UNIDAD 2

Instituto Tecnológico de Reynosa
Instituto Tecnológico de México

Integrantes:
Castillo Jr Gregorio
Bermúdez Domínguez Juan Carlos
Flores Acosta Sheila Lizeth

Materia:
Auditoria en Tecnologías de la información

Docente:
Miriam Puente Jimenez

Carrera:
TIC’s
8vo Semestre
Grupo 1

Índice

2.1 La protección de datos de carácter personal

La protección de datos de carácter personal es un conjunto de medidas y prácticas destinadas a garantizar la privacidad y la seguridad de la información personal que una persona pueda proporcionar a una entidad o empresa. Esta información puede incluir, entre otros datos, el nombre, la dirección, el número de teléfono, la dirección de correo electrónico, la información financiera y otros datos personales.

La protección de datos de carácter personal se basa en la idea de que estas informaciones son propiedad exclusiva de la persona a la que pertenecen y que su divulgación sin su consentimiento puede poner en riesgo su privacidad, seguridad e incluso su libertad.

La protección de datos de carácter personal implica, entre otras medidas:

- La recopilación de datos solo con el consentimiento explícito de la persona afectada.
- El almacenamiento seguro de los datos para evitar su pérdida, robo o mal uso.
- La limitación del acceso a los datos solo a aquellos que necesiten utilizarlos para fines específicos y autorizados.
- La eliminación segura de los datos cuando ya no sean necesarios o cuando la persona afectada lo solicite.
- La obligación de informar a las personas afectadas en caso de una violación de la seguridad de los datos personales.
- La garantía del derecho a acceder, rectificar y eliminar los datos personales que una empresa o entidad posea.

Estas medidas y otras similares buscan proteger la privacidad y la seguridad de los datos personales de las personas y prevenir el uso no autorizado o malintencionado de estos datos.

En México, las principales leyes y normativas que regulan la protección de datos personales son las siguientes:

1. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP): Esta ley establece los principios, derechos y obligaciones para el tratamiento de los datos personales en posesión de los particulares. La LFPDPPP establece la obligación de obtener el consentimiento del titular de los datos personales para su tratamiento, así como la obligación de garantizar la confidencialidad y seguridad de los mismos.

2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: Esta ley establece las disposiciones aplicables a las autoridades y entidades del gobierno federal, estatal y municipal que tratan datos personales. La ley establece que estas entidades deben garantizar la protección de los datos personales de las personas, así como su acceso, rectificación, cancelación y oposición.

3. Ley de Transparencia y Acceso a la Información Pública: Esta ley establece el derecho de las personas a acceder a la información que se encuentra en posesión de las autoridades y entidades del gobierno. La ley establece que los datos personales que se encuentran en la información pública deben ser protegidos y tratados de acuerdo a la LFPDPPP.

Además de estas leyes, existen otras normativas y regulaciones que complementan la protección de datos personales en México, como el Reglamento de la LFPDPPP, las guías y lineamientos emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y la normativa emitida por otras autoridades en materia de protección de datos personales.

2.2 La protección jurídica de los programas de computadora

La protección jurídica de los programas de computadora se refiere al conjunto de leyes y regulaciones que garantizan la propiedad intelectual y los derechos de autor sobre los programas de computadora. Esto significa que el creador de un programa de computadora tiene derecho a controlar cómo se utiliza su obra y a recibir una compensación por su uso.

La protección legal de los programas de computadora varía según el país, pero en general se rige por las leyes de derechos de autor y patentes. La mayoría de los países consideran a los programas de computadora como obras protegidas por derechos de autor, lo que significa que el creador del programa tiene el derecho exclusivo de controlar la reproducción, distribución y exhibición del programa.

Además, los programas de computadora también pueden estar protegidos por patentes, lo que significa que el creador tiene el derecho exclusivo de utilizar, vender o licenciar su invención.

En general, la protección legal de los programas de computadora tiene como objetivo fomentar la innovación y el desarrollo tecnológico, proteger los derechos de los creadores de programas y garantizar que los programas se utilicen de manera legal y ética.

En México, la protección jurídica de los programas de computadora está regulada por la Ley Federal del Derecho de Autor (LFDA) y la Ley de la Propiedad Industrial (LPI). La LFDA establece que los programas de computadora son obras protegidas por derechos de autor, y que el creador de un programa tiene el derecho exclusivo de controlar su reproducción, distribución, exhibición y ejecución. La ley también establece que los programas de computadora pueden ser registrados en el Instituto Nacional del Derecho de Autor (INDAUTOR) para obtener una protección adicional.

Por su parte, la LPI establece que los programas de computadora pueden ser protegidos mediante patentes, siempre y cuando cumplan con los requisitos de patentabilidad establecidos en la ley. Es importante destacar que la protección mediante patentes sólo cubre la invención tecnológica del programa y no su expresión creativa.

En resumen, en México la protección jurídica de los programas de computadora está regulada tanto por la Ley Federal del Derecho de Autor como por la Ley de la

Propiedad Industrial, que establecen los derechos y mecanismos legales necesarios para proteger los programas de computadora como obras de propiedad intelectual.

En México, la protección jurídica de los programas de computadora está regulada principalmente por los siguientes artículos de la Ley Federal del Derecho de Autor (LFDA):

- Artículo 101: Este artículo define al programa de computadora como una obra protegida por derechos de autor y establece que el creador de un programa tiene el derecho exclusivo de explotar su obra y de autorizar su uso por terceros.
- Artículo 109: Este artículo establece que los programas de computadora pueden ser registrados en el Instituto Nacional del Derecho de Autor (INDAUTOR) para obtener una protección adicional.
- Artículo 113: Este artículo establece que los programas de computadora están protegidos por los derechos de autor durante toda la vida del autor y por 100 años después de su muerte.
- Artículo 148: Este artículo establece que la violación de los derechos de autor sobre un programa de computadora constituye un delito penal y establece las sanciones correspondientes.
- Artículo 149: Este artículo establece que el titular de los derechos de autor sobre un programa de computadora puede solicitar medidas cautelares para evitar su reproducción, distribución, exhibición o ejecución ilegal.

