AUDITORÍA INFORMÁTICA  
Preguntas de parciales anteriores

**Introducción a la auditoría informática**

* *Explicite la diferencia entre control interno y auditoría. Mencione similitudes y diferencias.*

El ***control interno*** es cualquier **actividad** o acción que se lleva a cabo de manera **manual** o **automática** para **prevenir**, **detectar** y **corregir** **errores** que puedan **afectar** el cumplimiento de los **objetivos** del **sistema**.

Una ***auditoría*** consiste en emitir una **opinión profesional** sobre un **objeto** para verificar que **cumple** con los **objetivos** que fueron prescriptos.

El ***control interno informático*** es un **control diario** de todas las actividades informáticas para asegurar que **cumplen** con los **procedimientos**, **estándares**, **normas** y **requerimientos legales** fijados por la **dirección informática** y la **dirección de la organización**.

La ***auditoría informática*** consiste en **recoger**, **agrupar** y **evaluar** **evidencias** para determinar que el sistema informatizado: **salvaguarda** los **activos**, mantiene la **integridad** de los **datos** y lleva a cabo **eficazmente** los fines de la organización utilizando **eficientemente** los recursos.

|  |  |  |
| --- | --- | --- |
|  | **Control Interno Informático** | **Auditoría Informática** |
| **Similitudes** | * Son realizados por **personal** con **conocimientos específicos** en tecnologías de la información. * **Verifican** si se cumplen los **Controles Internos**, **Normativas** y **Procedimientos establecidos** por la **Dirección General** y/o la **Dirección Informática**. | |
| **Diferencias** | Análisis de controles en el día a día (se controla diariamente). | Análisis de un momento informático determinado. |
| Informa a la Gestión del Departamento de Informática. | Informa a la Dirección General de la Organización. |
| Es realizado sólo por personal interno perteneciente a la organización. | Puede ser realizada por personal interno o externo a la organización. |
| El alcance de sus funciones es únicamente sobre el Departamento de Informática. | Cubre todos los componentes de los Sistemas de Información de la Organización. |

* *Emita una opinión sobre cómo justifica la inversión necesaria de ambas actividades (del control interno y de la auditoría informática).*

Se justifica la inversión en el **control interno informático** si queremos garantizar que el procesamiento, manejo y almacenamiento de la información y de los recursos que utiliza la organización se realicen con eficiencia y eficacia. Además, también se justifica si se busca dar tranquilidad a los dueños de la organización, consejo administrativo, clientes, accionistas, comités o al público en general.

Se justifica la inversión en la **auditoría informática** en principio si tenemos un **problema** o **necesidad** que debemos resolver y para el cual necesitamos una opinión, pero también si queremos mejorar la **imagen** de la **organización**, **generar confianza** en los usuarios sobre la seguridad y control de los servicios de tecnologías de la información, **optimizar** las **relaciones** internas y el clima de trabajo, **disminuir costos** por mala calidad, generar un **balance** de los **riesgos** de tecnologías de la información o generar un **control** de la **inversión** en un entorno de tecnologías de la información.

* *Explique los contenidos o puntos esenciales que deben estar presentes en el informe que confecciona el auditor como conclusión de su trabajo.*

El informe de auditoría es el documento más importante de la auditoría informática, en el cual se presentan los resultados obtenidos durante la evaluación.

* **Identificación del informe**: tipo de auditoría que se realizó (por ejemplo, Auditoría de Seguridad).
* **Identificación del cliente**: área de la organización en la cual se realizó la auditoría.
* **Identificación de la entidad auditada**: organización en la cual se realizó la auditoría.
* **Objetivos**: necesidades y problemas por los cuales se realiza la auditoría.
* **Alcance de la auditoría**: *período* (fechas de inicio y fin), detallando *limitaciones* y *restricciones* impuestas en la misma.
* **Conclusiones**: opinión certera basada en hallazgos y evidencias, junto a fortalezas y debilidades halladas en el proceso de auditoría.
* **Recomendaciones/Resultados**: cursos de acción que se recomiendan tomar con estimaciones reales y áreas de oportunidad.
* **Fecha del informe**
* **Identificación y firma de los auditores**
* **Distribución del informe**: se establece a quiénes se le entregará una copia del informe.
* *Mencione con qué elementos o hechos es necesario trabajar para la elaboración del informe mencionado.*

