AUDITORÍA INFORMÁTICA 2021

Bourlot, Jimena

UNIDAD 1: INTRODUCCIÓN

Clase 1:

La tecnología en las organizaciones

Arte, Técnica o manera de hacer cosas, construir objetos y artefactos que satisfagan las necesidades de personas y comunidades, mediante la aplicación de conocimientos técnicos ordenados científicamente.
Los adelantos tecnológicos en conjunto con el desarrollo de las comunicaciones permitieron que se de un proceso de expansión mundial denominado Globalización que impactó en las actividades humanas: económicas, políticas y culturales.
Los avances tecnológicos pasaron a ser poderosas fuerzas del cambio, en tanto si no se entienden o aplican pasan a asegurar una pérdida de la eficacia organizacional en un plazo cada vez más corto. De esa forma ponen en peligro la supervivencia de la organización.
Otras causas del éxito organizacional son:

- Tecnología
- Estructura organizacional
- Procesos
- Cultura
- Capacidad técnica
- Conocimientos individuales

Los aspectos actuales en los que pueden evidenciarse los adelantos tecnológicos son las plataformas digitales móviles, el crecimiento del software en línea como servicio, así como también la utilización de los servicios en la nube y la manipulación de altos volúmenes de datos (“Big Data”). De ese mismo modo se genera un uso intensivo del internet que permite la teleinformática masiva, permitiendo un intercambio de información al instante y sin costo. Esto supone una verdadera ventaja a la hora de realizar negocios electrónicos. Otro de los usos actuales de la tecnología se ve en la robótica y la inteligencia artificial.

Además, la tecnología per se permite mejorar partes del proceso de una organización:

- Facilitar los Procesos Productivos
- Reducir Costos
- Reducir tiempos
- Mejorar calidad de productos y/o servicios
- Alcanzar nuevos mercados y nuevos clientes
- Facilitar el negocio entre partes
- Mejorar la toma de decisiones (más rápidas, menos riegos)
- Desarrollar nuevos servicios

Dentro de las organizaciones la tecnología también impacta:

- En la cultura organizacional (las empresas eran reacias a aceptar la tecnología, y poco a poco fue cediendo para no quedarse atrás frente a la competencia)
- En el trabajo: nuevos procedimientos tecnológicos son incorporados al proceso productivo.
- En las estructuras organizacionales: nuevos sectores de la organización deben ser creados para poder amoldarse a las tecnologías. Así mismo otros deberán ser eliminados dado que hay procesos que ya no deberán realizarse gracias a que la tecnología facilita pasos que anteriormente deberían realizarse de manera manual, o se han tercerizado a empresas que sí cuentan con la tecnología necesaria.
- En los procesos.
- En los productos y servicios ofrecidos a clientes.
- En los sistemas de información.
- En la forma de hacer negocios: nuevas formas de negociar.
- En las comunicaciones.(la seguridad o las maneras de comunicarse)

Por ello las organizaciones deben realizar diversas **adaptaciones o cambios**:

- Nuevos mercados
- Tendencias Externas
- Nuevas Tecnologías
- Intensificación de la Competencia
- Globalización o Diversificación de la Actividad
- Eliminación de Ramas del Negocio NO Rentable
- Introducción de Nuevos Productos
- Fusiones y Alianzas Empresariales

Para lograr esto es necesario un **mecanismo de CONTROL** : el mismo se construye en base a normas y procedimientos, que mediante controles internos permite establecer tranquilidad en la organización y en su entorno (consejo de administración, accionistas, clientes, público y comités).

El control debe realizarse a partir de una función de comprobación en conjunto con una acción de vigilancia, orientada a los distintos aspectos de una organización: distintos recursos (materiales, humanos), actos de la dirección, gestión, circuitos de información, tecnología aplicada.

Control interno informático

Es una actividad repetitiva y rutinaria que controla diariamente que todas las actividades de los sistemas sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o la Dirección Informática, así como los requerimientos legales. Este tipo de controles permiten garantizar la eficiencia y eficacia en el procesamiento, manejo y almacenamiento de la información y de aquellos recursos que permitan cada día mejorar el funcionamiento de la entidad.

Busca darle un cierto nivel de tranquilidad a la organización misma y a todos los que tengan algún tipo de vínculo con ella o con la actividad que vamos a desempeñar.

El control interno informático debe formar parte del órgano staff de la dirección de informática. De esta forma permite controlar que todas las actividades se realicen cumpliendo los procedimiento y normas fijadas por la Dirección, y evaluar la bondad de las mismas asegurando el cumplimiento de normas legales. Para ello colabora y apoya el trabajo de Auditoría Informática y define, implementa y ejecuta mecanismos y controles.

De esta forma sus **objetivos** son:

- Establecer como prioridad la seguridad y Protección de la información
- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.
- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.
- Instaurar y hacer cumplir las **normas, políticas y procedimientos** que regulen las actividades de sistematización de la empresa. (por ejemplo normas de protección de datos)
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.

