o páginas web fraudulentos que intentan obtener datos personales (nombre de usuario, contraseñas, número de pasaporte, número de tarjeta de crédito, etc.) para utilizarlos después en transacciones ilícitas.
Software, aplicaciones o archivos que puedan suponer un riesgo.	Avisa sobre software, aplicaciones o archivos cuya confiabilidad es desconocida, evitando así riesgos para el equipo de cómputo y los datos personales tratados en el mismo.
Software malicioso *(malware).*	Ayuda a prevenir la descarga de software malicioso que podría causar daño en el equipo de cómputo o en los datos personales u otra información.

Es recomendable tener activado y configurado Windows SmartScreen de manera que, en su caso, se requiera una aprobación previa a la descarga e instalación o ejecución de software o aplicaciones desconocidos que podrían causar daños al equipo de cómputo, los datos personales u otra información.



— ¿Cómo funciona SmartScreen?

Cuando Usted navega usando Internet Explorer, SmartScreen analiza los sitios y páginas web buscando características sospechosas que permitan identificar si se trata de un intento de robo de datos personales para la suplantación de identidad *(phishing)* y también determinar si un software, aplicación o archivo no es confiable y, por tanto, podría ser software malicioso *(malware)*.

A través del uso de una lista de sitios de *phishing* y de software malicioso, SmartScreen presenta una ventana de advertencia que alerta al usuario.

3.5. Instalación, administración y revisión de software y aplicaciones

3.5.1. Revisión del software instalado

¿Qué y por qué?

☑ Revisar el software (los programas de cómputo) instalados en el equipo de cómputo o dispositivo para asegurar que no hay software malicioso (virus, *malware*, *spyware*, etc.), no autorizado o que no sea necesario.

Además, asegurarse de que el software instalado está licenciado y no hay más software del que es necesario.

Referencia al Manual del INAI

Ver el apartado C.2. – Revisión de software instalado (pág. 29)

¿Cómo con Microsoft?

☑ **Solución propuesta:** Microsoft le ofrece la posibilidad de controlar fácilmente qué software tiene instalado:

— **Programas y características**: en la opción de programas y características podrá encontrar información sobre cada programa relativa a: nombre del programa, editor, fecha de instalación, tamaño y versión. Además, dando clic en cada programa obtendrá más información sobre el mismo.

— **Desinstalar, cambiar o reparar**: también puede desinstalar, cambiar o reparar un programa.

Instalación y revisión de software en la práctica

Gestión de programas instalados
Configuración > Panel de control > Programas > Desinstalar o cambiar un programa > Seleccionar el programa > Desinstalar.

Ventajas de revisar los programas instalados
— Mantener los programas actualizados evitando así vulnerabilidades y otros riesgos, tales como tener instalado software sin la licencia necesaria y/o software ilegal o más software del necesario.
— Garantizar que sólo se tienen instalados los programas o software necesario.
— Detectar programas que se han instalado sin autorización que pueden ser virus u otro software malicioso (*malware*, etc.).

Acción recomendada
Revisar con frecuencia o, en su caso, periódicamente, si el software o las aplicaciones que están instaladas están actualizadas, autorizadas y/o son necesarias.

3.5.2. Administración de aplicaciones y dispositivos

¿Qué y por qué?	¿Cómo con Microsoft?
☑ Facilitar a los empleados de una organización que puedan hacer uso de sus aplicaciones favoritas así como el uso de dispositivos al mismo tiempo que se asegura la protección de la información de la organización. Permite gestionar la identidad, el uso de dispositivos y aplicaciones y separar los datos para protegerlos.	☑ **Solución propuesta:** Microsoft proporciona a quienes quieran suscribirlo su producto Microsoft Entreprise Mobility Suite (EMS) que facilita que los empleados de la organización puedan hacer uso de sus aplicaciones y dispositivos favoritos al mismo tiempo que se protege la información de la organización. — **Gestión de la identidad:** gestionar la identidad y el acceso. — **Gestión de dispositivos y aplicaciones:** protege la información separando ésta de las aplicaciones.

Referencia al Manual del INAI

Véanse los apartados *C.3., C.5. y C.6.*

Administración de aplicaciones y dispositivos en la práctica

Administración de aplicaciones y dispositivos
Sobre la gestión de identidad, administración de dispositivos móviles y protección de la información, vea más información sobre Microsoft Enterprise Mobility en: http://www.microsoft.com/es-es/server-cloud/enterprise-mobility/

Ventajas de administrar aplicaciones y dispositivos
— Hacer posible que los empleados puedan hacer uso de sus aplicaciones y dispositivos favoritos, lo que además beneficia la productividad.
— Microsoft Entreprise Mobility está preparado para trabajar con un amplio listado de aplicaciones y sistemas operativos (iOS, Android y Windows).
— Proteger la información de la organización gracias a la encriptación o cifrado y separar las aplicaciones y los datos personales de los corporativos.

Acción recomendada
Gestionar la identidad de los usuarios, los dispositivos, las aplicaciones y la información con Microsoft Entreprise Mobility, para asegurar la información.

3.5.3. Revisión de las actualizaciones instaladas

¿Qué y por qué?

☑ Revisar si las actualizaciones automáticas para Windows y otros productos Microsoft están activadas y, en su caso, revisar periódicamente que el software está actualizado para evitar vulnerabilidades, tales como errores en el software o la posibilidad de que alguien explote las vulnerabilidades para instalar software malicioso (virus, *malware*, etc.) o incluso llegar a conseguir información o acceso.

¿Cómo con Microsoft?

☑ **Solución propuesta:** Microsoft le ofrece Windows Update para gestionar las actualizaciones:

— **Activar o desactivar la actualización automática**: de manera que las actualizaciones se descarguen automáticamente y se complete posteriormente la instalación.

— **Buscar otras actualizaciones e instalar actualizaciones opcionales**: estas opciones permiten, respectivamente, buscar otras actualizaciones que estén disponibles así como instalar otras actualizaciones. También puede verse el historial de actualizaciones.

Referencia al Manual del INAI

Ver el apartado *C.1. – Actualizaciones al equipo de cómputo* (pág. 29).

Windows Update en la práctica

Actualizaciones con Windows Update
Configuración > Panel de control > Sistema y seguridad > Windows Update > Activar o desactivar la actualización automática y otras opciones.

Ventajas de mantener los programas o software actualizado
— Mantener los programas o software para Windows y otros productos Microsoft actualizados de manera que se tengan los parches o actualizaciones necesarios.
— Evitar vulnerabilidades que puedan ser aprovechadas por software malicioso o por quien busca en su caso un acceso no autorizado a través de ciertas vulnerabilidades.
— Garantizar que los programas están actualizados, reduciendo riesgos tecnológicos.

Acción recomendada
Revisar periódicamente si se han llevado a cabo las actualizaciones automáticas así como si hay otras actualizaciones que estén disponibles para instalar.

3.6. Validación de destinatarios y seguridad de la información enviada y recibida

¿Qué y por qué?

☑ Cuando Usted envía datos personales o información importante por medios electrónicos, como por ejemplo, correo electrónico, es necesario que se asegure de validar al destinatario o destinatarios de los mismos así como de la seguridad del envío.

Igualmente, es necesario asegurarse de que cuando recibe datos o archivos por medios electrónicos, estén y sean seguros.

Referencia al Manual del INAI

Ver el apartado *C.6. – Cuidar el movimiento de información* (pág. 33).

¿Cómo con Microsoft?

☑ **Solución propuesta:** La configuración de Outlook le ayuda a mantener los documentos seguros y proteger el equipo:

— **Evitar riesgos**: la configuración de Outlook permite evitar que se descarguen automáticamente imágenes incluidas en el e-mail (tales como logos, etc.). Para proteger la privacidad; recibir notificaciones de seguridad, así como cifrar el contenido y datos adjuntos para mensajes salientes.

— **Garantizar la confidencialidad**: cuando envía un correo es importante validar los destinatarios y usar la copia oculta (CCO) para garantizar la confidencialidad y evitar revelar direcciones de correo electrónico a terceros.

Validación de usuarios y seguridad de la información en la práctica

Configurar Outlook y verificar los destinatarios de los envíos
Outlook > Archivo > Opciones > Centro de confianza > Configuración del Centro de confianza.

Ventajas de configurar adecuadamente y utilizar Outlook
— Evita riesgos para su equipo de cómputo y datos personales u otra información ya que impide que automáticamente se descarguen archivos que podrían ser un virus.
— Permite configurar características para autoarchivar mensajes y, en su caso, mantenerlos durante períodos de tiempo determinados.
— Avisa sobre la descargas de imágenes que podrían suponer un riesgo para su privacidad y protección de datos personales.
— Permite establecer reglas para evitar la recepción de mensajes de *spam*.

Acción recomendada
Revisar la configuración de Outlook para asegurarse de que las opciones de privacidad y seguridad son las deseadas.

3.7. Copias de seguridad e historial de archivos

¿Qué y por qué?

☑ La copia de seguridad sirve para proteger los datos personales en casos de pérdida, daños o imposibilidad de acceder a los mismos por cualquier otro evento que ocurra.