Algunas evidencias que permiten identificar fortalezas y debilidades, y elaborar el informe de auditoría son:

* **Problemas** o **necesidades** planteadas por quien solicita la auditoría.
* **Observaciones** realizadas en el sector informático u otros sectores de la organización involucrados en la auditoría.
* Documentación sobre los **controles** **internos realizados** en la organización.
* Manuales de **políticas**, **reglamentos** y **normas** de la organización.
* **Entrevistas**/**cuestionarios**/**encuestas** realizadas a diferentes actores de la organización y al departamento informático en particular.
* **Diagramas de flujo de procesos**.
* **Pruebas de cumplimiento de seguridad**.
* **Procesos históricos** (backups).
* *Dé 8 ejemplos de Controles Internos Informáticos que considere vitales de implementar en las distintas actividades informáticas. Ordénelos según su criterio enumerándolos de mayor a menor importancia.*
* **Registro** de intentos de **acceso** no autorizado a la **base de datos**. (Control detectivo)
* Implementación de **software** de seguridad que **impida el acceso** no autorizado al **sistema**. (Control preventivo)
* Implementación de **medidas** que **impidan el acceso** no autorizado a las **redes**. (Control preventivo)
* Implementación de diferentes **niveles de backup** de la base de datos. (Control preventivo)
* **Recuperación** de una base de datos desde una **copia de seguridad**. (Control correctivo)
* *Detalle la metodología de la Auditoría Informática.*
* **Estudio preliminar**: aquí se incluye la definición del objetivo de la auditoría, el equipo de trabajo, programa de auditoría, sector a evaluar; también la visita al sector informático para conocerlo, conocer su plan de actividades, evaluar el control interno, solicitar manuales de política, reglamentos, normas, y entrevistar a los principales referentes del mismo y de la organización en general.
* **Revisión y evaluación de controles y seguridades**: aquí se tienen en cuenta diagramas de flujos de los procesos, pruebas de cumplimiento de las seguridades, aplicaciones de las áreas críticas, procesos históricos (backups), documentación y archivos.
* **Examen detallado de las áreas críticas**: aquí se incluye la distribución de tareas entre el grupo de trabajo, la definición de motivos, objetivos, alcances y recursos a utilizar, la metodología de trabajo, el establecimiento de las fechas y duración de la auditoría, la presentación del plan de trabajo y el análisis detallado de cada problema encontrado en la etapa anterior.
* **Comunicación de resultados**: aquí se puede tener un informe preliminar para ser discutido con los ejecutivos o un informe definitivo con matrices, cuadros, redacción simple y concisa que destaque los problemas encontrados, efectos y recomendaciones de la auditoría. Ambos documentos deben contener motivos de la auditoría informática, objetivos, alcance, configuración del software/hardware instalado, estructura orgánico-funcional del área informática, control interno, resultados de la auditoría, conclusiones y recomendaciones.

**Auditoría de la Dirección Informática**

* *¿Qué aspectos debe considerar el auditor al evaluar cómo la dirección o gerencia de informática* ***organiza y coordina*** *las actividades de sus sectores o áreas?*

Para evaluar cómo la dirección o gerencia de informática **organiza y coordina** las actividades de sus sectores o áreas, el auditor debe considerar:

* Si existe un **Comité de Informática** y, de ser así, si cumple su papel adecuadamente, cuáles son sus funciones y quiénes son sus integrantes.
* Si el **Departamento de Informática** de la organización se encuentra en una **posición** alta de la jerarquía de la misma, si cuenta con masa crítica suficiente y si posee autoridad e independencia frente a las áreas de los usuarios.
* Si el **Departamento de Informática** de la organización está dividido en unidades organizativas, y si tiene **funciones y responsabilidades** bien delimitadas, documentadas y comunicadas al personal.
* Si existen **Estándares de Funcionamiento y Procedimientos** promovidos por la Dirección de Informática para saber qué controles deben establecerse y como son las relaciones entre las áreas de la organización, y si están bien documentados, actualizados y comunicados al personal.
* Cómo se realiza la **gestión de los recursos humanos** en cuanto a su selección, formación, evaluación del desempeño, promoción y finalización.
* Si la **comunicación** entre la Dirección de Informática y el Personal de Áreas Informáticas es efectiva y eficiente.
* Cómo realiza la **gestión económica** la Dirección de Informática en cuanto a presupuestación, adquisición de bienes y servicios, y medición y reparto de los costos.
* Si la organización posee **seguros** o coberturas para los sistemas informáticos y si los mismos son suficientes.
* *Dé su opinión sobre quién o quiénes deben realizar cada una de las actividades de organizar y coordinar.*

Debido a que en las actividades de **organización y coordinación** la **Dirección de Informática** y las **áreas usuarias** deben estar en estrecha **comunicación y entendimiento**, creo que quienes deben estar involucrados en esas funciones son:

* **Comité de Informática**: Para debatir asuntos informáticos que repercuten a toda la empresa, para fijar prioridades, aprobar el plan estratégico de sistemas de información, aprobar inversiones en TIC’s y vigilar y realizar el seguimiento de las actividades del departamento informático.
* **Área de Gestión de Recursos Humanos**: Para selección, formación, evaluación de desempeño, promoción y finalización del personal involucrado.
* **Área de Gestión Económica**: Para presupuestación, adquisición de bienes y servicios, medición y reparto del costo.
* *Explique en qué consiste la actividad* ***controlar*** *llevada a cabo por la Dirección de Informática.*

La actividad de **controlar** consiste en efectuar un **seguimiento permanente** de las distintas actividades del **Departamento de Informática**. Asegura el **cumplimiento** de la **normativa legal** en cuanto a distintos rubros como higiene y seguridad, protección de datos personales, contratos e-commerce, normatividad laboral y sindical, etc.

**Auditoría de la seguridad física**

* *¿Cuáles son los objetivos/áreas de una Auditoría de Seguridad Física?*

Se realiza una Auditoría de Seguridad Física para asegurar que la organización va a seguir dando servicio siempre que se lo necesite y de una manera segura. A su vez, los objetivos de dicha auditoría consisten en el análisis de:

* **Edificio:** normalmente debe encargarse a profesionales especializados en el ámbito, ya que el auditor suele conocer muy poco de construcciones.
* **Instalaciones:** organigrama de la empresa, CPD, salas, oficinas, almacenes, instalaciones eléctricas.
* **Equipamiento y telecomunicaciones:** hosts, terminales, computadoras personales, equipos de almacenamiento masivo de datos, impresoras, medios y sistemas de telecomunicaciones.
* **Datos e información:** cómo están resguardados.
* **Personas**
* *Identifique las áreas y fuentes de la Auditoría de Seguridad Física.*
* **Edificio:** parte de la cual se encargarán peritos especializados, ya que el auditor puede conocer muy poco de construcciones.
* **Organigrama de la empresa**: Dependencias orgánicas, funcionales y jerárquicas, cargos y empleos, separación de funciones, rotación del personal, visión del centro de proceso.
* **Auditoría Interna:** (si existe) personal, planes de auditoría, historia de auditorías físicas.
* **Administración de la seguridad**: director o responsable de la seguridad integral, responsable de la seguridad informática, administradores de redes, administradores de bases de datos, responsables de la seguridad activa y pasiva del entorno físico, normas, procedimientos y planes existentes (distribuidos, emitidos y controlados).
* **Centro de Procesamiento de Datos e instalaciones. Elementos accesorios para la función informática**: entorno donde se encuentra el CPD como elemento físico, sala de host, sala de operadores, sala de impresoras, cámara acorazada, oficinas, almacenes, instalaciones eléctricas, aire acondicionado, áreas de descanso y servicios.
* **Equipos y comunicaciones**: host, terminales, computadoras personales, equipos de almacenamiento masivo de datos, impresoras, medios y sistemas de telecomunicaciones.
* **Seguridad física del personal**: Accesos seguros, salidas seguras, medios y rutas de evacuación, extinción de incendios, sistemas de bloqueos de puertas y ventanas, normas y políticas emitidas y distribuidas al personal referente al uso de las instalaciones.
* *Explique qué es el plan de contingencia y qué aspectos se deben tener en cuenta para su preparación.*