Características del Control Interno Informático:

- Definir, implantar y ejecutar mecanismos y controles.
- Evaluar su bondad y asegurar el cumplimiento de normas legales.
- Colaborar y apoyar el trabajo de Auditoría Informática.
- Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados por la Dirección.

Tipos de controles internos informáticos:

Por un lado se encuentran los controles **manuales**, que son aquellos realizados por el personal del área usuaria o de informática sin la utilización de herramientas computacionales; y por otro lado se encuentran los controles **automáticos** que están generalmente incorporados en el software, ya sean de operación, comunicación, gestión de bases de datos, programas de aplicación, etc. Por otro lado se tienen los controles **preventivos**, que establecen las condiciones necesarias para que el error no se produzca, y de esta forma anticipan eventos no deseados antes que ocurran. Controles de este tipo son los softwares de seguridad que impiden el acceso no autorizado a un sistema. Como complemento se hallan los controles **detectivos**, los cuales identifican el error en el momento en que se presentan, pero no se evitan, sino que actúan como

alarmas que permiten registrar el problema y sus causas. Así, sirven como verificación de los procesos y de sus controles preventivos. Relacionando esto con el tipo anterior, ejemplos de este tipo de control es el registro de intento de acceso no autorizado. Para investigar y rectificar los errores y sus causas, existen los controles **correctivos**, destinados a procurar que existan las acciones necesarias para su solución. Ejemplos de esto son los mecanismos de recuperación de una base de datos desde una copia de seguridad.
Para llevar adelante el control interno informático, se necesitan los siguientes elementos:

- Organización del área informática
- Análisis, desarrollo e implementación de sistemas
- Operación de los sistemas.
- Procesamiento de entrada de datos, de información y emisión de resultados.
- Seguridad de área de sistemas.

Clase 2:
Auditoría

Es la actividad que consistente en la emisión de una opinión profesional, sobre si el objeto sometido a análisis, presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido establecidas.

Es un proceso evolutivo "que mediante técnicas y procedimientos aplicados en una organización por persona independiente a la operación de la misma, evalúa la función de tecnología de información y su aportación al cumplimiento de los objetivos institucionales; emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de apoyo al cumplimiento de dichos objetivos". Es decir que **evalúa, opina y recomienda.**

Beneficios de la auditoría:

- Mejora la imagen pública.
- Genera confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, etc).
- Genera un balance de los riesgos de TI.
- Realiza un control de la inversión en un entorno de TI, muchas veces impredecible.

Clases de auditoría
Auditoría financiera: refiere al control de las cuentas anuales, con el objetivo de determinar si representan la realidad.
Auditoría de gestión: se encarga de la auditoría de la dirección/conducción, con la finalidad de controlar la eficiencia, eficacia y economicidad.
Auditoría de cumplimiento: se dedica al control de las normas establecidas, analizando para ello que las operaciones que realiza la organización se adecúen a las mismas. Generalmente es llevada a cabo por un abogado.
Auditoría informática: se halla dirigida a los sistemas de aplicación, recursos informáticos, planes de contingencia, seguridad e infraestructura. Tiene por finalidad analizar la operatividad, su eficiencia y que se realice según las normas, procedimientos y estándares.

Tipos de Auditoría
Interna: es realizada con recursos y personas pertenecientes a la empresa auditada. Existe por expresa decisión de la empresa.
Externa: es la realizada por personas no pertenecientes a la empresa auditada. De esta forma se presume mayor objetividad, y es la que realiza el seguimiento de la auditoría interna.
Ambas auditorías son compatibles y recomendables, ya que su cometido es complementario.

Objetivos de la Auditoría Informática
Salvaguardar los activos: se refiere a la protección del hardware, software y recursos humanos.

Integridad de datos: los datos deben mantener consistencia y no duplicarse.
Efectividad de sistemas: los sistemas deben cumplir con los objetivos de la organización.
Eficiencia de sistemas: que se cumplan los objetivos con los menores recursos.
Seguridad y confidencialidad.

Procedimientos y técnicas de la AI: la auditoría exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la **evidencia** recopilada (la evidencia es el sustento que va a sostener la opinión que voy a dar como auditor, sin evidencia no puedo hacer un trabajo de auditoría, los "me parece o puede ser" no sirven), y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia. Para la **recolección de información** se utilizan la observación, entrevistas, cuestionarios, encuestas, y la actuación.
Metodología:
1. **Estudio Preliminar:** Definir el grupo de trabajo. Definir el programa de auditoría. Visitar el Sector informático. Evaluar el Control interno. Conocer el plan de actividades. Solicitar documentos de política, reglamentos, normas. Entrevistar a los principales referentes de la Organización y del Departamento Informático.
2. **Revisión Y Evaluación De Controles Y Seguridades:** Diagramas de flujo de procesos. Pruebas de cumplimiento de las seguridades. Aplicaciones de las áreas críticas. Procesos históricos (backups). Documentación y archivos.
3. **Examen Detallado De Las Áreas Críticas:** Distribución de tareas entre su grupo de trabajo. Define motivos, objetivos, alcances y recursos a utilizar. Define metodología de trabajo. Establece la duración de la auditoría (durante este periodo no debería modificarse el objeto de estudio). Presenta el plan de trabajo. Analizará detalladamente cada problema encontrado con lo ya analizado en la etapa 2. (Revisión y evaluación de controles y seguridades).
4. **Comunicación De Resultados:** Informe preliminar para ser discutido con los ejecutivos. Informe definitivo (matriz, cuadros, redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la auditoría). El **informe es el documento más importante de la auditoría informática, en el cual se presentan los resultados obtenidos durante la evaluación**. Debe contener:

- Motivos de la auditoría.
- Objetivos: cuestiones a verificar (existencia de.., si la selección de.., si existen garantías para..)
- Alcance: período que comprende, cuáles departamentos abarca y las correspondientes limitaciones y restricciones encontradas.
- Estructura Orgánico-funcional del área informática.
- Configuración del Hardware y Software instalado.
- Control Interno.
- Resultados de la Auditoría.
- Conclusiones.
- Recomendaciones.
- Fecha
- Identificación y firma de los auditores.
- Distribución del informe.

Así mismo el informe debe ser claro, adecuado, suficiente, comprensible, y debe encontrarse redactado en un formato lógico y organizado. De esta forma debe incluir suficiente información para que sea comprendido por los destinatarios esperados facilitando las acciones correctivas.

Para evidenciar esto el informe cuenta con una serie de **requisitos**:

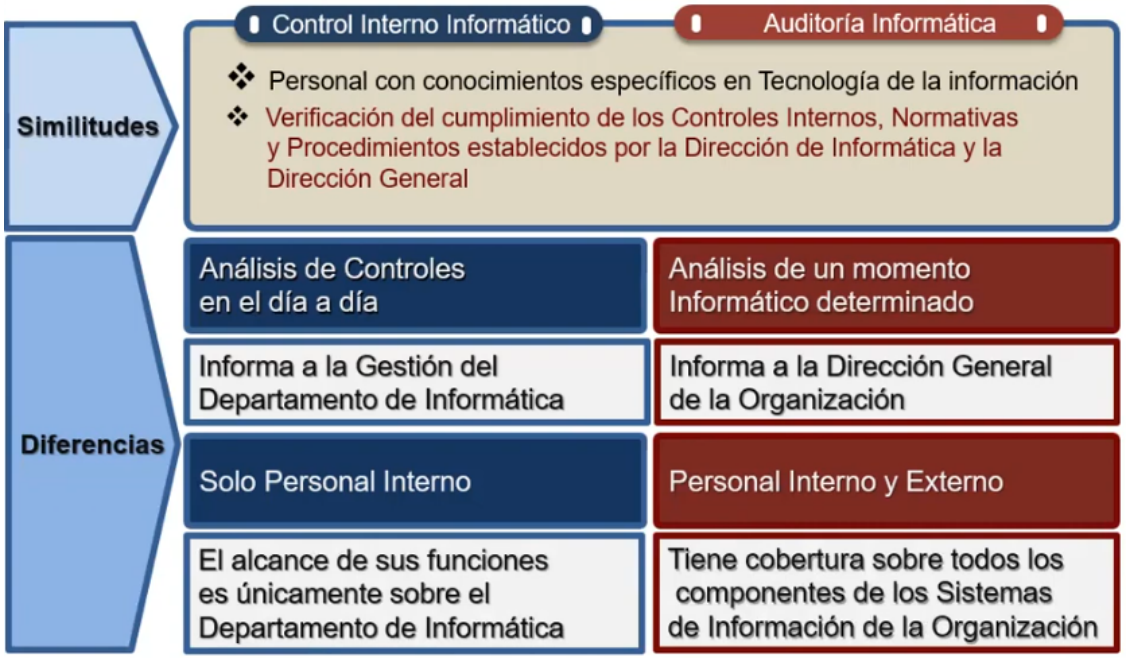
- Ser veraz
- Estar documentado formalmente
- Mostrar las observaciones (debilidades) encontradas
- Tener recomendaciones y soluciones para cada una de las observaciones.
- Reflejar las áreas involucradas y cursos de acción.

Cualidades y requisitos de un auditor

- Formación (buen profesional, conocimientos completos)
- Experiencia
- Independencia (actitud mental, actuar con libertad)
- Objetividad (actitud imparcial – no dejarse influenciar)
- Madurez
- Integridad (rectitud intachable, honestidad)
- Capacidad de análisis y síntesis
- Responsabilidad e interés
- Perfil específico según: nivel del puesto, entorno de trabajo y áreas a auditar
- Puesta al día de los conocimientos.