Por otro lado, la Ley de la Propiedad Industrial también establece disposiciones para la protección de los programas de computadora mediante patentes. Los artículos más relevantes de esta ley en relación con los programas de computadora son:

- Artículo 16: Este artículo establece los requisitos de patentabilidad para los programas de computadora.
- Artículo 19: Este artículo establece que la patente otorga al titular el derecho exclusivo de explotar la invención patentada y de prohibir que terceros la utilicen sin su autorización.
- Artículo 97: Este artículo establece las sanciones para la infracción de las patentes, incluyendo la indemnización por daños y perjuicios y la posibilidad de iniciar acciones penales.

2.3 Las bases de datos y multimedia

La protección en las bases de datos y multimedia se refiere a las medidas de seguridad que se implementan para proteger la información almacenada en estas bases de datos y medios multimedia. Esta protección puede incluir:

Acceso restringido: Se utiliza para limitar el acceso a la base de datos o multimedia sólo a personas autorizadas, con permisos específicos y niveles de seguridad.

Encriptación: Los datos se cifran mediante algoritmos criptográficos para evitar el acceso no autorizado y protegerlos contra posibles ataques.

Copias de seguridad: Se realizan copias de seguridad periódicas de los datos almacenados para asegurarse de que, en caso de fallo del sistema o de ataques maliciosos, se pueda recuperar la información.

Firewall: Es una medida de seguridad que ayuda a prevenir el acceso no autorizado a la base de datos o multimedia.

Verificación de integridad: Se realiza una comprobación regular para asegurarse de que los datos almacenados no se hayan visto comprometidos y estén completos.

Protección contra virus y malware: Se utilizan programas antivirus y antimalware para detectar y eliminar virus y otros programas maliciosos que puedan afectar a la base de datos o multimedia.

Monitoreo de actividad: Se monitorea constantemente la actividad en la base de datos o multimedia para detectar posibles amenazas de seguridad y tomar medidas preventivas.

Todas estas medidas de protección ayudan a mantener la integridad y seguridad de los datos almacenados en bases de datos y multimedia, evitando posibles ataques y reduciendo los riesgos de pérdida de información.

Entre las medidas que establece la ley, se encuentran las siguientes:

Consentimiento informado: Se debe obtener el consentimiento del titular de los datos personales para su tratamiento, y se deben informar las finalidades y usos específicos para los que serán utilizados.

Finalidades específicas: Se deben establecer finalidades específicas y legítimas para el tratamiento de los datos personales, y no se deben utilizar para otros fines diferentes a los previstos.

Calidad de los datos: Los datos personales deben ser exactos, completos y actualizados, y se deben tomar medidas para mantenerlos actualizados y eliminar los datos innecesarios.

Seguridad: Se deben implementar medidas de seguridad técnicas, administrativas y físicas para proteger los datos personales contra el acceso no autorizado, la pérdida o la alteración.

Transferencia de datos: La transferencia de datos personales a terceros debe realizarse con el consentimiento del titular y en cumplimiento con la ley.

Derechos ARCO: Los titulares de los datos personales tienen derecho a acceder, rectificar, cancelar u oponerse al tratamiento de sus datos personales.

Responsabilidad: Los responsables del tratamiento de los datos personales son responsables de cumplir con las obligaciones establecidas por la ley y deben tomar medidas para garantizar la protección de los datos personales.

Es importante destacar que estas son sólo algunas de las medidas establecidas por la ley, y que existen otras medidas específicas para cada tipo de base de datos o multimedia. En cualquier caso, es importante cumplir con las obligaciones legales y tomar medidas adecuadas para garantizar la protección de los datos personales.

2.4 Los delitos informáticos

Los delitos informáticos o conocidos como ciberdelitos o delitos electrónicos, son actividades ilegales que se cometen utilizando las TIC como una herramienta, como objeto o medio para cometerlos. Estos delitos informáticos pueden incluir una amplia gama de actividades ilegales que van desde el acceso no autorizado a sistemas informáticos hasta la distribución de material ilegal a través de la red, para entrar más en contexto podemos mencionar unos ejemplos de delitos que se pueden encontrar en casos reales como violación a la privacidad, la estafa, el robo, la distribución de material ilegal, la difamación, entre otros.

Los delitos informáticos más comunes se encuentran en:

- Acceso no autorizado: es un acceso ilegal a sistemas informáticos y redes sin autorización.
- Ataques de denegación de servicio (DDoS): el uso de software malicioso para inundar un sitio web o servidor con tráfico para hacer que sea inaccesible.
- Phishing: el uso de mensajes de correo electrónico o sitios web fraudulentos para engañar a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito.
- Malware: el uso de software malicioso para dañar sistemas informáticos, robar información o espiar a los usuarios.
- Robo de identidad: el uso de información personal robada para realizar actividades ilegales como compras en línea, solicitar préstamos o tarjetas de crédito.
- Fraude en línea: la realización de actividades fraudulentas, como vender productos falsificados o no entregados, o el uso de información robada para realizar compras ilegales.
- Distribución de material ilegal: la distribución de material ilegal como pornografía infantil o información confidencial robada.

Los delitos informáticos pueden ser difíciles de investigar y prevenir debido a la naturaleza global de internet y la facilidad de ocultamiento de los delincuentes detrás de identidades falsas o en línea. Para combatir los delitos informáticos, se han

desarrollado leyes y normativas específicas, así como equipos especializados de fuerzas de seguridad que se dedican a investigar y prevenir estos delitos. Es importante estar al tanto de las amenazas cibernéticas y tomar medidas de precaución para proteger nuestra información personal y financiera en línea.

Los delitos informáticos se originaron con el crecimiento de la informática y el uso de las redes de computadoras. Con el aumento del uso de la tecnología y la conectividad, también aumentó el número de personas que intentaban explotar estas tecnologías para llevar a cabo actividades ilegales.

Uno de los primeros delitos informáticos documentados se remonta a la década de 1960, cuando un estudiante de informática llamado Alan Konrad utilizó una computadora para cometer fraudes bancarios. Konrad utilizó una técnica llamada "salto de línea" para obtener acceso no autorizado a la red de computadoras de un banco y transferir fondos a una cuenta falsa.