Un plan de contingencia es un instrumento que contiene los medios necesarios, medidas técnicas, humanas y organizativas, para afrontar un desastre y garantizar la continuidad del negocio y las operaciones de una compañía u organización. El mismo está compuesto por un **Plan de Recuperación de Desastres** y un **Centro Alternativo de Procesamiento de Datos**.

Para su preparación se deben tener en cuenta los siguientes aspectos:

* ¿Quiénes y cómo deben elaborar el plan?
* ¿Cómo se implementará, probará y mantendrá (¿cada cuanto tiempo se revisará?)?
* ¿Qué debe contemplar y dónde se debe desarrollar?
* Si deberá limitarse a los equipos centrales o incluir equipos departamentales, PC’s y LAN’s.
* ¿Qué procesos son estratégicamente más importantes?
* ¿Cuáles serían las consecuencias de la ocurrencia de un siniestro o desastre?
* ¿Cuáles son las aplicaciones críticas, qué prioridades tienen, cuáles son sus recursos necesarios?
* ¿Cuál sería el período máximo de recuperación?
* Si están conforme todos los involucrados en su elaboración.
* *Explique ante la presencia de qué tipo de auditoría nos encontramos y qué información debe obtener el auditor para entender cómo se ha formalizado el plan de contingencia.*

Un **plan de contingencia** se analiza dentro de la **Auditoría de seguridad Física**.

Para poder determinar cómo se realizó el plan de contingencia hay que conocer el organigrama de la empresa y el centro de proceso. También realizar una especie de auditoría interna (personal, planes de auditoría, historia de auditorías físicas). También el auditor deberá acercarse al responsable de seguridad integral informática, redes, bases de datos, etc. Deberá conocer el Centro de Procesos de Datos e Instalaciones, los elementos accesorios para la función informática, equipos de comunicación y la seguridad física del personal.

**Auditoría del desarrollo**

* *¿Qué aspectos debe comprobar el auditor cuando audita las funciones o tareas que son responsabilidad del* ***área de desarrollo****?*
* El área de desarrollo debe tener **objetivos asignados** dentro del departamento y una organización que le permita el **cumplimiento** de los mismos.
* El **personal** del área de desarrollo debe contar con la **formación** adecuada y estar **motivado** para la realización del trabajo.
* Si existe un **plan de sistemas**, los proyectos que se lleven a cabo se basarán en dicho plan y lo mantendrán actualizado.
* La **propuesta** y **aprobación** de nuevos **proyectos** deben realizarse de forma **reglada**.
* La **asignación de recursos** a los **proyectos** debe hacerse de forma **reglada**.
* El **desarrollo** de sistemas de información debe hacerse aplicando **principios** de **ingeniería de software** ampliamente aceptados.
* Las **relaciones** con el **exterior** del departamento tienen que producirse de acuerdo a un **procedimiento**.
* La **organización del área** debe estar siempre **adaptada** a las necesidades de cada momento.
* *¿Qué aspectos debe tener en cuenta un auditor al auditar un* ***proyecto*** *de desarrollo de software?*

Ciclo de vida del desarrollo del software:

* **Análisis**: Ingeniería de requerimientos. Estudio de factibilidad.
* **Diseño**: Diseño general del sistema. Diseño detallado del sistema.
* **Desarrollo**: Programación. Prueba modular y prueba del sistema integral. Desarrollo de manuales. Entrenamiento.
* **Implementación**: Conversión. Revisión post-implementación.
* *¿Qué aspectos considera relevantes para mantener motivado al personal del área de desarrollo?*

¿Entorno de trabajo ameno, reconocimiento al trabajo?