Control interno informático =/ Auditoría informática

Ambos sectores se encargan de verificar el cumplimiento de los Controles Internos, normativas y procedimientos establecidos por la Dirección de Informática y la Dirección General, utilizando para ello personal con conocimiento específico en tecnologías de la información.
La diferencia entre ambos son que el Control Interno Informático realiza un análisis día a día, en cambio la A.I analiza un momento informático determinado. Por otro lado el CII informa los resultados a la gestión del departamento de informática de la organización; en cambio, la AI informa a la Dirección general de la organización.
Otra de las diferencias es que los CII utilizan para su desarrollo a integrantes del personal interno únicamente, a diferencia de la AI que requiere personal interno y externo para su implementación. Finalmente como consecuencia de las demás diferencias se evidencia que el CII tiene un alcance reducido de sus funciones, sólo sobre el departamento de informática; y, en cambio, la AI tiene cobertura sobre todos los componentes de los Sistemas de Información de la organización.



UNIDAD 2: Auditoría de la Dirección de Informática

Clase 3:

Actividades básicas de la Auditoría de la Dirección Informática:

1 - Planificar

Los beneficios que se tienen, en primer lugar, es que se evita improvisar en las acciones a tomar. Eso implica determinar en dónde se está, hacia dónde se quiere ir y cómo se va a llegar a ese punto, para lo cual es necesario determinar el esfuerzo requerido, así como los beneficios asociados.

Realizar una planificación permite tanto ahorrar tiempo y dinero, como así también tomar mejores decisiones en cuanto a informática, teniendo de este modo, una herramienta que permita medir los avances en automatización. Además, facilita el entendimiento y la comunicación.

Pasos de la Planificación:

Prever la Utilización de las Tecnologías de la Información (TICs) en la Empresa ➡ Creación de Planes Informáticos ➡ PLAN ESTRATÉGICO DE SISTEMAS DE INFORMACIÓN.

Distintos planes que se llevan adelante:

Plan estratégico de sistemas de información: debe estar aprobado y una vez que sucede esto tiene una vigencia de largo plazo (1 a 3 años). A su vez debe estar alineado con los objetivos empresariales, y una vez puesto en marcha no es responsabilidad exclusiva de la Dirección de Informática, pero sí su impulso y concreción.

Plan Operativo Anual: Se establece al comienzo de cada año. El mismo describe las actividades a realizar durante el ejercicio: Sistemas a Desarrollar, cambios tecnológicos previstos, recursos necesarios y plazos a cumplir.

Plan de Recuperación ante Desastres: Tiene en cuenta desastres de variada naturaleza, la indisponibilidad del servicio informático adecuado, o la falla de algún componente crítico de hardware.

Tareas de Auditoría en la etapa de planificación:

1. Examinar el Proceso de Planificación de Sistemas de Información
2. Evaluar si razonablemente cumple con los Objetivos
3. Evaluar si las Tareas y Actividades en el Plan tienen la correspondiente y adecuada Asignación de Recursos para poder llevarse a cabo.
4. Revisar Actas Confeccionadas Dedicadas a la Planificación Estratégica

2 - Organizar y coordinar

Sirve para Estructurar los Recursos, los Flujos de Información y los Controles que permitan alcanzar los Objetivos marcados durante la Planificación.

En esta etapa es fundamental la existencia de un **Comité de Informática:** Lugar de Encuentro dentro de la Empresa de los Informáticos y sus Usuarios, en donde se debaten los grandes asuntos de la Informática que afectan a toda la Empresa. Permite a los Usuarios conocer las necesidades del conjunto de la Organización y participar en la Fijación de Prioridades. La conformación del comité permite impedir favoritismos y fomentar una mejor utilización de los recursos informáticos, los cuales son recursos escasos.

Funciones del comité de informática:

1. Aprobación Plan Estratégico de Sistemas de Información
2. Aprobación Inversiones en Tecnología de la Información
3. Fijación de Prioridades entre los grandes Proyectos Informáticos
4. Vehículo de discusión entre la Informática y sus Usuarios
5. Vigila y Realiza Seguimiento de la Actividad del Departamento de Informática.

Auditoría del comité de informática:

1. Asegurar que el Comité de Informática existe y cumple su papel adecuadamente
2. Conocer las Funciones encomendadas al Comité y sus Integrantes
3. Entrevistas a Miembros Destacados del Comité
4. Entrevistas a Representantes de los Usuarios
5. Establecer Juicio sobre validez, adecuación y Actuación del Comité

Departamento de Informática:

Ubicación en la empresa: Ubicación ALTA en la Jerarquía de la Empresa. Contar con Masa Crítica suficiente. Poseer Autoridad e Independencia frente a las Áreas de los Usuarios.

Auditoría: Revisar el Emplazamiento Organizativo del Departamento Informática y Evaluar su Independencia

Descripción de Funciones y Responsabilidades del Dpto. de Informática: División en Unidades Organizativas. Funciones y Responsabilidades delimitadas y documentadas. Personal que conoce las mismas

Auditoría:

1. Examen del Organigrama del Dpto. Informática e Identificación de las grandes Unidades Organizativas
2. Revisión Documentación existente sobre Funciones y Responsabilidades
3. Entrevistas a responsables de cada Unidad Organizativa
4. Entrevistas y Observación al Personal de las otras Áreas

Estándares de Funcionamiento y Procedimientos: Deben existir estándares para saber qué Controles se deben establecer y cómo son las Relaciones entre Áreas.