Desde entonces, el número y la complejidad de los delitos informáticos han aumentado significativamente. A medida que la tecnología ha avanzado, los delincuentes informáticos han encontrado formas más sofisticadas de aprovechar las vulnerabilidades de los sistemas informáticos y redes. Los delitos informáticos se han convertido en una industria importante, con delincuentes que buscan ganancias financieras y otros objetivos, como la obtención de información confidencial o el sabotaje.

Los delitos informáticos también se han expandido a medida que ha crecido el uso de Internet y las redes sociales, lo que ha permitido a los delincuentes acceder a una gran cantidad de información personal y financiera de las personas. Además, la globalización y la interconexión de las redes informáticas han hecho que sea más fácil para los delincuentes operar desde cualquier lugar del mundo y dificultar su detección.

Los delitos informáticos son una amenaza cada vez mayor en nuestra sociedad cada vez más digitalizada. Los delincuentes cibernéticos pueden ser individuos o grupos que utilizan la tecnología para llevar a cabo actividades ilegales y fraudulentas, como el robo de información confidencial, el fraude financiero y la distribución de malware. Estos delitos son muy lucrativos para los delincuentes, ya que pueden operar desde cualquier parte del mundo y pueden cometer los delitos sin ser detectados fácilmente.

Los delitos informáticos pueden tener un impacto significativo en las personas y las empresas. Los individuos pueden verse afectados por el robo de identidad y el fraude

en línea, lo que puede resultar en la pérdida de información personal y financiera. Las empresas también pueden ser víctimas de delitos informáticos, lo que puede resultar en la pérdida de información confidencial de la empresa y la pérdida de ingresos.

Para combatir los delitos informáticos, se han establecido leyes y regulaciones específicas en muchos países. En los Estados Unidos, por ejemplo, se ha establecido la Ley de Fraude y Abuso en Computadoras, que establece las penas para los delitos informáticos, como el acceso no autorizado a sistemas informáticos y la destrucción de datos.

Además, se han establecido equipos especializados de fuerzas de seguridad, como la unidad de delitos cibernéticos del FBI, para investigar y prevenir los delitos informáticos. Los individuos y las empresas también pueden tomar medidas para protegerse contra los delitos informáticos, como mantener el software de seguridad actualizado, no hacer clic en enlaces sospechosos o abrir correos electrónicos no solicitados y utilizar contraseñas seguras y únicas.

2.5 Los contratos informáticos

Los contratos informáticos, también conocidos como contratos electrónicos o contratos digitales, son acuerdos legales celebrados por medios electrónicos y tecnológicos en lugar de medios físicos tradicionales, como el papel. Estos contratos pueden abarcar una amplia variedad de transacciones comerciales, desde compras en línea hasta acuerdos empresariales complejos.

Un contrato informático es legalmente vinculante, siempre que se cumplan ciertas condiciones. Por ejemplo, las partes deben haber acordado mutuamente los términos y condiciones del contrato, y el consentimiento debe ser otorgado de manera clara y unívoca. Además, el contrato debe ser legible y accesible para todas las partes, y las firmas electrónicas deben ser seguras y confiables.

Los contratos informáticos se han vuelto cada vez más comunes a medida que más empresas y personas realizan transacciones comerciales en línea. Los beneficios de los contratos informáticos incluyen la facilidad y la rapidez con la que se pueden crear y firmar, la reducción de costos y la mayor eficiencia en la gestión de documentos.

Sin embargo, también hay desafíos y riesgos asociados con los contratos informáticos. Uno de los mayores desafíos es garantizar la validez y la integridad de los contratos en un entorno digital en el que pueden surgir problemas de autenticidad y confidencialidad. Además, las leyes y regulaciones relacionadas con los contratos informáticos aún están evolucionando, lo que puede generar incertidumbre legal.

Tipos de contratos informáticos

Existen varios tipos de contratos informáticos, que varían según el contexto de la transacción y la industria. A continuación, se describen algunos de los tipos más comunes:

1. Contratos de compraventa en línea: Estos son contratos que se realizan a través de tiendas en línea, en los que el comprador realiza una compra en la plataforma digital y se compromete a pagar el precio acordado, mientras que el vendedor se compromete a entregar el producto o servicio adquirido.

2. Contratos de licencia de software: Estos son contratos que establecen los términos y condiciones bajo los cuales se otorga el derecho de utilizar un

software determinado. Estos contratos pueden incluir detalles sobre la duración de la licencia, el alcance de los derechos de uso y cualquier restricción de uso.

3. Contratos de servicios en línea: Estos son contratos que se utilizan para acordar la prestación de servicios en línea, como la creación de un sitio web, el diseño gráfico, la edición de videos, entre otros.

4. Contratos de alojamiento web: Estos son contratos que se utilizan para acordar el alojamiento de un sitio web en un servidor de Internet.

5. Contratos de colaboración: Estos son contratos que se utilizan para establecer los términos y condiciones de una colaboración en línea entre dos o más partes. Por ejemplo, un acuerdo de colaboración puede ser utilizado por desarrolladores de software que trabajan juntos en un proyecto en línea.

6. Contratos de confidencialidad: Estos son contratos que se utilizan para proteger la información confidencial o secreta de una de las partes en una transacción en línea. Por ejemplo, un contrato de confidencialidad puede ser utilizado para proteger la información de propiedad intelectual o secreta de una empresa que se comparte con un contratista o colaborador.

Estos son solo algunos de los tipos de contratos informáticos más comunes, pero hay muchos más, y las características específicas de cada contrato variarán según el contexto y las necesidades de las partes involucradas.

Consideraciones importantes:

Hay algunas consideraciones importantes a tener en cuenta al momento de celebrar un contrato en línea. Aquí hay algunos temas clave que debes conocer:

- Firma electrónica: Para que un contrato informático sea legalmente vinculante, debe haber algún tipo de firma electrónica que autentique la identidad de las partes involucradas y su acuerdo con los términos del contrato. La firma electrónica puede ser tan simple como escribir el nombre o hacer clic en un

botón para aceptar los términos del contrato, o puede implicar métodos más avanzados, como la autenticación biométrica o el uso de códigos de acceso.

- Protección de datos personales: Cuando se celebran contratos informáticos, a menudo se comparte información personal, como nombres, direcciones, números de tarjeta de crédito, etc. Es importante que las partes involucradas en la transacción se aseguren de que sus datos personales estén protegidos y que el contrato incluya disposiciones claras sobre cómo se manejarán y protegerán los datos personales.