**Auditoría de la ofimática**

* *¿Qué es la ofimática? ¿Cuáles son las características de los entornos ofimáticos y cuáles las consecuencias que posibilitan la auditoría sobre los mismos?*

La **ofimática** es todo **sistema informatizado** que genera, procesa, almacena, recupera, comunica y presenta **datos** relacionados con el funcionamiento de las **oficinas**.

Las características de los entornos ofimáticos son:

* Las **aplicaciones** se encuentran **distribuidas** por los diferentes departamentos de la organización en lugar de encontrarse en una única ubicación centralizada.
* Se produce un **traslado** de la **responsabilidad** sobre ciertos **controles** de los **sistemas** de información a usuarios finales NO dedicados profesionalmente a la informática, que pueden NO comprender de un modo adecuado la importancia de los mismos y la forma de realizarlos.

Consecuencias:

* **Adquisiciones** poco planificadas.
* **Desarrollos** ineficaces e ineficientes.
* Falta de conciencia de los usuarios sobre la **seguridad de la información**.
* Deficientes **copias de seguridad**.
* Escasa **formación** del personal.
* Ausencia de **documentación**.
* *¿Qué controles son recomendables de realizar en los entornos ofimáticos? Explique la necesidad de cada uno de los mencionados.*

**Economía**, **eficiencia** y **eficacia**:

* Determinar si el **inventario** ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.
* Determinar y evaluar el procedimiento de **adquisición** de equipos y aplicaciones.
* Determinar y evaluar las **políticas de mantenimiento** definidas en la organización.
* Evaluar la **calidad** de las **aplicaciones** del entorno ofimático **desarrolladas** por **personal** de la propia organización.
* Evaluar la corrección del **procedimiento** existente para la realización de los **cambios de versiones** y **aplicaciones**.
* Determinar si los usuarios cuentan con suficiente **formación** y con la **documentación** de apoyo necesaria para desarrollar sus tareas de un modo eficaz y eficiente.
* Determinar si el **equipamiento** existente se ajusta a las **necesidades reales** de la organización.

**Seguridad** y **condicionantes legales**:

* Determinar si existen **garantías** suficientes para **proteger** los accesos no autorizados a la **información** reservada de la empresa y la integridad de la misma en estos entornos.
* Determinar si el procedimiento de generación de las **copias de respaldo** es **fiable** y **garantiza** la **recuperación** de la Información en caso de necesidad.
* Determinar si está garantizado el **funcionamiento ininterrumpido** de aquellas **aplicaciones** cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.
* Determinar el grado de exposición ante la posibilidad de intromisión de **virus**.
* Cumplir con la **legislación** vigente.

**Protección de datos personales**

* *Enumere y explique las normas aplicables en nuestro país para la protección de datos personales.*

Artículo 43 de la Constitución Nacional - Reforma 1994: da a los ciudadanos la posibilidad de **interponer** la acción de amparo **Habeas Data** para que puedan **tomar conocimiento** de sus datos personales que consten en registros o bancos de datos públicos o privados, conocer la **finalidad** para la que se emplean y en caso de falsedad o discriminación, poder **exigir** la *supresión*, *rectificación*, *confidencialidad* o *actualización*.

Ley Nacional de la Protección de Datos Personales N° 25326 / 2000: tiene por objeto la **protección integral** de los **datos personales** asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos **públicos** o **privados**, destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Esta ley es aplicable a **personas físicas** o de **existencia ideal**.

Ley 26951 / 2014 Registro Nacional “NO LLAME”: tiene por objeto **proteger** a los titulares o **usuarios** autorizados de los servicios de **telefonía**, en cualquiera de sus modalidades, de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados.

* *¿En qué consisten los datos personales y cómo deben ser los mismos?*

Los **datos personales** son información de cualquier tipo referida a **personas físicas** o **ideales** y pueden ser **determinados** o **determinables**.  
Los datos **determinados** son aquellos que son regularmente fijos, como el nombre de la persona, DNI, fecha de nacimiento, domicilio, etc.  
Los datos **determinables** son por ejemplo, el perfil psicológico, fisiológico, económico, social, etc.