La Dirección de Informática es quien promueve estándares y procedimientos, que deben ser documentados, actualizados cuando se deba, y comunicados.

Auditoría: Adquisición de Equipos y/o Materiales para el Dpto. de Informática. Diseño, Desarrollo y Mantenimiento de Sistemas. Producción o Explotación (segregación de funciones).

Gestión de Recursos Humanos

La calidad de los recursos humanos influye en la calidad de los sistemas informáticos. En ese sentido es fundamental que se **Audite** el modo de:

1. Selección: se basa en criterios objetivos y tiene en cuenta la Formación, Experiencia y los Niveles de Responsabilidad.
2. Formación: Existen Procesos para determinar las necesidades de Formación de los Empleados en Base a su Experiencia, Puesto de Trabajo, Responsabilidades y Desarrollo futuro personal y tecnológico de la Instalación.
3. Evaluación del desempeño: El Rendimiento de cada Empleado se evalúa regularmente en base a Estándares establecidos y Responsabilidades Específicas del Puesto de Trabajo.
4. Promoción: Existen Procesos para la Promoción del Personal que tienen en cuenta su Desempeño Profesional.
5. Finalización de los recursos humanos: Existen Controles que tienden a asegurar que el Cambio de Puesto de Trabajo y la Finalización de los Contratos Laborales NO afecten a los Controles Internos y a la Seguridad Informática.

Comunicación

Una buena comunicación entre la Dirección de Informática y el Personal de las áreas informáticas permite un compromiso con la calidad, actitud positiva hacia los controles, integridad, ética y el cumplimiento de las normas internas.

Gestión económica

Responsabilidades de la Dirección Informática: presupuestación, adquisición de bienes y servicios, y medición y reparto de costos.

Seguros

La dirección de informática debe poseer suficientes coberturas para los sistemas informáticos.

3 - Controlar

Refiere a efectuar un Seguimiento Permanente de las Distintas Actividades del Departamento. Para ello es posible aplicar estándares de rendimiento relacionados al consumo de recursos, operatividad y desarrollo.

A su vez se debe asegurar el cumplimiento de la normativa legal:

1. Seguridad e Higiene en el Trabajo
2. Normatividad Laboral y Sindical
3. Protección de Datos Personales
4. Propiedad Intelectual del Software
5. Requisitos Definidos en la Cobertura de Seguros

6. Contratos de Comercio Electrónico
7. Transmisión de datos por líneas de Comunicaciones
8. Normativas emitidas por Órganos Reguladores Sectoriales

Auditoría de la Dirección Informática

Es una tarea muy difícil pero esencial, que tiene gran influencia en el comportamiento de los sistemas informáticos.

UNIDAD 3: Protección de Datos Personales

Clase 4:

Información y datos sobre los integrantes de una organización:

- Personalidad
- Actitud
- Comportamiento
- Economía
- Hábitos sociales
- Hábitos de consumo

Estos datos están en manos de terceros, conocidos y desconocidos. Por eso surgen distintas preguntas como ¿Dónde están mis datos? ¿Cuál es el destino de los datos que proporcionamos en las múltiples transacciones cotidianas? ¿Quiénes los utilizan y con qué fines? ¿Tenemos verdadera autodeterminación sobre nuestros datos? ¿Qué control ejerce el Estado para protegernos?

Perfiles virtuales: el la acumulación de los distintos tipos de datos acerca de una persona que se pueden tener a disposición, ya sea en la industria privada del dato (creación de bancos de datos) como en la industria del dato público (gobierno electrónico y servicios), que permiten generar una idea de quién es una persona, y se convierte en un factor para la toma de decisiones. Esto afecta de forma positiva o negativa a las personas.
El uso de la tecnología y el tratamiento de los datos no afectan a los derechos de las personas. Lo que pone en riesgo los derechos, es el uso indebido y no ético de los datos.

Leyes regulatorias de los datos personales:

Constitución Nacional Art. 43 - 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 los cuales los emplean, y en caso de falsedad o discriminación, poder exigir la supresión, rectificación, confidencialidad o actualización.

Ley Nacional de Protección de Datos Personales - Ley 25326 / 2000

Protección integral de los datos personales de personas físicas e ideales, que se encuentren asentados en archivos, registros, bancos de datos, y otros medios técnicos de tratamiento de datos.
La protección integral sirve para garantizar el derecho al honor y a la intimidad de las personas, como así también tener acceso a la información que sobre las mismas se registre de conformidad a la constitución nacional en su artículo 43.

Dato personal: información de cualquier tipo referida a personas físicas o de existencia ideal, ya sean determinadas (nombre y apellido, DNI, fecha de nacimiento, domicilio), como así también la determinable

(identidad que pueda determinarse directa o indirectamente: perfil psicológico, físico, fisiológico, económico, cultural o social).

Datos personales excluidos: aquellos datos almacenados en archivo de uso interno, personal o doméstico, bases de datos de fuentes periodísticas, y archivos de datos recopilados con fines estadísticos, disociados de la entidad titular.