- Leyes aplicables: Los contratos informáticos pueden involucrar a partes de diferentes países o jurisdicciones legales. En estos casos, es importante que el contrato establezca la ley aplicable que regirá el contrato y cualquier disputa que pueda surgir en relación con él.

- Procedimientos de resolución de disputas: Si surge una disputa en relación con un contrato informático, es importante que el contrato incluya disposiciones claras sobre cómo se resolverán las disputas. Esto puede incluir la elección de un tribunal o árbitro, el idioma en el que se llevará a cabo la disputa y los procedimientos específicos para la resolución de la disputa.

- Cambios en los términos del contrato: Los contratos informáticos pueden ser actualizados o modificados con cierta frecuencia. Es importante que el contrato incluya disposiciones claras sobre cómo se manejarán los cambios en los términos del contrato, incluyendo cómo se notificarán a las partes involucradas y cómo se obtendrá el consentimiento para cualquier cambio.

- Propiedad intelectual: Los contratos informáticos a menudo implican la creación o el uso de contenido protegido por derechos de autor u otras formas de propiedad intelectual, como software, música o imágenes. Es importante que el contrato incluya disposiciones claras sobre la propiedad intelectual, incluyendo quién tiene los derechos de propiedad, cómo se pueden usar los contenidos protegidos y cómo se manejarán las infracciones de propiedad intelectual.

- Términos y condiciones de servicio: Los términos y condiciones de servicio son contratos que establecen los términos bajo los cuales se proporcionan servicios en línea, como servicios de redes sociales o servicios de alojamiento web. A menudo, estos términos se presentan en forma de un acuerdo que los usuarios deben aceptar antes de utilizar el servicio. Es importante leer cuidadosamente estos términos y comprender cómo afectarán el uso del servicio.

- Cumplimiento normativo: Algunos tipos de contratos informáticos pueden estar sujetos a leyes y regulaciones específicas, como el Reglamento General de Protección de Datos de la UE o la Ley de Prácticas Comerciales Desleales. Es importante que los contratos informáticos incluyan disposiciones que permitan el cumplimiento con estas leyes y regulaciones.

En conclusión, los contratos informáticos son una parte importante del comercio electrónico y de los negocios en línea. Es importante entender las diferentes formas de contratos informáticos, así como las consideraciones clave que deben tenerse en cuenta al celebrar estos contratos, como la firma electrónica, la protección de datos personales, las leyes aplicables y los procedimientos de resolución de disputas, la propiedad intelectual, los términos y condiciones de servicio y el cumplimiento normativo.

2.6 El intercambio electrónico de datos

El intercambio electrónico de datos (Electronic Data Interchange o EDI, por sus siglas en inglés) se refiere al intercambio de información comercial estructurada entre empresas mediante el uso de sistemas informáticos. En esencia, EDI es un conjunto de protocolos y estándares que permiten a diferentes sistemas informáticos comunicarse y compartir información de manera automatizada, sin la necesidad de intervención humana.

En un proceso típico de EDI, dos empresas establecen una conexión electrónica entre sus sistemas informáticos y acuerdan un conjunto de protocolos y estándares que se utilizarán para intercambiar información. Luego, las empresas pueden enviar y recibir información estructurada, como órdenes de compra, facturas y confirmaciones de envío, directamente entre sus sistemas informáticos, sin la necesidad de imprimir o enviar documentos en papel.

El intercambio electrónico de datos tiene varios beneficios para las empresas, como la reducción de costos y la mejora de la eficiencia al eliminar la necesidad de procesar manualmente la información. También puede mejorar la precisión y la velocidad del procesamiento de datos, reducir los errores y mejorar la visibilidad y el control sobre el flujo de información.

Sin embargo, para implementar EDI, las empresas deben asegurarse de tener la infraestructura adecuada y cumplir con los estándares y protocolos de EDI que se utilizan en su industria. También es importante tener en cuenta las implicaciones de seguridad y privacidad de los datos al implementar EDI, así como la necesidad de mantener la compatibilidad con otros sistemas de información y tecnologías emergentes.

¿Como hacer uso del intercambio electrónico de datos?

El intercambio electrónico de datos (EDI) se utiliza típicamente en el contexto de transacciones comerciales entre empresas, y hay varios pasos clave involucrados en su implementación y uso. Aquí hay una descripción general de los pasos comunes que se deben seguir:

- Identificar los requisitos de EDI: La primera etapa en el uso de EDI es determinar si es apropiado para su negocio. Para hacer esto, es necesario identificar las transacciones comerciales que se realizan con regularidad y evaluar si existe una oportunidad de mejorar la eficiencia y reducir los costos mediante la implementación de EDI. También es importante investigar los estándares y protocolos de EDI que se utilizan en su industria.

- Seleccionar un proveedor de EDI: Una vez que se ha decidido que se desea implementar EDI, el siguiente paso es seleccionar un proveedor de EDI. Hay muchos proveedores de EDI en el mercado, y es importante investigar y comparar las opciones disponibles. Se deben tener en cuenta factores como el costo, la confiabilidad, la escalabilidad y el soporte al cliente al seleccionar un proveedor de EDI.

- Implementar la solución de EDI: Una vez que se ha seleccionado un proveedor de EDI, es necesario implementar la solución. Esto puede implicar la integración de la solución de EDI con los sistemas internos de la empresa, así como la configuración de la conexión de red para permitir el intercambio de datos.

- Realizar pruebas y certificación: Después de la implementación de la solución de EDI, es importante realizar pruebas y certificación para asegurarse de que todo funcione correctamente. Esto puede implicar pruebas internas, así como pruebas con los socios comerciales para garantizar que los datos se estén intercambiando de manera eficiente y efectiva.

- Monitorear y mantener la solución de EDI: Una vez que la solución de EDI está en funcionamiento, es importante monitorear su desempeño y realizar mantenimiento regular para garantizar la continuidad del servicio. También es importante estar al tanto de los cambios en los estándares y protocolos de EDI y actualizar la solución de EDI en consecuencia.