Además, es necesario establecer un procedimiento de conservación de los datos durante los plazos aplicables, pudiendo hacer uso del Historial de archivos para ello.

Referencia al Manual del INAI

Ver el apartado *A.5. – Respaldos de los datos personales* (pág. 27).

¿Cómo con Microsoft?

☑ **Solución propuesta:** Con Microsoft Usted puede gestionar fácilmente la realización de copias de archivos y el plazo de conservación:

— **Historial de archivo**: activándolo, permite hacer copias de archivos con datos personales u otra información importante para la organización. El historial se guarda en un dispositivo externo, evitando así que la pérdida o daño del equipo de cómputo suponga perder todo.

— **Frecuencia de la copia y plazo de conservación**: con la configuración avanzada se puede establecer cada cuánto tiempo hacer la copia de seguridad y durante qué plazo mantenerla guardada.

Historial de archivos en la práctica

Activar Historial de archivos
Configuración > Panel de control > Sistema y seguridad > Historial de archivos > Activar.

Ventajas de utilizar el Historial de archivos
— Hacer una copia de seguridad de los archivos con una frecuencia determinada, por ejemplo, cada hora o diariamente.
— Guardar una copia de los archivos que contienen datos personales u otra información importante.
— Recuperar la copia de un archivo que se ha dañado o perdido.
— Establecer el plazo de conservación de las copias de seguridad, por ejemplo, un mes, seis meses o hasta dos años.

Acción recomendada
Activar el Historial de archivos utilizando un dispositivo externo de manera que se puedan guardar una copia de los archivos y recuperarlos si fuera necesario. Para Azure, véase más información en http://azure.microsoft.com/en-us/services/backup/

3.8. ¿Cómo le ayuda Microsoft a cumplir con las medidas de seguridad en el entorno digital?

Siguiendo el Manual de seguridad de datos personales para MiPyMEs y organizaciones pequeñas del INAI, la siguiente tabla tiene por objeto hacer referencia a con qué herramienta de Windows se pueden adoptar acciones para ayudar con el cumplimiento de las medidas de seguridad de la categoría c) Medidas de seguridad en el entorno de trabajo digital. En la columna de la izquierda se indica la correspondiente medida de seguridad prevista en el Manual del INAI y en las columnas central y de la derecha, respectivamente, la herramienta de Windows y los servicios de nube de Microsoft de los que puede hacer uso para adoptar la(s) medida(s) de seguridad.

Cabe señalar que la implementación de estas medidas de seguridad sólo aplican al entorno Microsoft, por lo cual no garantizan el cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, sino que únicamente ayudan a los responsables con el deber de seguridad.

Medidas de seguridad en el entorno de trabajo digital		
Manual de seguridad de datos personales para MiPyMEs y organizaciones pequeñas, del INAI	**Herramientas de Windows**	**Servicios de nube de Microsoft**
C.1. Actualizaciones al equipo de cómputo	Windows Update	—
C.2. Revisar periódicamente el software instalado en el equipo de cómputo	Windows Update, Panel de Control, Microsoft Security Essentials y Microsoft Defender	—
C.3. Medidas de seguridad para acceder al entorno de trabajo electrónico	BitLocker, comprobador de contraseñas, bloqueo de sesión, salvapantallas, configuración de Windows, Microsoft Passport y Microsoft Hello	Office 365 y Azure
C.3.1. Uso de contraseñas y/o cifrado	Comprobador de contraseñas y BitLocker	Office 365 (por ejemplo, Rights Management Services) y Azure (cifrado y administración de contraseñas)
C.3.2. Uso de contraseñas sólidas	Comprobador de contraseñas	Office 365 (por ejemplo, autenticación multifactor) y Azure (por ejemplo, almacén de claves)
C.3.3. Bloqueo y cierre de sesiones	Salvapantallas y bloqueo de sesión con contraseña	—
C.3.4. Administrar usuarios y accesos	Configuración de Windows, Control de cuentas de usuario y Windows SmartScreen	Office 365 (por ejemplo, control de acceso basado en roles (RBAC)) y Azure (por ejemplo, Azure Active Directory)
C.4. Revisar la configuración de seguridad del equipo de cómputo	Configuración de Windows, Internet Explorer, Microsoft Security Essentials y Microsoft Defender	Office 365 y Azure

Manual de seguridad de datos personales para MiPyMEs y organizaciones pequeñas, del INAI	Herramientas de Windows	Servicios de nube de Microsoft
C.5. Medidas de seguridad para navegar en entornos digitales	Windows Firewall, Internet Explorer y Microsoft Edge	Office 365 y Azure
C.5.1. Instalar herramientas antimalware y de filtrado de tráfico (firewall o muro de protección)	Microsoft Security Essentials, Microsoft Defender, Windows Firewall, Windows SmartScreen, Internet Explorer, Panel de Control y UEFI Secure Boot	Office 365 (por ejemplo, detección de vulnerabilidades perimetrales e intrusiones) y Azure
C.5.2. Reglas de navegación segura	Internet Explorer y Windows SmartScreen	Office 365 (por ejemplo, Exchange Online Protection, EOP)
C.5.3. Reglas para la divulgación de información	Configuración de Windows	Office 365 (por ejemplo, Rights Management Services) y Azure (por ejemplo, Azure Active Directory)
C.5.4. Uso de conexiones seguras	Internet Explorer, Microsoft Edge y Outlook	Office 365 (por ejemplo, cifrado en tránsito con SSL/TLS entre Usted y Microsoft) y Azure
C.6. Cuidar el movimiento de la información	Outlook	Office 365 y Azure
C.6.1. Validación del destinatario de una comunicación	Outlook	Office 365 (por ejemplo, S/MIME para acceso seguro al correo electrónico)
C.6.2. Seguridad de la información enviada y recibida	Outlook	Office 365 (por ejemplo, cifrado de mensajes) y Azure

Además de las herramientas y características que ofrecen productos de cómputo en la nube como Office 365 y Azure, los usuarios de los mismos también pueden tener en consideración, entre otras, las características de seguridad específicas que ofrecen los servicios de nube empresarial de Microsoft.

En concreto, por lo que se refiere a la seguridad lógica, la seguridad de los datos y los controles de administrador y usuario, cabe destacar las siguientes características específicas:

Seguridad lógica:

- Detección de malware: con el servicio Exchange Online Protection (EOP) para Office 365 se robustece la protección del correo electrónico contra spam, virus y software malicioso (malware). Se trata de un servicio de filtrado que proporciona una protección adicional (en inglés, Exchange Online Advanced Threat Protection, ATP) contra tipos específicos de amenazas avanzadas. Entre otros beneficios, este servicio de Microsoft permitirá a sus usuarios protegerse frente a malware y virus, así como URLs maliciosas que se encuentren en mensajes de correo electrónico recibidos a través de Office 365. En el caso de Azure, el servicio Microsoft Antimalware también permite una protección en tiempo real contra virus, spyware y otro software malicioso (malware), así como intentos de penetración gracias al uso de defensas contra ataques distribuidos de denegación de servicios (en inglés, distributed denial-of-service, DDoS).
- Escaneo de puertos y detección de otras vulnerabilidades perimetrales e intrusiones, lo que permite prevenir o, en su caso, detectar intentos de accesos no autorizados.
- Para ampliar la información al respecto, específicamente en el caso de Azure puede verse también el vínculo electrónico http://azure.microsoft.com/es-es/support/trust-center/security/

Seguridad de archivos y/o datos:

- Prevención de pérdida de información (en inglés, Data Loss Prevention, DLP): en el caso de Office 365, por ejemplo, esta característica sirve para impedir que salgan de la organización datos confidenciales y también, combinada con Rights Management Services y el cifrado de mensajes de Office 365, sirve para establecer más controles o reglas para la divulgación de información.
- Microsoft Enterprise Mobility: facilita la gestión de la identidad, administración de dispositivos móviles y protección de la información al mismo tiempo que maximiza la productividad de los empleados cuando usan sus aplicaciones y dispositivos favoritos asegurando que los datos corporativos, ya sean datos personales u otra información, son protegidos. Al respecto, puede verse más información en http://www.microsoft.com/es-es/server-cloud/enterprise-mobility/
- Cifrado y administración de claves:
  - Elementos de protección tecnológica, como las comunicaciones cifradas y los procesos de operaciones, ayudan a mantener los datos del cliente seguros. Dispone de la flexibilidad para implementar cifrado adicional y administrar sus propias claves.

    Para los datos en tránsito, Azure usa protocolos de transporte estándar de la industria entre dispositivos de usuarios y centros de datos de Microsoft, así como dentro de los propios centros de datos. Puede habilitar el cifrado para el tráfico entre sus propias máquinas virtuales (VM) y los usuarios finales. Con las redes virtuales, puede usar el protocolo IPsec estándar de la industria para cifrar el tráfico entre su puerta de enlace de VPN corporativa y Azure.

    Para los datos en reposo, Azure ofrece una amplia variedad de capacidades de cifrado hasta AES-256, que le proporcionan la flexibilidad de elegir la solución que mejor satisfaga sus necesidades.