Datos sensibles: son aquellos datos que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, información referente a la salud, e información referente a la vida sexual. Son datos que ponen en peligro nuestra integridad y nuestro honor. Ninguna persona puede ser obligada a proporcionarlos, solo pueden ser recolectados por razones de interés general autorizadas por ley, o también con finalidad estadística o científica cuando no se identifiquen sus titulares. Está prohibido formar archivos, bases o registros de datos con datos sensibles.
Solo pueden usarse datos sensibles bajo ciertos contextos:

- ➔ Asociaciones religiosas, organizaciones políticas o sindicales pueden llevar registros de sus miembros.
- ➔ Las autoridades competentes bajo leyes y reglamentaciones pueden utilizar antecedentes penales o contravencionales.
- ➔ Establecimientos sanitarios, públicos, privados, y profesionales de la salud pueden hacer uso de datos sensibles bajo el secreto profesional.
- ➔ Las entidades financieras pueden revelar datos personales solo ante causas judiciales, organismos recaudadores, y ante el banco central.

Archivo, registro, base o banco de datos: Es un conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. El RESPONSABLE de archivo, registro, base o banco de datos es una persona física o de existencia ideal, pública o privada que es titular de un archivo, registro, base o banco de datos.

Datos informatizados: son aquellos datos personales sometidos a tratamiento o procesamiento electrónico o automatizado.

Tratamiento de datos: son aquellas operaciones y procedimientos sistemáticos, electrónicos o no, que permiten la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo y restricción y en general todo procesamiento de datos personales. Así también contempla la cesión a terceros a través de comunicaciones, consultas, interconexiones, o transferencias.
Titular de los datos: persona física o de existencia ideal con domicilio legal en el país, cuyos datos sean objeto del tratamiento.

Usuarios de datos: persona pública o privada que realice a su arbitrio el tratamiento de datos ya sea en archivos, registros, o base de datos propios o a través de conexión con los mismos.

Disociación de datos: tratamiento de datos personales de manera que la información obtenida no puede asociarse a persona determinada o determinable.

Licitud: formar archivos de datos personales es lícito solo si se encuentran debidamente inscriptos en los organismos de control (agencia de acceso a la información pública).
Licitud sin consentimiento: el tratamiento de datos personales es lícito sin necesidad de consentimiento cuando se trate de

- ➔ Datos obtenidos por fuentes de acceso público e irrestricto
- ➔ Datos 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 de nacimiento - Domicilio.
- ➔ Derivados de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento.

Registro de archivos de datos

Al registrar un archivo de dato se debe especificar:

- ➔ Nombre y domicilio del responsable
- ➔ Características y finalidad del archivo
- ➔ Destino de los datos y a quiénes pueden ser transmitidos
- ➔ Modo de interrelacionar la información registrada
- ➔ Medios para garantizar la seguridad de los datos
- ➔ Tiempo de conservación de los datos
- ➔ Forma y condiciones para el acceso a los datos
- ➔ Procedimientos para realizar rectificación o actualización.

Bases de datos personales

El responsable de las Bases de datos personales es la persona humana o jurídica pública o privada (empresas, instituciones, organizaciones de la sociedad civil, etc) que sean titulares de un archivo, registro, base o banco de datos.

De acuerdo a la normativa vigente, los responsables de bases de datos personales públicas y privadas destinadas a dar informes, deberán inscribirlas en el Registro Nacional de Bases de Datos. Las bases de datos de uso exclusivamente personal están exceptuadas de la obligación de inscripción, por ejemplo: direcciones de amistades en computadoras personales, agendas personales, etc.

Bases de datos personales destinada a dar informes: es todo registro, archivo, base o banco de datos que permita obtener información sobre las personas, se transmitan o no a terceros. Es un banco de datos destinado a describir algo sobre las personas. Se brinda un informe cuando se accede a una base de datos que interrelaciona datos, y produce una serie de informaciones acerca de una persona determinada.

Obligaciones de los responsables de bases de datos personales:

1 - Inscripción

2 - Información al titular

- ➔ Se debe informar la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios.
- ➔ Informar la 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.
- ➔ Consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de estos.
- ➔ Posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.

3 - Seguridad de los datos

El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

4 - Transferencia internacional

Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

La prohibición no regirá en los siguientes supuestos:

- ➔ Colaboración judicial internacional;
- ➔ Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso del artículo anterior;
- ➔ Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

- ➔ Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;
- ➔ Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Bases de datos de videovigilancia:
Una imagen o registro fílmico constituye, a efectos de la ley 25326 un dato de carácter personal, en tanto que una persona pueda ser determinable o determinada. Una imagen con formato digital permite su tratamiento a través de sistemas informáticos y conformar un sistema organizado de fácil consulta.
La base de datos de videovigilancia debe ser declarada a través de un formulario, además de presentar también el manual de tratamiento de datos personales cuyos requisitos mínimos son los aclarados en la disposición 10/2015.
El manual de videovigilancia debe contener:

- ➔ Forma de recolección
- ➔ Referencia de lugares, fechas y horarios en los que se prevé que operarán
- ➔ Plazo de conversación de los datos
- ➔ Mecanismo técnicos de seguridad y confidencialidad previstos.
- ➔ Medidas para el cumplimiento de los derechos del titular del dato según la ley 25326
- ➔ Argumentos que justifiquen la toma de fotografías
- ➔ Se debe informar al público la existencia de cámaras de seguridad, los fines para que se captan las imágenes, y los datos de contacto del responsable de la base de datos, para que las personas puedan ejercer sus derechos como titulares de datos personales.