Por otro lado, existen otros tipos de datos personales:

**Datos personales excluidos**: son datos personales almacenados para uso interno, personal o doméstico. Son archivos con **fines estadísticos**, **disociados** de la entidad titular.

**Datos sensibles**: aquellos que revelan origen racial/étnico, opiniones políticas, convicciones religiosas/filosóficas/morales, información sexual, etc.

* *¿Qué derechos tengo como titular de datos personales?*

El titular de los datos, al proporcionarlos, tiene derecho a informarse cuál es el **fin** de esos datos, con qué **objeto** se almacenan, identidad y domicilio del **responsable**. También tiene derecho de **acceso**, de **rectificación**, **actualización** y **supresión**.

Existen casos donde estos derechos hacen excepciones:

* Protección de la defensa de la nación.
* Orden y seguridad pública.
* Protección de derechos e intereses a terceros.
* *¿Cuál es la autoridad de la aplicación de la ley y cuáles son sus funciones?*

La autoridad es la **Dirección Nacional de Protección de Datos Personales**.

Sus funciones son:

* Hacer **cumplir** la ley.
* **Informar** a los titulares.
* Dictar **normas** y **reglamentaciones**.
* Censar archivos.
* **Solicitar** información a entidades **públicas** y **privadas**.
* Imponer **sanciones**.
* Controlar la **integridad** y **seguridad** existente sobre datos.
* *¿Se pueden ceder o transferir los datos personales? Justifique.*

Los datos sí pueden ser transferidos, pero solo bajo situaciones específicas; por **consentimiento contractual**, **protección de la nación**, **protección a terceros**. También, si se transfieren **fuera del país**, la organización que cede datos, debe asegurarse que transfiere datos a una nación con seguridad por lo menos del **mismo nivel**.

* *¿Cuál es el objeto de la ley 25.326 de Datos Personales?*

La Ley 25.326 tiene como objetivo la **proyección integral** de los datos personales en archivos, registros, bancos de datos, etc., ya sean **públicos** o **privados** y que estén destinados a **dar informes**.

**Protección Integral**: Garantizar el derecho al **honor** e **intimidad** de las personas y el **acceso** a la **información** que sobre las mismas se registre.

* *En el tratamiento de Datos Personales, cuando el titular presta su consentimiento ¿Cómo debe ser el mismo y qué debe conocer al darlo? Especifique en qué casos no es necesario el consentimiento del titular.*

El **consentimiento** debe ser **libre**, **expreso** e **informado**, el titular debe prestar su consentimiento.

Para ello, el titular debe conocer:

* **Finalidad** y quienes pueden ser sus **destinatarios**.
* Existencia del **banco de datos**, electrónico o no y la identidad y domicilio del **responsable**.
* Carácter facultativo u obligatorio de las respuestas al cuestionario que se proponga.
* Las **consecuencias** de proporcionar los datos, negativa a hacerlo o inexactitud de los mismos.
* Posibilidad de ejercer los derechos de **acceso**, **rectificación** y **supresión** de los datos.

No es necesario el consentimiento cuando:

* Datos obtenidos por **fuentes de acceso público** e irrestricto.
* Recabados por el ejercicio de funciones propias de los poderes del estado o en virtud de una **obligación legal**.
* Listados limitados a: Nombre, DNI, Identificación tributaria o Previsional, Ocupación, Fecha Nacimiento, Domicilio.
* Derivados de una **relación contractual**, **científica** o **profesional** del titular de los datos y resulten necesarios para su desarrollo o cumplimiento.
* *¿Qué son los datos sensibles?*

Los **datos sensibles** son aquellos que revelan origen racial o étnico, opiniones políticas, religión, sindicatos, salud, vida sexual, etc.

* *¿Qué es un archivo, registro, base o banco de datos?*

Conjunto organizado de datos personales para tratamiento o proceso.