    El Almacén de claves de Azure le permite simplificar de manera fácil y rentable la administración de claves y mantener el control de las claves que usan los servicios y las aplicaciones en la nube para cifrar datos

    Sobre Azure, puede verse más información en http://azure.microsoft.com/es-es/support/trust-center/security/

- Controles de administrador y usuario: administración de usuarios: Para Administrar y proteger el acceso de los usuarios a sus entornos, datos y aplicaciones, puede federar las identidades de los usuarios en *Azure Active Directory* y habilitar *Multi-Factor Authentication* para obtener un inicio de sesión más seguro.

  Azure Active Directory es una solución en la nube de administración integral de identidades y acceso que ayuda a proteger el acceso a sus datos y aplicaciones locales y en la nube, además de simplificar la administración de usuarios y grupos. Combina servicios de directorio fundamentales, control avanzado de la identidad, seguridad y administración del acceso a las aplicaciones. *Azure Active Directory* también facilita a los desarrolladores la generación de administración de identidades basada en directivas en sus aplicaciones.

Azure Multi-Factor Authentication requiere el uso de más de un método de comprobación para autenticar a un usuario. Azure protege el acceso de los usuarios a datos y aplicaciones con esta capa adicional de autenticación para aplicaciones locales y en la nube. Proporciona autenticación sólida con una variedad de opciones de comprobación fácil a la vez que satisface la demanda, por parte de los usuarios, de un proceso de inicio de sesión

Para obtener más información al respecto, puede verse http://azure.microsoft.com/es-es/support/trust-center/security/

- Administración de dispositivos móviles: Office 365 cuenta con capacidades generalmente disponibles de gestión de dispositivos móviles (en inglés, *Mobile Device Management*, MDM) lo que facilita su administración y, al mismo tiempo, responde a las necesidades derivadas de un escenario de movilidad y de tendencias basadas en "trae tu propio dispositivo" (en inglés, *Bring Your Own Device*, BYOD). Al respecto, téngase en consideración *Microsoft Enterprise Mobility* y las posibilidades que ofrece esta suite. Puede ver más información al respecto en http://www.microsoft.com/es-es/server-cloud/enterprise-mobility/

- Administración de identidad y acceso: en el caso de Azure, Microsoft cuenta con una experiencia demostrada en la administración de identidades gracias a Windows Server Active Directory y Forefront Identity Manager. Entre las ventajas que pueden destacarse se encuentran las relativas a crear y administrar una identidad única para cada usuario en toda la empresa híbrida, lo que mantiene los usuarios, grupos y dispositivos sincronizados, así como proporcionar un acceso de inicio de sesión único a las aplicaciones, incluidas miles de aplicaciones SaaS preintegradas.

4. Uso de la nube con OneDrive, Office 365 y Azure

El cómputo en la nube es una oportunidad para las organizaciones y Microsoft, como uno de los principales proveedores de nube a nivel mundial, trabaja día a día para acercarla también a las MiPyMEs y pequeñas organizaciones con la finalidad de que puedan beneficiarse de su uso.

Son muchas las organizaciones y personas que, desde hace ya muchos años, están haciendo uso de la nube. En este sentido es frecuente encontrar usuarios de correo electrónico de Hotmail, un claro ejemplo de uso del cómputo en la nube.

Actualmente, Microsoft ofrece varios servicios de nube, pudiendo destacar aquí OneDrive, como servicio para el almacenamiento de archivos en la nube, Office 365, como ejemplo de software como un servicio (en inglés, *Software as a Service*, SaaS) y otros servicios basados en la nube, así como Microsoft Azure, como ejemplo de plataforma (en inglés, *Platform as a Service*, PaaS) y también infraestructura (en inglés, *Infraestructure as a Service*, IaaS) que permite a sus clientes desarrollar, implementar y administrar aplicaciones.

Todos los servicios y aplicaciones de nube proporcionados por Microsoft están desarrollados con base en los más altos estándares internacionales de privacidad y seguridad.

Tome en cuenta que existen muchas ofertas de servicios y aplicaciones en la nube, de muchos proveedores. Asegúrese de usar y contratar aquéllas de proveedores que cumplan con altos estándares de privacidad de su información. Recuerde que muchos servicios y aplicaciones en Internet, que se ofertan bajo el título de gratuitos o con pretextos tales como "mejorar la experiencia del usuario", utilizan en realidad su información personal como moneda de cambio, para propósitos de publicidad o comercialización posterior a terceros, sin su consentimiento informado y el aviso de privacidad específico al respecto.

Lo mismo ocurre con algunos motores de búsqueda o servicios de correo electrónico, plataformas de video o redes sociales. En ocasiones, efectúan "screening" o "minería" de la información personal, comportamiento o contenido de las comunicaciones, sin su consentimiento informado y el aviso de privacidad respectivo.

En el caso de los servicios de nube tales como Office 365 y Microsoft Azure, Usted tiene la seguridad de que cualquier información personal le pertenece sólo a Usted en todo momento, y que Microsoft no usa su información para efectos de publicidad.

Siga las recomendaciones de esta guía para incrementar el nivel de seguridad de los servicios y aplicaciones en la nube, ya que algunos mecanismos de seguridad pueden depender de la configuración que defina el usuario.

OneDrive es un servicio de nube, consistente en el almacenamiento de archivos de forma segura y confiable, dirigido tanto a usuarios domésticos como MiPyMEs y otras organizaciones pequeñas. Microsoft cuenta con dos ediciones de OneDrive, la que está disponible al público en general conocida como OneDrive, y la edición para empresas denominada OneDrive para la Empresa.

En el caso de las MiPyMEs, poder acceder a documentos e información desde cualquier lugar y en cualquier momento, gracias al uso de la nube, facilita la movilidad de las personas y se convierte también en una ventaja competitiva.

Además, el uso de OneDrive para almacenar archivos que contengan datos personales u otra información relevante para la organización tiene importantes ventajas, en particular, en el caso de que se haya suscrito al servicio OneDrive para la Empresa, pudiendo señalar, entre otras, las siguientes:

 Seguridad	 Confiabilidad	 Cumplimiento
Microsoft ha sido reconocido como líder del sector en materia de seguridad en la nube gracias a las directivas y controles implementados. Entre otras, los servicios de nube de Microsoft tienen otorgada la certificación ISO 27001, tras la verificación mediante auditorías independientes.	Los servicios de nube de Microsoft ofrecen un tiempo de actividad del 99,9%. Además, Microsoft no utiliza los datos con fines de publicidad y, en caso de que decida dejar el servicio, facilita poder llevárselos antes de borrarlos.	Microsoft ofrece a todos sus clientes un marco jurídico integrado que facilita el cumplimiento en materia de protección de datos personales y seguridad. De esta manera, Microsoft busca mantener un alto nivel de cumplimiento, siguiendo altos estándares a nivel internacional, de manera continua.

Microsoft trabaja para introducir mejoras continuas en sus servicios y por lo que se refiere a OneDrive para la Empresa, entre otras, ofrece ya capacidades adicionales para la prevención de pérdida de datos; auditorías e informes, así como otras funcionalidades de uso.

OneDrive ofrece varios planes en función de las necesidades del cliente, pudiendo hacerse uso del mismo gratuitamente hasta 15 GB o suscribirse a otros planes mensuales con capacidades de almacenamiento y/o servicios adicionales.

En cualquier caso, la posibilidad de almacenar bases de datos, documentos con datos personales u otra información corporativa contenida en archivos en un lugar seguro permite a la organización contar con un nivel de seguridad adicional, proporcionado por Microsoft, de manera que, por ejemplo, en caso de robo o pérdida del equipo de cómputo o dispositivo, los datos personales estarían separados y almacenados en un lugar seguro. También, la posibilidad de acceder a medidas de seguridad ofrecidas por un tercero, experto en la materia, supone un valor agregado que además facilita el cumplimiento de los requisitos normativos y regulatorios en materia de protección de datos personales y seguridad.

Es así que OneDrive permite tanto a personas físicas como a MiPyMEs y empresas almacenar información en la nube y hacer uso de diversos servicios. Además, OneDrive para la Empresa ofrece características específicas en materia de protección de datos, privacidad, seguridad y confiabilidad, con la finalidad de entregar un servicio de productividad de nube para el que se han adoptado rigurosos estándares de la industria.

Si Usted desea obtener más información sobre OneDrive, los planes de uso, sus características, consejos y, en su caso, descargarlo, puede ver OneDrive para usuarios que sean personas físicas y MiPyMEs (https://onedrive.live.com/about/es-mx/) y OneDrive para la Empresa (https://onedrive.live.com/about/es-mx/business/).

Facilitando la Nube

protección y regulación de datos para el impulso de Latinoamérica

Las decisiones sobre el cómputo en la nube que tomen los responsables de las políticas y las partes interesadas influirán en los empleos, la competitividad, la innovación, la inclusión social y el nivel de vida de la región.

Muchas naciones evalúan la necesidad de leyes acordes a la realidad y necesidades del cómputo en la nube, sin dejar a un lado el interés por la legislación en materia de privacidad.

*Empoderar decisiones de los individuos en materia de privacidad.

*Matener la seguridad de la información

*Construir confianza alrededor de la tecnología.