En el área de trabajo

El intercambio de datos en el área de trabajo puede realizarse de diversas formas, dependiendo del tipo de datos que se estén intercambiando, de la frecuencia con que se intercambian y de los sistemas que se utilizan para su intercambio. A continuación, se describen algunas de las formas más comunes de intercambio de datos en el área de trabajo:

- Correo electrónico: El correo electrónico es una forma común de intercambio de datos en el área de trabajo. Los datos se adjuntan a un correo electrónico y se envían a un destinatario específico. El correo electrónico puede ser utilizado para enviar documentos, informes, imágenes y otros tipos de archivos.

- Redes compartidas: Las redes compartidas permiten que los datos se almacenen y se accedan desde múltiples ubicaciones en la empresa. Los datos pueden estar alojados en un servidor o en la nube, y los empleados pueden acceder a ellos desde cualquier dispositivo conectado a la red.

- Sistemas de gestión de contenido: Los sistemas de gestión de contenido permiten a los empleados compartir y colaborar en documentos y otros contenidos. Los sistemas de gestión de contenido pueden incluir wikis, plataformas de colaboración en línea y otros sistemas de software especializados.

- Aplicaciones en línea: Las aplicaciones en línea son otra forma común de intercambio de datos en el área de trabajo. Las aplicaciones pueden estar alojadas en la nube o instaladas localmente, y pueden ser utilizadas para compartir datos, trabajar en equipo y colaborar en proyectos.

- Intercambio electrónico de datos (EDI): Como se mencionó anteriormente, el intercambio electrónico de datos es una forma de intercambio de datos entre empresas. Sin embargo, también se puede utilizar dentro de una empresa para el intercambio de datos entre departamentos o sucursales.

En resumen, el intercambio de datos en el área de trabajo puede realizarse mediante una variedad de métodos, desde el correo electrónico hasta el uso de aplicaciones en línea y sistemas de gestión de contenido. El método elegido dependerá de la naturaleza de los datos que se estén intercambiando, de la frecuencia con que se intercambian y de los sistemas que se utilizan en la empresa.

2.7 La transferencia electrónica de fondos

¿Qué es?

La transferencia electrónica es una operación completamente digital que no requiere el manejo de dinero en efectivo y que se realiza a través del uso de dispositivos tecnológicos —como un ordenador, un celular o un POS— que autorizan al banco a emitir la transferencia.

Estas son cada vez más populares, sobre todo a la hora de enviar dinero al extranjero. Esto se debe a que el proceso está enteramente automatizado y no requiere que el emisor del pago acuda a una sucursal para efectuar la operación. Además, se caracterizan por tener costes muy bajos (en algunas ocasiones son incluso gratuitas) y se llevan a cabo en muy poco tiempo. Las operaciones se pueden efectuar entre dos cuentas que pertenecen a la misma entidad bancaria o instituciones diferentes.

La transferencia electrónica de fondos incluye una gran variedad de transacciones como las siguientes:

- Transferencias a cuentas de terceros (incluso de una entidad financiera a otra).
- Pago por bienes o servicios.
- Pago de tarjetas de crédito.
- Transacciones en comercios electrónicos.
- Pago de nóminas por parte de las empresas.

¿Cómo funcionan?

Para realizar una transferencia es necesario que la persona que envía el pago introduzca la información necesaria para llevar a cabo la operación. Estos datos incluyen la cantidad de dinero a enviar, el día en que debe enviarse el dinero y la cuenta del destinatario de los fondos. En el día solicitado por el emisor del pago, la entidad financiera eliminará los fondos de su cuenta para acreditarlos al destinatario. Los bancos se comunican entre sí a través de una red computarizada que incluye las cuentas de sus clientes y se aseguran de que se efectúen los ajustes necesarios de manera correcta. La red que más se emplea para las transacciones internacionales electrónicas es la SWIFT. En algunos países europeos también se utiliza la red SEPA para este tipo de transacciones.

Todas las transferencias electrónicas de fondos se realizan mediante ACH, es decir, la red de Cámara de Compensación Automatizada. Se trata de un servicio que controla todas las transacciones electrónicas y que utiliza dos cámaras de compensación que actúan como intermediarias entre las entidades financieras que se sirven del modelo ACH.

¿Cuánto tarda una transferencia electrónica de fondos?

Cuánto tarda una transferencia electrónica variará, dependiendo del tipo transacción que elijas. Si es transferencia ordinaria, puede demorar uno o dos días laborales. Para las transferencias urgentes, el dinero se verá reflejado el mismo día, incluso unos minutos o segundos después de hacer la operación.

Seguridad

Hacer una transferencia electrónica directamente desde tu banco hacia un destinatario confirmado y conocido, o para hacer el pago de algún producto o servicio o producto es bastante seguro, el problema real puede llegar hacer por parte del humano y oportunistas convergen: dar por error tus datos bancarios, dejar tu cuenta abierta en alguna computadora o creer en la trampa de una tienda en línea falsa. Son errores comunes, pero fácilmente evitables, simplemente deveras poner tus 5 sentidos al realizar cualquier transacción.

Ventajas

- Tienen costes muy bajos porque están automatizadas.
- La información de cada transferencia se registra, por lo que no es necesario volver a introducirla cuando se envíe otro pago al mismo destinatario.
- Tienen un mayor nivel de seguridad y protección.
- El modelo ACH proporciona una capa adicional de seguridad.
- Es posible configurar pagos recurrentes.
- No requieren documentos físicos o dinero en efectivo.

Desventajas

- Son transferencias difíciles de realizar para una persona que no está familiarizada con los medios electrónicos o Internet.

- En algunos casos, estas operaciones cobran una comisión adicional, con lo cual tendría que evaluarse el coste-beneficio de hacer la operación en línea o de forma presencial.
- Los datos bancarios de los usuarios pueden ser vulnerados por un hacker o un malware financiero (programa que roba la información).

2.8 La contratación electrónica

Definición

El concepto de contrato electrónico hace referencia a todo aquel acuerdo de voluntad establecido por medio de herramientas electrónicas donde los firmantes se comprometen al cumplimiento de lo establecido. Incluye tanto el manejo del tratamiento de la información como el almacenamiento de esos datos.

Un contrato electrónico conserva las características básicas del contrato tradicional y sus términos y condiciones tienen efecto legal.