* *¿Cuándo es lícita la formación de archivos?*

Los archivos son lícitos cuando están debidamente **inscriptos** en la **Dirección Nacional de Protección de Datos**.

Los datos **lícitos** **sin** necesidad de **consentimiento** son datos obtenidos por fuentes de **acceso público** e irrestricto, recabados por **poderes del estado** o virtud legal, **listados básicos** (nombre, DNI, ocupación, fecha de nac., domicilio), derivado de una **relación contractual**, **científica** o **profesional** (cuando resulten necesarios para su desarrollo/cumplimiento).

* *Al registrar una base de datos ¿Debo informar al Registro los datos de las personas que la componen?*

Si.

* *¿Cómo se debe efectuar la recolección de los datos personales?*

¿?

* *¿Se pueden usar los datos personales para otras finalidades distintas a la que motivan su obtención?*

No. Sería una violación a la Ley.

* *¿Durante cuánto tiempo debo mantener los datos personales?*

Los datos personales recabados deben permanecer en la base de datos hasta que se haya **completado** la **actividad** por la cual fueron recabados.

* *¿Es necesario mi consentimiento para que se puedan tratar datos sobre mi persona? ¿En qué caso no es necesario el consentimiento?*

Si. No es necesario el consentimiento cuando:

* Datos obtenidos por **fuentes de acceso público** e irrestricto.
* Recabados por el ejercicio de funciones propias de los poderes del estado o en virtud de una **obligación legal**.
* Listados limitados a: Nombre, DNI, Identificación tributaria o Previsional, Ocupación, Fecha Nacimiento, Domicilio.
* Derivados de una **relación contractual**, **científica** o **profesional** del titular de los datos y resulten necesarios para su desarrollo o cumplimiento.
* *¿Qué información debo requerir antes de suministrar datos personales?*

* **Finalidad** y quienes pueden ser sus **destinatarios**.
* Existencia del **banco de datos**, electrónico o no y la identidad y domicilio del **responsable**.
* Carácter facultativo u obligatorio de las respuestas al cuestionario que se proponga.
* Las **consecuencias** de proporcionar los datos, negativa a hacerlo o inexactitud de los mismos.
* Posibilidad de ejercer los derechos de **acceso**, **rectificación** y **supresión** de los datos.
* *¿Estoy obligado a proporcionar datos sensibles?*

**Nunca**.

* *¿Qué se debe hacer para asegurar los datos personales?*
* *¿Qué sanciones pueden aplicarse en caso de incumplimiento?*

Propiedad intelectual

* *¿Quiénes son los titulares del derecho de propiedad intelectual?*

La **propiedad intelectual** es el conjunto de **derechos de autor**, **morales** (personales) y **económicos** (patrimoniales) que corresponden a los autores sobre las obras de su creación.

Los titulares son:

* El **autor** de la obra
* Los **herederos** o **derechohabientes**.
* Los que con permiso del autor **traducen**, **adaptan** o **modifican**.
* Las **personas físicas** o **jurídicas** cuyos dependientes contratados para elaborar un programa de computación hubiesen producido este en el desempeño de sus funciones laborales.
* *¿Qué son las obras de software y base de datos?*

**Obras de software**:

* Los **diseños**, generales y detallados, del **flujo** lógico de los **datos** en un **sistema** de computación.
* Los **programas** de computación, tanto en su versión ***fuente*** (lector humano) como su versión ***objeto*** (destinada a ser ejecutada por el computador).
* La **documentación** técnica, cuyos fines sean la explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.

**Obras de bases de datos** (obras literarias):

* Las **producciones** constituidas por un conjunto organizado de **datos** interrelacionadas, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos.

**OTRAS**

* *¿Qué son los delitos informáticos?*

Es un hecho ilícito que se comete mediante medios o sistemas informáticos. Dentro de los delitos tipificados podemos mencionar la pornografía infantil, acceso a Bases de Datos no autorizado, SPAM, estafas, daño a sistemas informáticos, falsificación de datos, etc.