"[SON IMPORTANTES] REGLAS CLARAS Y AMIGABLES CON LA NUBE... [PORQUE] UNA NUBE SIN PROTECCIÓN CLARA Y ROBUSTA NO ES EL TIPO DE NUBE QUE NECESITAMOS."-NEELIE KROES, COMISIONADA PARA LA AGENDA DIGITAL DE LA UNIÓN EUROPEA (2010)

BENEFICIOS DEL CÓMPUTO EN LA NUBE

La nube puede ser motor del crecimiento económico y beneficios sociales.

1. GENERA EMPLEOS

En América Latina el crecimiento de puestos de trabajo (calificados y bien remunerados) relacionados con la Nube aumentará 34% anualmente.

2. AHORROS

Un desarrollo híbrido de nube puede significar ahorros en TI de entre el 20 y el 30%

3. INCLUSIÓN SOCIAL

El cómputo en la nube no sólo se trata de eficiencia sino de aumentar la equidad. Por ejemplo: un hospital rural con especialistas a distancia en tiempo real o escuela aprovecha el aprendizaje a distancia, las aplicaciones web y el bajo costo de almacenamiento.

4. AGILIDAD Y FLEXIBILIDAD

Las instituciones y empresas pueden ajustar de manera sencilla la demanda de servicios según necesidades: periodos específicos y/o requerimientos de movilidad.

5. SEGURIDAD

Según estudio sobre 70 mil vulnerabilidades en 1,600 compañías, encontró que los sistemas 'on premises' son más vulnerables que las aplicaciones en la nube.

LA IMPORTANCIA DE LA REGULACIÓN

Las reglas dan certidumbre a los usuarios sobre la seguridad y privacidad de su información.

1. ASEGURAR PROTECCIÓN A LA PRIVACIDAD

Los reguladores pueden asegurarse de que las personas, negocios e instituciones no se preocupen por su información gracias a un marco jurídico adecuado.

2. INSTAR A LA TRANSPARENCIA

Servicios 'gratuitos' obtienen ganancias de la venta de datos personales a terceros. Por ello es importante que los usuarios entiendan la naturaleza de los términos de uso y sus consecuencias.

3. PERMITIR Y PROTEGER LOS FLUJOS DE DATOS A TRAVÉS DE FRONTERAS

Para aprovechar las economías a escala es importante permitir el movimiento -seguro y confiable- de datos a través de diferentes localidades en la orbe.

4. ARMONIZACIÓN DE LA INTEROPERABILIDAD Y REGLA DE PROTECCIÓN DE DATOS

Las diferencias entre países en legislaciones de protección de datos y la interoperabilidad hacen necesaria la consistencia regulatoria.

5. REFORZAR LEYES CONTRA LOS CRÍMENES CIBERNÉTICOS

Prevenir estas amenazas construirá mayor confianza en el computo en la nube a la vez que se protege a los individuos, las naciones y la economía.

Microsoft

ALGUNOS PROVEEDORES DE SERVICIOS DE NUBE
obtienen ganancias al revisar y vender la información encontrada
en tus correos electrónicos y búsquedas.

SI OBTIENES UN SERVICIO EN LINEA GRATUITO,
TÚ INFORMACIÓN PERSONAL PODRÍA SER
LA MONEDA DE CAMBIO.

Nuestra Privacidad no debe ser el precio que pagamos por conectarnos a Internet

EL COMPROMISO DE MICROSOFT CON LA PRIVACIDAD
EN LA NUBE SE DEBE A QUE LA EMPRESA GENERA
GANANCIAS POR LA VENTA DE SOFTWARE Y SERVICIOS
INNOVADORES, LO CUAL VALORA SU PRIVACIDAD Y EXPERIENCIA DE USO.

ASÍ MICROSOFT PROTEGE SU PRIVACIDAD EN LA NUBE:

PROGRAMA DE MEJORA DE LA EXPERIENCIA DEL CLIENTE

Los usuarios de manera voluntaria comparten información sobre el uso de productos de MIcrosoft. Información que es respetada en todo momento con respecto a su privacidad y seguridad.

OFFICE 365 TRUST CENTER

Provee transparencia acerca de la privacidad de la información y prácticas de seguridad en Office 365. Muestra de manera clara y transparente cómo la información es recolectada y revisada.

INTERNET EXPLORER

Ofrece protección de rastreo para evitar que terceras partes usen los datos de sus usuarios. El control de rastreo permite a los usuarios el control total de su información de navegación.

WINDOWS PHONE

Windows Phone 8 incluye geolocalización, sólo con autorización de los usuarios, característica que permite tomar ventaja de esta información para aprovechar aplicaciones y servicios.

POLÍTICA DE ACCESO DE INFORMACIÓN

Si una entidad gubernamental se acerca a Microsoft para obtener información de nuestros clientes, Microsoft intentará en primera instancia redirigir la entidad al cliente para permitir al cliente la oportunidad de determinar cómo responder. No obstante, si por razones legales es requerida la información. Microsoft sólo proporcionará información de sus clientes cuando esté legalmente obligado a hacerlo.

WINDOWS

Windows 8 BitLocker y BitLocker To Go son herramientas para el manejo de información sensible mediante la encriptación de datos en PC y dispositivos USB.

ENCRIPTACIÓN

Encriptación más robusta a través de redes y servicios, como Office 365 y Outlook.com

NO BACK DOORS

Certifica el código del software para evitar las puertas traseras que gobiernos pudieran explotar para acceder a datos de los clientes.

LIDERAZGO EN LA INDUSTRIA

Al mismo tiempo, Microsoft se une con otras empresas para pedir reformas que cambien los métodos de vigilancia de los gobiernos.

Microsoft continuará participando de manera activa en los esfuerzos para crear prácticas de protección de la privacidad. Invitamos a los gobiernos a revisar sus marcos legales para fomentar el cómputo en la nube en beneficio de los ciudadanos y nuestras comunidades.

Microsoft

Microsoft Office 365 está pensado para MiPyMEs, ofreciendo la posibilidad de hacer uso de los servicios (software y almacenamiento) en línea (online), lo que permite utilizar el software así como compartir y almacenar documentos y archivos a los que puede accederse desde cualquier lugar y en cualquier momento. Sobre Office 365, puede verse también más información en el Centro de Confianza disponible en el vínculo electrónico https://products.office.com/es-MX/business/office-365-trust-center-cloud-computing-security?tab=7a3a6365-14c0-81ac-34ff-f4a416599263&omkt=es-MX

Con Office 365 cualquier MiPyME y otras organizaciones pequeñas tienen acceso a software y servicios basados en la nube seguros y confiables, que han sido diseñados siguiendo altos estándares en materia de protección de datos personales, privacidad y seguridad (al respecto, puede verse la información disponible en https://www.microsoft.com/online/legal/v2/?docid =27&langid=es-es), además del compromiso que Microsoft asume en cuanto a facilitar su control de los datos personales, de manera que éstos no serán utilizados con fines publicitarios y pudiendo recuperarlos en cualquier momento o si decide no seguir haciendo uso de la nube de Microsoft.

Microsoft diseñó Office 365 y otros productos y servicios, para poner a su disposición software y servicios diseñados conforme a altos estándares de privacidad y seguridad. Sin perjuicio de la información disponible en https://products.office.com/es-MX/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy?omkt=es-MX, a continuación, se incluyen las diez características principales de Microsoft Office 365 en materia de seguridad, privacidad desde el diseño y protección de datos personales, transparencia y cumplimiento continuo:

Seguridad integrada

Privacidad desde el diseño y protección de datos personales

Transparencia

Cumplimiento continuo

Seguridad integrada	Privacidad desde el diseño y protección de datos personales	Transparencia	Cumplimiento continuo
1. Controles de seguridad. **2.** Servicio de nube con certificaciones internacionales: ISO 27001, etc. **3.** El enfoque de seguridad de Microsoft abarca la seguridad física de los centros de datos, las directivas y los controles. **4.** Las medidas de seguridad adoptadas por Microsoft son comprobadas por auditores independientes. **5.** Las características de seguridad se dividen en seguridad integrada y controles del cliente. **6.** Microsoft le informará puntualmente si se ha accedido indebidamente a	**1.** Controles de protección de datos personales y privacidad, habiendo adoptado también los de la **ISO/IEC 27018**. **2.** Los controles de privacidad son auditados de manera independiente. **3.** Los datos personales son suyos. **4.** Microsoft solo usa sus datos para brindarle el servicio. **5.** Los datos no se utilizan con fines publicitarios. **6.** Como responsable del tratamiento de los datos personales, usted puede descargar una copia de los mismos en cualquier momento y por cualquier motivo.	**1.** Centro de confianza de Microsoft Office 365. **2.** Microsoft publica la lista de subcontratistas. **3.** Usted sabe para qué se usan sus datos. **4.** Microsoft es transparente sobre dónde se encuentran sus datos. **5.** Microsoft le informará puntualmente si se ha accedido indebidamente a sus datos. **6.** Microsoft le informará de cambios importantes al servicio con respecto a la seguridad, la privacidad y el cumplimiento normativo. **7.** Microsoft facilita que sepa si alguien ha accedido a sus datos (acceso administrativo).	**1.** Microsoft sigue procesos proactivos en relación con el cumplimiento. **2.** Microsoft le facilita controles para el cumplimiento organizativo. **3.** Microsoft aplica procedimientos recomendados en el diseño y las operaciones, como redundancia, y supervisión, entre otros. **4.** Actualización constante en cuanto a los estándares y las regulaciones que se aplican a su sector de actividad. **5.** Los subcontratistas cumplen con estándares de seguridad y privacidad equivalentes. **6.** Microsoft tiene un