La contratación electrónica involucra diversos aspectos, entre ellos, el más común es la firma de convenios de compra o venta de cualquier producto, bien o servicio.

¿Cómo se utilizan?

Debido a su versatilidad y seguridad, este formato puede utilizarse para concretar acuerdos de todo tipo. En general se puede establecer en circunstancias como las siguientes:

- En función de los intervinientes, es decir, en aquellos contratos mercantiles y de consumo donde una de las partes es consumidor final.
- De acuerdo con el modo de ejecución, es decir, con los contratos directos (que se firman 100% digitales) o los indirectos (donde se requiere la ejecución física de algún punto del proceso).
- Según la forma de manifestación de voluntad, es decir, puede ser puro (donde las partes dan su consentimiento de forma 100% electrónica) o mixto (el cual se suscribe una parte en digital y otra físicamente).
- Y de acuerdo con el objeto por el que se realice el contrato. bien por entrega (de un producto) o de prestación (cuando se presta algún servicio).

¿Para qué sirven?

Actualmente, se puede verlos adoptados en diversos casos de uso, por ejemplo:

- Acuerdos de contratación de servicios en línea;
- Compra y venta de bienes;
- Acuerdos comerciales a distancia;
- Documentos relacionados con la contratación de empleados; y muchas otras posibilidades.

Características de un contrato electrónico

El **contrato electrónico** se distingue particularmente por el vehículo utilizado para expresar la voluntad de los declarantes.

Sus características distintivas, son:

- está escrito y contenido en soporte electrónico;
- está firmado digitalmente por las dos partes.

Tipos de contratos electrónicos más usados en México

- Contrato de arrendamiento
- Convenio comercial
- Mandato comercial
- Protección de obras intelectuales

En los **contratos electrónicos**, la única diferencia con un contrato tradicional, es el formato, en este caso electrónico, en el que se presenta el acuerdo. Sin embargo, no solo la oferta debe ser electrónica, sino la celebración de la contratación debe ser de este modo.

2.9 El documento electrónico

Un documento electrónico es todo contenido originalmente creado desde una aplicación electrónica y que contiene información para facilitar transacciones o compartir información entre las partes.

Estos instrumentos virtuales reemplazan a sus contrapartes físicas y, por lo general, tienen el mismo propósito, excepto que en formato digital.

La naturaleza digital de estos documentos facilita compartir, organizar y colaborar. Dependiendo del sistema que utilicemos, podremos incluso controlar la versión, rastrearlos y firmarlos.

Características

1. Fácil accesibilidad

Los documentos electrónicos tienen la principal característica de que podemos acceder a ellos de múltiples formas; desde cualquier dispositivo móvil, y en el lugar en que estemos, incluso si trabajamos de manera remota.

2. Búsqueda y recuperación instantánea

Cuanto más fácil de usar una herramienta de gestión de documentos electrónicos, mejor. Todos utilizamos motores de búsqueda para ubicar lo que necesitamos en Internet y, como tal, debe esperar una función de búsqueda en su plataforma digital de Electronic Document Management —EDM—elegida que sea igual de fácil y completa de usar.

De esta manera, tendremos la posibilidad de buscar lo que necesitamos incluso si solo conocemos fragmentos del nombre del archivo o una palabra clave, como la razón social de una empresa cliente o la dirección que se usa en el documento.

3. Integración abierta

Un EDM puede integrarse con las otras herramientas comerciales esenciales que tenemos, desde el correo electrónico hasta las firmas electrónicas.

Esto optimizará el flujo de trabajo, ya que permitirá que la información esté disponible en todos los sistemas que se usen en cada departamento de la empresa.

Tipos de documentos electrónicos

1. Registros de personal

Los registros de personal son archivos que pertenecen a los empleados de la organización y, por lo general, los administra el departamento de recursos humanos.

Comúnmente, los registros de personal incluyen detalles sobre la solicitud de un empleado, la descripción del trabajo y sus datos salariales únicos.

Como es evidente, la mejor manera de mantener los registros de personal de tu organización mediante el uso de la tecnología es a través de la documentación digital, ya que este método garantiza que todos los datos sean privados.

2. Documentos legales

La verdad es que es probable que los registros de personal y los documentos legales se superpongan en algún momento y, saber diferenciarlos automáticamente, es indispensable para mejorar el compliance y aprovechar sus beneficios.

Esto se debe a que elementos como los acuerdos de confidencialidad, las verificaciones de antecedentes y los registros médicos están relacionados con los empleados y, al mismo tiempo, son de naturaleza legal.

3. Contratos electrónicos

Un contrato digital o "e-contract", en pocas palabras, es un acuerdo formulado en línea.

Las partes interactúan entre sí en formato digital, en lugar de en persona o por teléfono. Aunque es digital, un e-Contract sigue siendo un contrato; lo que hace, a su vez, mucho más sencilla la administración de contratos.

Ventajas

1. Más organización

La organización puede significar la diferencia entre un negocio rentable o no rentable. Los procesos comerciales de rutina, como la revisión, la aprobación, la contratación y la incorporación, pueden ser un dolor de cabeza en un sistema tradicional. De hecho, la investigación indica que el 53% de los empleados buscan formas simples, pero sólidas de firmar y enrutar documentos de la empresa

2. Reducción de errores humanos

La entrada manual de datos suele estar plagada de errores humanos que cuestan tiempo y dinero.

Las soluciones de automatización del flujo de trabajo nos ayudan a eliminar los errores humanos, lo que impulsa nuestro proceso comercial.

3. Acceso más fácil a los datos

Todos sabemos que recuperar documentos manualmente puede ser un proceso lento y, en algunos casos, imposible porque están dañados o rotos. ¡El tiempo es dinero!

Imagínate cuánto tiempo podrías ahorrar, y utilizarlo productivamente en otro lugar, si los documentos casi de manera inmediata.

Definir cada tema y describir las leyes que regulan las TI para su observación en las actividades propias de la auditoría. Elabora un cuadro resumen que incluya su descripción y las regulaciones establecidas en México y otros países.