Calidad de los datos

1. Los datos pertenecientes a archivos de datos deben ser ciertos, adecuados y pertinentes o no excesivos.
2. No deben utilizar medios de captura desleales o fraudulentos.
3. No pueden utilizarse para otras finalidades distintas a las que motivaron su obtención
4. Datos exactos y actualizados, o deben suprimirse.
5. Almacenados de forma tal que permitan el derecho al acceso de su titular.
6. Deben destruirse cuando dejan de ser necesarios o pertinentes.

Seguridad de los datos
El responsable o usuario de un archivo debe adoptar medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales, de modo tal que se pueda evitar la adulteración, pérdida, consulta o tratamiento no adecuado, detectando así las desviaciones de información.
Está prohibido reunir datos personales sin implementar medidas acerca de la integridad y seguridad de los datos, así como también transferir datos personales a países y organismos internacionales que no proporcionen niveles de protección adecuadas.

Derechos de los titulares de datos: derecho de información, acceso, rectificación, actualización o supresión.

Violación de los derechos: cuando exista un archivo que no se ajuste a la ley, se debe denunciar el hecho ante la Agencia de Acceso a la Información Pública, y también existe la acción judicial de Habeas DAta, para tomar conocimiento de datos personales alamcenados.

Agencia de Acceso a la Información Pública: es el órgano de control que hace cumplir la ley y sus disposiciones, informa a los titulares, censa archivos, dicta normas y reglamentaciones, controla la integridad y seguridad existente sobre los datos, solicita información a entidades públicas y privadas, e impone sanciones.

Decreto Reglamentario 1558 / 2001 y sus modificatorias

Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizados

A. **Recolección de datos:** Relacionado con los procesos necesarios para asegurar la completitud e integridad de los datos, minimizar los errores e implementar las medidas técnicas con el objeto de asegurar la confidencialidad y limitar el acceso durante la recolección.

B. **Control de acceso:** Relacionado con la implementación de medidas de seguridad, mecanismos de autenticación, segregación de roles y funciones, y demás características del acceso a los sistemas para la protección de la identidad y la privacidad.

C. **Control de cambios:** Relacionado con la implementación de los procesos para identificar fehacientemente a toda persona que acceda a realizar cambios en los entornos productivos que contengan datos personales, garantizando su identificación, autenticación y autorización correspondiente.

D. **Respaldo y recuperación:** Destinado a la implementación de los procesos de respaldo que permitan una correcta recuperación ante un incidente que impida el acceso a la información originalmente almacenada, definiendo prácticas de seguridad, difusión, entrenamiento y capacitación, para el desarrollo de tareas preventivas y correctivas de los incidentes de seguridad.

E. **Gestión de vulnerabilidades:** Destinado a la implementación de procesos continuos de revisión que permitan identificar, analizar, evaluar y corregir todas las vulnerabilidades posibles de los sistemas informatizados que traten información, aplicando técnicas de control de la integridad, registro, trazabilidad y verificación.

F. **Destrucción de la información:** Relacionado con la implementación de los procesos de eliminación de datos, asegurando que el contenido confidencial sea debidamente destruido, utilizando métodos de borrado seguro y aplicando un control eficaz del proceso.

G. **Incidentes de seguridad:** Relativo al tratamiento de los eventos y consecuentes incidentes de seguridad que puedan afectar los datos personales, su detección, evaluación, contención y respuesta, como así también las actividades de escalamiento y corrección del entorno técnico y operativo.
   Notificación ante incidentes: se deben establecer procedimientos de gestión ante incidentes de seguridad, así como también establecer una persona que sea responsable de la comunicación en estos casos. Además, al ocurrir un incidente se debe elaborar el correspondiente informe que tenga de contenido mínimo la naturaleza de la violacion, la categoría de datos personales que fueron afectados, quiénes fueron los usuarios afectados, la medidas que adoptará el responsable para mitigar el incidente, y cuáles son las medidas que se aplicarán para evitar ese tipo de incidentes. Además se deberá informar por mail una notificación del incidente ocurrido a la Agencia de Acceso a la Información Pública.

H. Entornos de Desarrollo: Relativo a la definición de los entornos de desarrollo de los sistemas de información, sean propios o de terceros.

The General Data Protection Regulation (GDPR)

Regulación General de Protección de información

Los afectados son organizaciones que retengan o usen información de personas pertenecientes a la Unión Europea, independientemente de dónde estén ubicadas.

Da a las personas más control sobre sus datos personales y obliga a las empresas a asegurarse de que la forma en que recopilan, procesan y almacenan información es segura.
La idea central es la privacidad por defecto.