sus datos. **7.** El acceso a sus datos se registra de manera que usted puede saber quién y para qué se ha accedido a los mismos. **8.** Periódicamente hacemos copia de seguridad de sus datos. **9.** Aplicamos contraseñas "seguras" para aumentar la seguridad de sus datos. **10.** Microsoft habilita el cifrado de los datos entre el centro de datos y usted, como usuario.	**7.** Usted puede activar y desactivar las características relacionadas con la privacidad para ajustarlas a sus necesidades. **8.** Firmamos un acuerdo de procesamiento de datos. **9.** Si recibimos una solicitud gubernamental de acceso a los datos, siempre que sea posible, se la redirigimos al titular de los mismos. **10.** Office 365 cumple con normas internacionales sobre privacidad, tales como HIPAA (Estados Unidos de América) o PIPEDA (Canadá).	**8.** Microsoft le informa de características y medidas sobre el servicio a través del centro de mensajes de Office 365. **9.** Microsoft publica trimestralmente el tiempo de actividad (99,9%). **10.** Microsoft le ofrece soporte técnico en línea o telefónico.	contrato de nivel de servicio. **7.** Auditorías independientes. **8.** Microsoft tiene un equipo de profesionistas dedicados al cumplimiento y que monitorean continuamente cambios normativos y regulatorios. **9.** Acuerdo de procesamiento de datos detallado. **10.** Centro de confianza de Office 365.

Una cuestión importante a tener en consideración es la norma ISO/IEC 27018:2014 que establece controles y directrices para proteger la información personal en los servicios de nube pública proporcionados por proveedores de servicios de cómputo en la nube. Esta norma es el primer estándar internacional relativo a la protección de datos personales en el cómputo en la nube.

En particular, uno de los controles que establece la norma ISO/IEC 27018:2014 y, por tanto, que tiene que garantizar el proveedor de servicios de cómputo en la nube para cumplir con la misma, es el relativo a demostrar que no usa los datos personales con fines de publicidad, a menos que obtenga el consentimiento necesario para ello.

Microsoft ha adoptado este estándar internacional para todos sus servicios de cómputo en la nube empresarial: Office 365, Dynamics CRM Online y Microsoft Intune. Para ello, ha sido auditado por terceros independientes. La adopción de los controles de la norma ISO 27018 para estos servicios se suma, como veremos a continuación, a que también los cumple en Azure, que es una plataforma de nube.

Seis controles clave de la norma ISO/IEC 27018

La norma ISO/IEC 27018:2014 implica que el proveedor de servicios que la adopta tiene que cumplir con seis principios clave, que son los siguientes:

1. **Consentimiento:** el proveedor de servicios de cómputo en la nube no puede usar los datos personales que se le encomiendan con fines de publicidad, a menos que se tenga la autorización necesaria para ello.
2. **Control:** de los clientes, como responsables del tratamiento, sobre el uso de los datos personales por el proveedor de servicios.
3. **Transparencia:** del tratamiento de datos personales por el proveedor de servicios hacia el cliente
4. **Responsabilidad (”accountability”):** por lo que se refiere a la seguridad de los datos personales tratados por el proveedor de servicios de cómputo en la nube.
5. **Comunicación:** a los clientes de los servicios de cómputo en la nube en caso de que se produzca una brecha o vulneración de las medidas de seguridad.
6. **Auditoría anual independiente:** sobre el cumplimiento de los controles de manera que el proveedor de servicios de cómputo en la nube demuestre que puede seguir manteniendo la certificación que se le ha otorgado.

Microsoft Azure

Azure es una plataforma de nube abierta y flexible, que incluye una colección de servicios integrados (proceso, almacenamiento, datos, redes y aplicación) lo que permite que los clientes puedan desarrollar, implementar y administrar aplicaciones rápidamente en toda una red mundial de centros de datos administrados por Microsoft. Se trata, por tanto, de una solución de infraestructura como servicio (en inglés, *Information as a Service*, IaaS) y plataforma como servicio (en inglés, *Platform as a Service*, PaaS).

Con Azure puede:

- **Crear infraestructuras.** Aprovisionando máquinas virtuales para su uso.
- **Desarrollar aplicaciones modernas.** Puede crear e implementar una amplia variedad de aplicaciones para Android, iOS y Windows.
- **Obtener información a partir de los datos.** A través de los servicios administrados de SQL (siglas en inglés de *Structured Query Language* y que en español puede traducirse como Lenguaje de Consulta Estructurado, siendo un lenguaje vinculado a la gestión de bases de datos de carácter relacional que permite realizar determinadas operaciones entre dichas bases de datos) y NoSQL (o "Not only SQL", pudiendo traducirse como "No solo SQL" y que se trata de una amplia clase de sistemas de gestión de bases de datos que no usan SQL) que proporciona Azure.
- **Administrar identidades y accesos.** Administrar las cuentas de usuario, sincronizar con directorios locales existentes y utilizar el inicio de sesión único en Azure u Office 365, entre otros, así como interactuar con software No Microsoft de manera natural.

Además, Azure ofrece, entre otras características relevantes:

- Uso de servicios en la nube de forma predeterminada, como la instalación de actualizaciones.
- Está listo para un uso híbrido.
- Es abierto y flexible.
- Listo para funcionar.
- Económico y escalable.

Las principales características de Microsoft Azure por lo que se refiere a su diseño y seguridad operacionales así como su funcionalidad y controles de seguridad son las que se indican a continuación:

Diseño y seguridad operacionales	Funcionalidad y controles de seguridad
Microsoft ha desarrollado prácticas recomendadas que son líderes del sector para el diseño y administración de servicios en línea, como: • **Centros de seguridad de excelencia.** Microsoft Digital Crimes Unit, Microsoft Cybercrime Center y Microsoft Malware Protection Center proporcionan una visión de las cambiantes amenazas globales para la seguridad. • **Ciclo de vida de desarrollo de la seguridad** (en inglés, *Security Development Lifecycle*, **SDL**). Desde 2004, todos los productos y servicios de Microsoft se han diseñado y creado teniendo en cuenta el ciclo de vida de	Azure ofrece una base de confianza sobre la cual los clientes pueden diseñar, construir y administrar sus propias aplicaciones e infraestructura en la nube seguras: • **Seguridad física con supervisión durante 24 horas.** Los centros de datos se construyen, administran y supervisan físicamente para proteger los datos y servicios contra el acceso no autorizado, así como de las amenazas medioambientales. • **Supervisión y registro.** La seguridad se supervisa con ayuda de sistemas de supervisión, correlación y análisis

desarrollo de la seguridad, un enfoque amplio para escribir código más seguro, confiable y de seguridad mejorada. • **Garantía de la seguridad operacional** (en inglés, *Operational Security Assurance*, **OSA**). El programa OSA de Microsoft proporciona una línea de base de seguridad operacional en todos los principales servicios en la nube, lo que ayuda a garantizar que los riesgos clave se mitigan sistemáticamente. • **Supuesto de infracción.** Los equipos especializados de ingenieros de seguridad de Microsoft utilizan prácticas de seguridad pioneras y trabajan con el "supuesto de infracción" en mente para identificar las vulnerabilidades potenciales y eliminar de forma proactiva las amenazas antes de que se conviertan en riesgos para los clientes. • **Respuesta a los incidentes.** Microsoft trabaja con un equipo global de respuesta a incidentes y eventos las 24 horas del día y los 7 días de la semana para ayudar a mitigar las amenazas de ataques y actividades malintencionadas.	centralizados que administran la gran cantidad de información generada por los dispositivos del entorno, proporcionando alertas puntuales. Además, existen varios niveles de supervisión, registro e informes para proporcionar visibilidad a los clientes. • **Aplicación de revisiones.** Los sistemas de implementación integrados administran la distribución e instalación de revisiones de seguridad. Los clientes pueden aplicar procesos de administración de revisiones similares para las máquinas virtuales implementadas en Azure. • **Protección antivirus y antimalware.** Microsoft Antimalware se integra en los servicios en la nube y se puede habilitar para máquinas virtuales para ayudar a identificar y quitar virus, spyware y otro software malintencionado, así como para proporcionar protección en tiempo real. Los clientes también pueden ejecutar soluciones antimalware de los asociados en sus máquinas virtuales. • **Detección de intrusiones y DDoS** (Distributed Denial of Service)**.** Los sistemas de detección y prevención de intrusiones, la prevención de ataques por denegación de servicio (DDoS), las pruebas de penetración regulares y las herramientas forenses ayudan a identificar y mitigar las amenazas desde fuera y dentro de Azure. • **Ausencia de privilegios por derecho.** El personal de operaciones y soporte técnico de Microsoft no tiene libre acceso a los datos de los clientes, ya que se les deniega de forma predeterminada. Cuando se concede, el acceso se administra y se registra de forma cuidadosa. El acceso del centro de datos a los sistemas que almacenan los datos de los clientes se controla estrictamente por medio de procesos de bloqueo de seguridad. • **Aislamiento.** Azure utiliza el aislamiento de red para impedir la comunicación no deseada entre las implementaciones, y los controles de acceso que bloquean a los usuarios no autorizados. Las máquinas virtuales no reciben tráfico de entrada desde Internet a menos que los clientes las configuren para ello. • **Redes virtuales de Azure.** Los clientes pueden decidir asignar varias implementaciones a una red virtual aislada y permitir que esas implementaciones se comuniquen entre sí a través de direcciones IP privadas. • **Comunicaciones cifradas.** La criptografía SSL (Secure Sockets Layer) y TLS (Transport Security Layer) integrada permite a los clientes cifrar las comunicaciones dentro de las implementaciones y entre ellas, desde Azure hasta los centros de datos locales y desde Azure hasta los administradores y usuarios. • **Conexión privada.** Los clientes pueden usar ExpressRoute para establecer una conexión privada con los centros de datos de Azure, manteniendo el tráfico fuera de Internet. • **Cifrado de datos.** Azure facilita una amplia gama de funcionalidad de cifrado, hasta AES-256, por lo que ofrece a los clientes la flexibilidad de implementar los métodos que mejor se ajustan a sus necesidades. • **Identidad y acceso.** Active Directory de Azure permite a los clientes administrar el acceso a Azure, Office 365 y otras muchas aplicaciones en la nube. La autenticación multifactor y la supervisión del acceso ofrecen seguridad mejorada.