Tema	Descripción	Leyes
2.1 La protección de datos de carácter personal	Implica que la información personal de un individuo, como su nombre, dirección, número de identificación, información financiera, historial médico, entre otros, no pueda ser recopilada, almacenada, procesada o utilizada sin su consentimiento explícito	Articulo 1 Articulo 2 Articulo 3 Articulo 6 Articulo 7 Articulo 8 Articulo 15 Articulo 16 Articulo 17 Articulo 18 Articulo 19 Articulo 20 De la LFPDPPP de México
2.2 La protección jurídica de los programas de computadora	Se refiere a los derechos de propiedad intelectual que tienen los creadores o propietarios de un programa de computadora sobre su obra, los cuales les permiten controlar el uso, reproducción y distribución de dicho programa.	Articulo 101 Articulo 111 Articulo 112 Articulo 113 Articulo 118 De la LFDA de México Artículo 16 Bis Artículo 19 Bis Artículo 87 De la LPI de México
2.3 Las bases de datos y la multimedia	La protección de bases de datos se refiere al derecho exclusivo que tienen los creadores o propietarios de la base de datos sobre la selección, disposición y organización de los datos que conforman dicha base de datos.	Artículo 2 Bis Artículo 13 Bis Articulo 87 Articulo 111 Articulo 113 Articulo 116 De la LFDA de México Artículo 2 Bis Artículo 4 Bis Articulo 215 Articulo 223 Articulo 227 De la LPI de México
2.4 Los delitos informáticos	Son aquellos que se cometen utilizando la	Artículo 211 Bis Artículo 212 Bis

	tecnología y los sistemas informáticos. Se trata de actividades ilícitas que se llevan a cabo a través de Internet, redes de computadoras, dispositivos electrónicos y otros medios tecnológicos.	Artículo 213 Bis Artículo 216 Artículo 226 Bis Artículo 289 Bis Del código penal federal Artículo 9 Artículo 11 Artículo 14 De la ley de la policía de seguridad publica
2.5 Los contratos informáticos	Es un acuerdo legal que se celebra entre dos o más partes, en el que se establecen los términos y condiciones para la prestación de servicios o el suministro de bienes mediante el uso de tecnología informática	Artículo 1793 del código civil federal Artículo 76 Bis Artículo 76 Bis 1 Artículo 76 Bis 2 Artículo 76 Bis 3 Artículo 76 Bis 4 De la ley federal de protección del consumidor
2.6 El intercambio electrónico de fondos	Se refiere a la transferencia de fondos de una cuenta bancaria a otra mediante el uso de tecnología electrónica. Esta transferencia puede realizarse de diversas formas, como mediante la banca en línea, el uso de tarjetas de crédito o débito, o mediante aplicaciones móviles.	Artículo 18 Artículo 19 Artículo 20 De la ley para la transferencia y ordenamiento de servicios financieros Artículo 31 Artículo 32 Artículo 33 De la ley de regulación de instituciones financieras
2.7 La transferencia electrónica de fondos	Es una forma de pago que permite la transferencia de fondos de una cuenta bancaria a otra mediante el uso de tecnología electrónica. La TEF se utiliza ampliamente en el mundo de los negocios para el pago de facturas, nóminas y otras transacciones comerciales	Artículo 56 Artículo 57 Artículo 58 De la ley de transparencia y ordenamiento de los servicios financieros Artículo 49 Artículo 50 Artículo 51 De la ley para Regular instituciones de tecnología financiera
2.8 La contratación electrónica	Es un proceso por el cual las partes involucradas en un contrato utilizan medios electrónicos para	Artículo 3 Artículo 9 Artículo 10 Artículo 13

	celebrar un acuerdo contractual. Esto significa que los términos y condiciones del contrato se establecen, negocian y acuerdan a través de medios electrónicos, como el correo electrónico, los formularios en línea o las plataformas de comercio electrónico.	De la ley de firma electronica avanzada Artículo 5 Artículo 12 Artículo 14 Del reglamento de la ley de firma electronica avanzada Artículo 87 Artículo 90 Artículo 93 De la ley de protección al consumidor Artículo 16 Artículo 17 Artículo 18 De la ley de comercio electronico
2.9 El documento electrónico	Es aquel que ha sido generado, enviado, recibido o archivado en formato electrónico. Es decir, se trata de un documento que existe exclusivamente en formato digital, y no en formato físico.	Artículo 2 Artículo 8 Artículo 15 Artículo 16 Artículo 17 De la ley de firma electronica avanzada Artículo 3 Artículo 9 Artículo 15 Artículo 19 De la ley federal de protección de datos personaless en posesión de particulares Artículo 87 Artículo 90 Artículo 91 De la ley de protección al consumidor

Investiga en internet 3 casos reales de problemas legales de la auditoría para analizar y proponer soluciones.

Empresa	Caso	Análisis	Solución
Toshiba	En 2015, la empresa japonesa de tecnología Toshiba se vio envuelta en un escándalo de contabilidad cuando se descubrió que había inflado sus ganancias en más de 1.200 millones de dólares durante varios años. Ernst & Young era la firma de auditoría externa de la empresa y fue criticada por no haber detectado la manipulación contable.	Este caso destaca la importancia de una auditoría rigurosa y profesional, y la necesidad de que las firmas de auditoría externa se aseguren de que las empresas estén cumpliendo con los estándares contables y financieros adecuados. Además, subraya la necesidad de una mayor supervisión y regulación para garantizar que las empresas cumplan con las leyes y regulaciones aplicables.	La solución a los problemas legales de Toshiba incluye cambios en la alta dirección, reformas de gobernanza corporativa, reestructuración de negocios y pago de multas y compensaciones. La empresa deberá tomar medidas para remediar la situación y restaurar la confianza de los inversores y los reguladores.
	En 2002, se descubrió que la empresa de seguridad Tyco había inflado sus ingresos y ocultado deudas significativas en sus estados financieros. PwC era la firma de auditoría externa de la empresa y fue criticada por no haber detectado las	El caso de Tyco International es un ejemplo de cómo la mala conducta empresarial puede afectar a una empresa y a sus accionistas. Destaca la importancia de la ética empresarial y la responsabilidad corporativa, así como	La solución en el caso de Tyco International incluye cambios en la alta dirección, compensaciones y sanciones, reforma de la gobernanza corporativa y reestructuración de negocios. Tyco deberá tomar medidas para remediar la