Ésta y otra información relevante, como por ejemplo, la Seguridad Aplicativa (WAF), puede consultarse en el Centro de Confianza de Microsoft Azure (véase http://azure.microsoft.com/es-es/support/trust-center/security/).

En relación con la norma ISO/IEC 27018:2014 citada y como se dijo anteriormente, Microsoft Azure ya cumple con los controles que establece dicha norma, habiendo sido auditado por un tercero independiente, el British Standards Institute (BSI). Esto significa que Microsoft fue el primer proveedor principal de servicios de cómputo en la nube que adoptó el código de práctica establecido por la ISO/IEC 27018.

Por lo tanto Azure es la plataforma de nube de Microsoft que cumple tanto con la norma ISO/IEC 27001 como con la norma ISO/IEC 27018 lo cual ayuda al cumplimiento también por sus clientes y es una clara ventaja competitiva para éstos al poder hacer uso de servicios de nube que cumplen con altos estándares internacionales en materia de seguridad y de protección de datos personales. Al respecto, puede verse más información en el vínculo electrónico http://azure.microsoft.com/es-es/support/trust-center/compliance/

5. Lista de comprobación sobre medidas de seguridad para un entorno digital

El siguiente cuestionario tiene como objetivo que Usted pueda comprobar si cuenta con las medidas de seguridad adecuadas en sus equipos de cómputo.

Medida de seguridad	Manual del INAI	Comprobación	Sí	No	No aplica	Mejora a implementar	Con Microsoft
1. Control de accesos y contraseñas	C.3.4	**1.1.** ¿Ha creado diferentes cuentas de usuario, con el perfil correspondiente, para cada usuario que tiene acceso al equipo de cómputo donde se tratan los datos personales?	○	○	○	○	**Control de cuentas de usuario**
		1.2. El tipo de cuenta (estándar, administrador o invitado) de cada usuario, ¿se otorga en función a su perfil y necesidades de tratamiento de datos personales?	○	○	○	○	
	C.3.1 y C.3.4	**1.3.** ¿Cada usuario tiene asignada una contraseña?	○	○	○	○	
	C.3.1	**1.4.** ¿Las contraseñas se cambian periódicamente o en caso de que estén expuestas a riesgos para su confidencialidad?	○	○	○	○	
	C.3.2	**1.5.** ¿Las contraseñas asignadas a los usuarios son sólidas o seguras?	○	○	○	○	**Comprobador de contraseñas**
	C.3.4	**1.6.** ¿Da de baja a los usuarios cuando éstos dejan de necesitar, por el motivo que fuera, el acceso a los datos personales?	○	○	○	○	**Control de cuentas de usuario**
		1.7. ¿Revisa que el acceso otorgado a los usuarios es el necesario para el desarrollo de sus funciones?	○	○	○	○	
2. Bloqueo de sesión	C.3.3	**2.1.** Cuando se ausenta de su mesa, ¿cierra la sesión de usuario en su equipo de cómputo o dispositivo?	○	○	○	○	**Protector de pantalla**
		2.2. Su dispositivo electrónico, ¿tiene activada la contraseña de usuario para evitar accesos por otros usuarios?	○	○	○	○	

Medida de seguridad	Manual del INAI	Comprobación	Sí	No	No aplica	Mejora a implementar	Con Microsoft
2. Bloqueo de sesión (cont.)	**C.3.3**	**2.3.** ¿Tiene activada una pantalla de bloqueo que requiera su contraseña para reiniciar la sesión?	○	○	○	○	**Protector de pantalla**
3. Filtro de tráfico (muro de protección o firewall)	**C.5.1**	**3.1.** ¿Tiene instalado o usa un muro de protección (firewall)?	○	○	○	○	**Firewall de Windows**
		3.2. ¿Mantiene activado el muro de protección y comprueba su estado?	○	○	○	○	
		3.3. ¿Atiende a las notificaciones del muro de protección cuando le avisan de descargas que pueden ser un riesgo o intento de acceso no autorizados?	○	○	○	○	
		3.4. ¿Cambia la configuración del muro de protección para bloquear las conexiones en virtud de que la red sea privada o pública?	○	○	○	○	
4. Antivirus y antimalware	**C.5.1**	**4.1.** ¿Tiene instalado un antivirus y hace uso del mismo para revisar software o aplicaciones en busca de virus y otras amenazas?	○	○	○	○	**Microsoft Security Essentials y Microsoft Defender**
	C.5.1. y C.5.2	**4.2.** Cuando descarga archivos de Internet o los copia de un dispositivo externo, ¿revisa que no tengan virus o se trate de software malicioso (malware)?	○	○	○	○	
	C.5.1 y C.2	**4.3.** ¿Revisa con frecuencia que su equipo de cómputo no tenga virus u otro software malicioso?	○	○	○	○	
	C.5.1 y C.4	**4.4.** ¿Mantiene actualizado el software antivirus y antimalware para evitar riesgos por virus o software malicioso nuevo?	○	○	○	○	
		4.5. ¿Ha configurado el software antivirus o antimalware de manera que le ofrezca el máximo nivel de protección?	○	○	○	○	

Medida de seguridad	Manual del INAI	Comprobación	Sí	No	No aplica	Mejora a implementar	Con Microsoft
4. Antivirus y antimalware (cont.)	**C.5.1**	**4.6.** ¿Revisa o atiende a los avisos del software antivirus o malicioso en caso de alerta sobre un virus o software malicioso?	○	○	○	○	**Microsoft Security Essentials y Microsoft Defender**
		4.7. ¿Consulta boletines, sitios o páginas web o centros de información sobre virus y otras amenazas?	○	○	○	○	
5. Cifrado	**C.3.1**	**5.1.** ¿Utiliza alguna herramienta de cifrado para evitar el acceso a datos personales por personas no autorizadas?	○	○	○	○	**BitLocker**
		5.2. En su caso, ¿cifra todo el contenido del equipo o sólo las carpetas o archivos que contienen datos personales?	○	○	○	○	
		5.3. Si distribuyen soportes (CDs, DVDs, etc.) con datos personales, ¿cifra el contenido para evitar que terceros no autorizados puedan tener acceso a los mismos?	○	○	○	○	
6. Copias de seguridad	**A.5**	**6.1.** ¿Tiene activado algún software que le permita hacer copias automáticas de los datos personales y otra información?	○	○	○	○	**Historial de archivos**
		6.2. Periódicamente, ¿hace copias de seguridad de los datos personales u otra información?	○	○	○	○	
		6.3. ¿Comprueba que las copias de seguridad funcionan correctamente y que puede recuperar los datos personales u otra información si es necesario?	○	○	○	○	
		6.4. ¿Mantiene las copias de seguridad durante algún período preestablecido y, en su caso, atendiendo a la normatividad aplicable?	○	○	○	○	
		6.5. ¿Guarda las copias de seguridad en un lugar seguro?	○	○	○	○	