Tyco	irregularidades contables.	la necesidad de una auditoría rigurosa y una supervisión adecuada para garantizar que las empresas cumplan con los estándares contables y financieros adecuados.	situación y restaurar la confianza de los inversores y el público en general.
Banco Nacional de Australia	En 2019, el Banco Nacional de Australia (NAB) fue multado con 57.5 millones de dólares australianos por la Comisión Australiana de Valores e Inversiones por no cumplir con las leyes de lavado de dinero. La auditoría interna del banco había informado de los problemas, pero la auditoría externa, EY, no había informado a los reguladores. EY fue criticada por su falta de diligencia y profesionalidad.	El caso del Banco Nacional de Australia es un ejemplo de cómo la falta de supervisión y control interno puede llevar a problemas significativos en una empresa. Destaca la importancia de la supervisión y el control interno adecuados, así como la necesidad de una cultura empresarial ética y transparente.	La solución en el caso del Banco Nacional de Australia incluye cambios en la alta dirección, compensaciones y sanciones, reforma de la gobernanza corporativa y mejoras en los controles internos. El NAB deberá tomar medidas para remediar la situación y restaurar la confianza de los inversores y el público en general.

Investigar 3 casos reales de fraudes informáticos y proponer controles para prevenirlos

1. Fallchill

Es un malware que fue detectado en varios equipos de una empresa de telecomunicaciones en la Ciudad de México. Entre sus capacidades están las siguientes:

- Extraer información de los discos duros de las computadoras donde se alojaba.
- Iniciar y terminar procesos.
- Intervenir cualquier archivo para modificarlo, ejecutarlo, moverlo o incluso eliminar elementos del sistema.
- Es capaz de borrarse a sí mismo, y así evitar dejar rastros de su presencia, lo que dificulta su detección en las redes vulnerables.

2. WannaCry

Tuvo alcance en más de 150 países, incluido México en 2017. Este programa operaba mediante extorsiones, ya que tenía la función de “secuestrar” información para luego “pedir pagos por su rescate”; este es el modus operandi típico de un ransomware.

Se calcula que el número de víctimas de este malware, hasta 2018, fue de al menos 200,000 a nivel global; mientras que en México, se estima que el 44% de las organizaciones fueron víctimas del secuestro de su información.

3. Janeleiro

Por último, este malware bancario creado originalmente para atacar corporativos de bancos en Brasil, del cual fue creada una variante para atacar usuarios en México, y poder robar su información bancaria y personal.

Este virus es distribuido a través de correos electrónicos, que contienen enlaces que redireccionan a los usuarios ventanas emergentes con formularios de banco apócrifos; de esta forma logran acceder y robar la información bancaria.

¿Cómo prevenirlos?

En un ataque por Denegación de Servicio Distribuido (DDoS). Típicamente, el DDos es utilizado para atacar y volver inestable un servidor, impidiendo así que los usuarios legítimos accedan a él.

Sin embargo, utilizado a la inversa puede ayudar a efectuar pruebas de penetración con el objetivo de identificar y eliminar vulnerabilidades o brechas en los sistemas, favoreciendo la prevención y control de riesgos informáticos.

Software como Servicio (SaaS). Los SaaS ayudan a centralizar la información para un óptimo manejo y protección; además, aportan a la ciberseguridad en tanto que permiten mantener control sobre el área de Cumplimiento.

Esto asegura el eficaz cumplimiento de las normativas aplicables, de acuerdo a las especificidades en cada rubro o industria.

Bibliografía

- ChatGPT. (2023, febrero 28). ¿Cómo funciona el intercambio de datos en el área de trabajo? [Respuesta a una pregunta de usuario]. Recuperado de https://www.gpt3api.com/
- Wiki Targeted (Entertainment). (s. f.). Legislación Informática Wikia. https://legislacion-informatica.fandom.com/wiki/Los_contratos_inform%C3%A1ticos
- Tipos de delitos informáticos. (s. f.). Delitos informáticos. https://www.delitosinformaticos.info/delitos_informaticos/tipos_de_delitos
- Westreicher, G. (2022, 24 noviembre). Transferencia electrónica de fondos. Economipedia. https://economipedia.com/definiciones/transferencia-electronica-de-fondos.html
- De DocuSign, C. (2021, 8 julio). ¿Qué es la contratación electrónica y cuándo es prudente usarla? DocuSign. https://www.docusign.mx/blog/contratacion-electronica
- Orca, E. (s. f.). 3 casos reales de delitos informáticos en México. https://blog.orcagrc.com/casos-de-delitos-informaticos-en-mexico
- De DocuSign, C. (2022, 4 julio). ¿Qué son los documentos electrónicos y cuál es su valor probatorio? DocuSign. https://www.docusign.mx/blog/documentos-electronicos
- "¿En qué consiste la protección de datos de carácter personal?" - OpenAI, (2023)
- "¿Qué leyes están enfocadas en la protección de datos en México?" - INAI. (2021). Leyes en materia de Protección de Datos Personales. Recuperado el 21 de febrero de 2022, de https://inicio.inai.org.mx/proteccion-datos/leyes
- "¿Cuáles son las leyes y normativas de la protección de datos?" - INAI. (2021). Leyes en materia de Protección de Datos Personales. Recuperado el 21 de febrero de 2022, de https://inicio.inai.org.mx/proteccion-datos/leyes
- "Ejemplos de las normativas de protección de datos" - INAI. (2021). Normativas y regulaciones en materia de protección de datos personales. Recuperado el 21 de febrero de 2022, de https://inicio.inai.org.mx/proteccion-datos/normativas

- “En que consiste la protección jurídica de los programas de computadora”-OpenAI (2023)

- Ley Federal del Derecho de Autor (2021). Última reforma publicada DOF 23-07-2021. Cámara de Diputados del H. Congreso de la Unión. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFDA.pdf

- Ley de la Propiedad Industrial (2021). Última reforma publicada DOF 05-03-2021. Cámara de Diputados del H. Congreso de la Unión. https://www.diputados.gob.mx/LeyesBiblio/pdf/162_050321.pdf

- "¿Qué es la protección en las bases de datos y multimedia?"-OpenAi (2023)

- "¿Qué medidas estarían en cuestión de leyes de México?"-OpenAi (2023)