Medida de seguridad	Manual del INAI	Comprobación	Sí	No	No aplica	Mejora a implementar	Con Microsoft
7. Navegación segura	**C.5.2**	**7.1.** Cuando navega por Internet, ¿tiene activado algún filtro que le ayude con la seguridad y proteja su privacidad?	○	○	○	○	**Windows SmartScreen**
		7.2. ¿Presta atención a los avisos y advertencias del filtro?	○	○	○	○	
		7.3. Si descarga software o archivos de Internet, antes de instalarlos o ejecutarlos, ¿comprueba que proceden de una fuente confiable y que no supongan un riesgo para su equipo de cómputo o los datos personales que trata?	○	○	○	○	
		7.4. ¿Ha configurado el filtro de manera que le ofrezca el mayor nivel de protección?	○	○	○	○	
	C.3.4	**7.5.** ¿Controla quién puede instalar o ejecutar software o aplicaciones desde Internet de manera que evite riesgos por virus, software malicioso u otros?	○	○	○	○	
8. Seguridad en Internet	**C.5.1 y C.5.2**	**8.1.** Cuando navega por Internet, ¿se asegura de no descargar o ejecutar software o aplicaciones que pudieran dañar su equipo de cómputo o los datos personales a través de la configuración del navegador o de un software antivirus o antimalware?	○	○	○	○	**Internet Explorer**
	C.5.2 y C.5.4	**8.2.** ¿Tiene un navegador que le permite configurar un nivel alto de seguridad y proteger su privacidad?	○	○	○	○	
	C.4 y C.5.2	**8.3.** ¿Mantiene actualizado el software del navegador para evitar riesgos de seguridad?	○	○	○	○	

Medida de seguridad	Manual del INAI	Comprobación	Sí	No	No aplica	Mejora a implementar	Con Microsoft
9. Comunicaciones seguras: validación de destinatarios y seguridad de la información intercambiada	**C.5.2 y C.6.2**	**9.1.** ¿Ha activado o mantiene activada la función que impide que se descarguen automáticamente imágenes en mensajes de correo electrónico en formato HTML para garantizar su privacidad?	○	○	○	○	**Outlook**
		9.2. ¿Ha activado o mantiene activada la función que le avisa antes de descargar contenido al editar o reenviar correo electrónico o responder al mismo?	○	○	○	○	
	C.6.2	**9.3.** Si envía datos personales sensibles, ¿tiene activada la opción de cifrar el contenido y datos adjuntos?	○	○	○	○	
	C.6.1	**9.4.** ¿Tiene activada la función de comprobación automática de nombres?	○	○	○	○	
10. Revisar el software instalado	**C.2**	**10.1.** ¿Revisa con frecuencia el software instalado para comprobar si es el necesario o si hay software que no debería estar instalado?	○	○	○	○	**Panel de control**
		10.2. Si encuentra software que no es necesario o que podría no ser confiable, ¿utiliza un software de escaneo para asegurarse de que no se trata de un riesgo?	○	○	○	○	
	C.2 y C.5.1	**10.3.** ¿Desinstala el software malicioso que ha encontrado o utiliza un antivirus o antimalware para evitar que pueda causar daños al equipo de cómputo o a los datos personales?	○	○	○	○	
11. Actualización del software y de las herramientas de seguridad	**C.1**	**11.1.** ¿Actualiza con frecuencia el software que tiene instalado para tener las últimas versiones?	○	○	○	○	**Windows Update**
		11.2. ¿Tiene la posibilidad de activar actualizaciones automáticas del software?	○	○	○	○	
		11.3. ¿Consulta alertas de seguridad de alguna fuente (boletín, sitio o página web, centro de información, etc.)?	○	○	○	○	

Con la finalidad de que pueda ser de utilidad práctica, para Windows 8.1, Windows RT 8.1 y Windows 10, a continuación se incluye una lista de comprobación de seguridad con herramientas o productos de Microsoft que son relevantes:

Lista de comprobación de seguridad de Microsoft	
Centro de actividades 	Compruebe en el Centro de actividades que el firewall está activado, la protección antimalware actualizada y el equipo configurado para instalar las actualizaciones automáticamente.
Windows Defender 	Use Windows Defender para evitar la instalación de virus, spyware y otro software malicioso o no deseado en el equipo sin su conocimiento.
Windows SmartScreen 	Windows SmartScreen le ayuda a proteger su PC y le avisa antes de ejecutar aplicaciones y archivos no reconocidos que se descargaron de Internet.
Control de cuentas de usuario (UAC) 	Asegúrese de que Control de cuentas de usuario pida permiso antes de instalar software o abrir ciertos tipos de aplicaciones que podrían llegar a ser perjudiciales para el equipo o exponerlo a amenazas de seguridad.
Historial de archivos 	Use el Historial de archivos para hacer regularmente copias de seguridad de los archivos, como documentos, de manera automática. Si el equipo tiene un error de hardware, puede restaurar cualquier versión de los archivos que considere más importantes.
Windows Update 	Use Windows Update para descargar e instalar de manera automática las actualizaciones más recientes para el equipo.
Firewall de Windows 	Active el Firewall de Windows para ayudar a impedir que hackers o software malicioso obtengan acceso al equipo a través de Internet.

Esta lista también está disponible en: http://windows.microsoft.com/es-mx/windows-8/security-checklist-windows En el caso de Windows 10, puede ver también más información sobre seguridad y privacidad en: http://windows.microsoft.com/en-us/windows-10/security-privacy

6. Diez consejos prácticos para proteger su equipo o dispositivo contra virus y otras amenazas

Microsoft le recomienda seguir estos diez consejos prácticos para proteger su equipo o dispositivo contra los virus y otras amenazas, así como mantener seguros los datos personales y la información:

Decálogo de consejos prácticos para aumentar la seguridad de su equipo y proteger su privacidad

1. Instale, use y mantenga actualizada una aplicación antimalware o antivirus.
2. Use un firewall (muro de protección).
3. Mantenga Windows actualizado.
4. Asegúrese de activar el Control de cuentas de usuario.
5. No abra mensajes de correo electrónico de remitentes desconocidos o archivos adjuntos que desconozca.
6. Use un bloqueador de elementos emergentes, tales como ventanas pop-up, con el explorador de Internet.
7. Si usa Internet Explorer, asegúrese de que el filtro SmartScreen está activado.
8. Preste atención a las notificaciones de Windows SmartScreen.
9. Use la configuración de privacidad de su explorador de Internet.
10. Borre la memoria caché de Internet y el historial de exploración.

7. Anexos

7.1. ¿Qué significa?

7.1.1. Conceptos en protección de datos personales y seguridad

A continuación se incluyen las definiciones más relevantes en protección de datos personales y seguridad, de manera que se presenta cada concepto con la correspondiente definición que proporciona la LFPDPPP o, en su caso, su Reglamento y, por último, un ejemplo práctico.

Concepto	Definición	Ejemplo
Datos personales	Cualquier información concerniente a una persona física identificada o identificable (fracción V del art. 3 de la LFPDPPP).	El nombre y apellidos, número de CURP, número de pasaporte, fotografía, voz o cualquier otro dato que permitan identificar a su titular.
Datos personales sensibles	Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual (fracción VI del art. 3 de la LFPDPPP).	El grado de discapacidad física de una persona, su pertenencia a un sindicato, el origen racial, su religión, etc.
Titular	La persona física a quien corresponden los datos personales (fracción XVII del art. 3 de la LFPDPPP).	La persona física, cualquiera que sea su edad y si se trata de un mexicano o extranjero.
Base de datos	El conjunto ordenado de datos personales referentes a una persona identificada o identificable (fracción II del art. 3 de la LFPDPPP).	Un listado de personas en soporte electrónico que permita la búsqueda por un criterio lógico, como por ejemplo el apellido, el número de pasaporte, etc.

Concepto	Definición	Ejemplo
Soporte electrónico	Medio de almacenamiento al que se pueda acceder sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms (fracción X del artículo 2 del Reglamento de la LFPDPPP).	Un CD, USB o incluso el disco duro de una máquina son ejemplos de soportes electrónicos.
Soporte físico	Medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales (fracción XI del art. 2 del Reglamento de la LFPDPPP).	El papel es un claro ejemplo de soporte físico, por lo que los formularios, boletos, etc., son soportes físicos.
Tratamiento	La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales (fracción XVIII del art. 3 de la LFPDPPP).	Cualquier operación que se lleve a cabo con respecto a los datos personales, como por ejemplo introducirlos en una base de datos, consultarlos o imprimirlos, así como comunicarlos o revelarlos a un tercero.
Responsable del tratamiento	Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales (fracción XIV del art. 3 de la LFPDPPP).	Quien decide sobre el tratamiento de los datos personales, ya sea por ejemplo, una empresa respecto del tratamiento de los datos personales de sus clientes y/o empleados, la guardería respecto de los datos de los padres y niñas/niños a los que presta el servicio correspondiente o el taller de restauración de autos respecto de sus clientes.

Concepto	Definición	Ejemplo
Encargado del tratamiento	La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable (fracción IX del art. 3 de la LFPDPPP). La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio (art. 49 del Reglamento de la LFPDPPP).	La empresa "B", que proporciona servicios de cómputo en la nube que implican el tratamiento de datos personales de los que es responsable la empresa "A". Por ejemplo, el almacenamiento de bases de datos personales de la empresa "A" en la nube ofrecida por la empresa "B".
Tercero	La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos (fracción XVI del art. 3 de la LFPDPPP).	El tercero es, por ejemplo, una empresa que recibe la base de datos de clientes de la que otra empresa es responsable para enviar publicidad, decidiendo sobre el tratamiento.
Remisión	La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano (fracción IX del artículo 2 del Reglamento de la LFPDPPP).	Cuando la empresa "A" contrata a la empresa "B" para que, en su nombre y siguiendo sus instrucciones, elabore una encuesta de satisfacción entre sus clientes del servicio que les ofrece.
Transferencia	Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento (fracción XIX del art. 3 de la LFPDPPP).	Cuando la empresa "A" le transfiere su base de datos de clientes a la empresa "B" para que ésta, a su vez, como responsable del tratamiento, haga uso de la misma, por ejemplo, con fines de publicidad.

Concepto	Definición	Ejemplo
Bloqueo	La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde (fracción III del art. 3 de la LFPDPPP).	Bloquear informáticamente uno o varios registros en una base de datos, cumpliendo con los requisitos de la definición de la Ley.
Supresión	Actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable (fracción XII del art. 2 del Reglamento de la LFPDPPP).	Destruir físicamente el CD (u otro soporte físico) en el que estén los datos personales, siguiendo el procedimiento establecido por el responsable del tratamiento.

7.1.2. Conceptos técnicos

Por lo que se refiere a términos técnicos, tales como muro de protección (firewall), software antivirus o software malicioso, a continuación se incluyen los conceptos más relevantes, su definición y, en su caso, un ejemplo práctico.

Concepto	Definición	Ejemplo
Botnet	Una *botnet* es una red de computadoras que se utilizan por los delincuentes para el envío de mensajes de correo electrónico no deseados, propagar virus o atacar computadoras y servidores para cometer otros delitos y fraudes. Su computadora, sin su conocimiento, puede convertirse en una *bot* (diminutivo de robot), también conocido como un zombi, si es víctima del software malicioso utilizado por los delincuentes. Es importante que mantenga la seguridad de su equipo para evitar ser parte de una *botnet*.	Entre los usos frecuentes de las botnets se encuentran los ataques de denegación de servicio distribuidos (en inglés, *Distributed Denial of Service*, DDoS) o el envío masivo de correos electrónicos no solicitados (en inglés, *spam*).
Muro de protección (firewall)	Es un programa informático o un componente de hardware, como por ejemplo un router, que ayuda a evitar el acceso por hackers, virus y gusanos u otro software malicioso que trata de llegar a su equipo a través de Internet.	Microsoft Firewall
Phishing	Consiste en que alguien, por medios electrónicos, como por ejemplo, el correo electrónico o un formulario web, intente obtener de manera fraudulenta información personal, como el nombre de usuario y contraseña de una dirección de correo electrónico o de una cuenta de banca electrónica u otra información bancaria, para utilizarla para sus propios fines y, por tanto, de forma ilícita.	Correo electrónico que supuestamente se recibe del banco en el que, con alguna excusa, se pide al destinatario que proporcione por este medio nombre de usuario y contraseña de banca electrónica.

Concepto	Definición	Ejemplo
Robo (o suplantación) de identidad	El robo o suplantación de identidad (en inglés, phishing) es una clase de fraude en la que un tercero roba los datos personales, tales como nombre de usuario, contraseña, número de tarjeta de crédito o una identificación oficial (CURP, número de pasaporte, etc.), utilizándolos para hacer transacciones no autorizadas en nombre del titular de los datos.	Uso no autorizado de los datos de una tarjeta de crédito o débito para hacer una compra suplantando la identidad del titular de tarjeta.
Software antivirus	Es un programa informático que detecta y permite tomar medidas para eliminar programas de software malicioso, tales como virus o gusanos.	Microsoft Security Essentials (para Windows 7 y Windows Vista) y Windows Defender (para Windows 8, Windows RT, Windows 8.1, RT 8.1 y Windows 10)
Software espía *(spyware)*	Es un tipo de software que se instala en el equipo para observar y registrar las actividades del usuario. Algunos tipos de spyware registran las pulsaciones de teclas y la información que el usuario especifica en sitios web o en otros programas. Después, dicha información se usa en robos de identidad o para enviar publicidad personalizada que no ha sido solicitada. Estos programas pueden instalarse en el equipo de muchas maneras, pero normalmente están ocultos dentro de programas de software como protectores de pantalla, cursores animados, juegos o aplicaciones gratuitas.	Los troyanos o los *keyloggers* son ejemplos de software espía que buscan conseguir información como nombres de usuario y/o contraseñas de acceso a cuentas de usuario.
Software malicioso (malware)	Son programas informáticos que han sido diseñados para causar daños en un equipo o en los archivos, poniendo en riesgo al equipo o a la información.	Gusanos, troyanos u otro software que interfiere con el buen funcionamiento del equipo.
Virus informático	Es un programa diseñado para propagarse de una computadora a otra e interferir con su funcionamiento, pudiendo causar daños o borrar los datos, personales o no, e incluso borrar todo el disco duro.	Melissa, I Love You o Cryptolocker, son ejemplos de algunos virus famosos por su peligrosidad.

Puede ver más términos de seguridad, tales como control ActiveX, cookie, filtro de Internet, ingeniería social o ventana emergente, en el siguiente vínculo electrónico http://www.microsoft.com/es-xl/security/resources/default.aspx#Términos-de-seguridad

7.2. Más información y recursos

A continuación se incluyen ligas y referencias a documentos, vídeos y otra información que puede ser de interés en relación con la protección de datos personales y la seguridad. Dicha información es proporcionada, en su caso, por el INAI y Microsoft, respectivamente.

También se incluye una referencia a la normatividad aplicable en materia de protección de datos personales y seguridad publicada en el Diario Oficial de la Federación (DOF) hasta la fecha de publicación del este Manual.

7.2.1. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
www.inai.org.mx

Seguridad de los datos personales: documentos de interés		
	**Título**	**Manual en materia de seguridad de datos personales para MiPyMEs y organizaciones pequeñas**
	Fecha	Julio 2014
	Vínculo electrónico	http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_seguridad_mipymes_julio2014.pdf
	**Título**	**Guía para cumplir con los principios y deberes de la Ley Federal de Protección Datos Personales en Posesión de los Particulares**
	Fecha	Julio 2014
	Vínculo electrónico	http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_julio2014.pdf
	**Título**	**Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales (Completa)**
	Fecha	Junio 2015
	Vínculo electrónico	http://inicio.inai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf
	**Título**	**Metodología de Análisis de Riesgo BAA**
	Fecha	Marzo 2014
	Vínculo electrónico	http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Riesgo_BAA_marzo2014.pdf
	**Título**	**Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales**
	Fecha	Noviembre 2014
	Vínculo electrónico	http://inicio.ifai.org.mx/DocumentosdeInteres/Guía%20implementación%20SGSDP%20-%20Noviembre2014.pdf

La lista actualizada de documentos puede verse en http://www.inai.org.mx

Con la entrada en vigor de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), el 5 de mayo de 2015, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), cambió su nombre por el de Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

7.2.2. Centros de información, recursos y ayuda en línea de Microsoft

Microsoft
www.microsoft.com/es-mx/default.aspx

Centros de información, recursos y ayuda en línea		
	**Centro**	**Centro de seguridad y protección** (Seguridad para su computadora, privacidad digital y seguridad en línea)
	Vínculo electrónico	http://www.microsoft.com/es-xl/security/default.aspx
	Centro	**Centro de respuesta de seguridad**
	Vínculo electrónico	http://www.microsoft.com/security/scanner/es-xl/default.aspx
	Centro	**Centro de protección contra el malware** [en inglés]
	Vínculo electrónico	http://www.microsoft.com/security/portal/mmpc/default.aspx
	Centro	**Centro de confianza de Office 365**
	Vínculo electrónico	http://office.microsoft.com/es-es/business/centro-de-confianza-office-365-seguridad-informatica-FX103030390.aspx
	**Centro**	**Centro de descargas**
	Vínculo electrónico	http://www.microsoft.com/es-mx/download/
	Centro	**Centro de seguridad TechCenter (TechNet)**
	Vínculo electrónico	http://technet.microsoft.com/es-mx/security/
	Centro	**Centro de desarrolladores de seguridad (MSDN)** [en inglés]
	Vínculo electrónico	http://msdn.microsoft.com/es-mx/security/

7.2.3. Normatividad básica sobre protección de datos personales y medidas de seguridad

Diario Oficial de la Federación
www.dof.gob.mx

Normatividad básica sobre protección de datos personales y medidas de seguridad		
	**Título**	**Parámetros de Autorregulación en materia de Protección de Datos Personales**
	Fecha	29 de mayo de 2014
	Vínculo electrónico	http://dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014
	**Título**	**Recomendaciones en materia de seguridad de datos personales**
	Fecha	30 de octubre de 2013
	Vínculo electrónico	http://dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013
	**Título**	**Lineamientos del Aviso de Privacidad**
	Fecha	17 de enero de 2013
	Vínculo electrónico	http://dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013
	**Título**	**Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos**
	Fecha	18 de abril de 2012
	Vínculo electrónico	http://dof.gob.mx/nota_detalle.php?codigo=5244229&fecha=18/04/2012
	**Título**	**Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**
	Fecha	21 de diciembre de 2011
	Vínculo electrónico	http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011
	**Título**	**Ley Federal de Protección de Datos Personales en Posesión de los Particulares**
	Fecha	5 de julio de 2010
	Vínculo electrónico	http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

Distribución gratuita