Ley 26951 / 2014 - Registro Nacional "NO LLAME"

Objeto. El objeto de la presente ley es 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.
Inscripción. Podrá inscribirse en el Registro Nacional "No Llame" toda persona física o jurídica titular o usuario autorizado del servicio de telefonía en cualquiera de sus modalidades que manifieste su voluntad de no ser contactada por quien publicitare, ofertare, vendiere o regalare bienes o servicios, sin perjuicio de lo dispuesto en el artículo 27 de la ley 25.326.
Efectos. Quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía en cualquiera de sus modalidades son considerados usuarios y/o responsables de archivos, registros y bancos de datos de acuerdo a lo dispuesto en la ley 25.326. Los mismos no podrán dirigirse a ninguno de los inscriptos en el Registro Nacional "No Llame" y deberán consultar las inscripciones y bajas producidas en el citado registro con una periodicidad de treinta (30) días corridos a partir de su implementación, en la forma que disponga la autoridad de aplicación.
Excepciones. Quedan exceptuadas de la presente ley:

1. Las campañas de bien público, tal como lo dispone la ley 25.326;
2. Las llamadas de emergencia para garantizar la salud y seguridad de la población;
3. Las campañas electorales establecidas por ley 19.945, modificatorias y concordantes;
4. Las llamadas de quienes tienen una relación contractual vigente, siempre que se refieran al objeto estricto del vínculo y sean realizadas en forma y horario razonables y de acuerdo a la reglamentación;
5. Las llamadas de quienes hayan sido expresamente permitidos por el titular o usuario autorizado de los servicios de telefonía en cualquiera de sus modalidades, inscriptos en el Registro Nacional "No Llame".

Creación de la Dirección Nacional de Protección de Datos Personales

Es el órgano de aplicación de la ley de protección de datos personales (ley 25.326) del gobierno de la República Argentina. Depende del Ministerio de Justicia y Derechos Humanos.
Tiene a su cargo el Registro Nacional de las Bases de Datos, instrumento organizado a fin de conocer y controlar las bases de datos que circulan en el país. Además, asesora y asiste a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos. Las denuncias que se hagan ante la DNPDP, son al exclusivo efecto de revelar deficiencias o incumplimientos a las normas aplicables en el tratamiento de los datos personales que hagan los archivos, registros bancos o bases de datos.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

UNIDAD 4: Firma Digital

Clase 5:

Problemática: poder enviar documentos electrónicos que mantengan las mismas garantías de seguridad jurídica a los documentos electrónicos que las establecidas para un documentos en papel firmado digitalmente.

Firma Digital: se entiende por firma digital al resultado de aplicar un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control.
La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.
Propiedades:

- ➔ Autenticidad del origen del mensaje: atribuye el documento a su autor de forma fidedigna, de manera de poder identificarlo.
- ➔ Integridad de la información: protege la información contra la modificación de los datos, poniendo en evidencia cualquier alteración posterior a la firma.
- ➔ No repudio: protege al receptor del documento de la negación del emisor de haberlo enviado.
- ➔ Exclusividad: garantiza que la firma se encuentra bajo el absoluto y exclusivo control del firmante

Certificado digital: documento digital que da fe de la vinculación entre una clave pública y una persona o entidad. Firmado digitalmente por la autoridad que lo emite y como mínimo contiene: nombre, clave pública, fecha de expiración, nombre de la autoridad emisora, certificado digital de la autoridad emisora.

Ley 25506/2001
Validez de firma electrónica y firma digital

Reconoce el empleo de la firma electrónica y firma digital y su eficacia jurídica. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital.
Establece una presunción de validez en la firma digital, **no así en el caso de la firma electrónica.**
Los documentos electrónicos firmados digitalmente se consideran originales y poseen valor probatorio.
La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los documentos digitales firmados digitalmente.
Permite la anulación o destrucción del papel.

Firma electrónica: conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

UNIDAD 5: Seguridad Informática - Seguridad de la Información - SGSI
Clase 6:

Seguridad Informática: Se hace alusión a los aspectos técnicos de la seguridad, es decir se refiere a la protección de los datos en formato digital almacenados o en tránsito.

Seguridad de la información: tiene un enfoque integral respecto a la protección de la información dentro de una organización, es decir independientemente al medio en que se almacene o transmita: digital, papel, cintas, conversaciones, personas, etc.

Flujo de la información: el intercambio de datos entre diferentes componentes de una organización dan lugar al flujo de la información, donde los involucrados comunican, procesan y almacenan la misma.
El intercambio de información ocasiona una transacción, y esto genera un riesgo.

Aspectos a cubrir en Seguridad de la Información:
La información es uno de los activos principales de una organización, es por eso que debe protegerse. Para ello se deben analizar:

- ➔ Vulnerabilidades / Amenazas

- ➔ Riesgos
- ➔ Procesos
- ➔ Planes de negocio
- ➔ RRHHs

Pilares de la Seguridad de la Información:

- ➔ Integridad: que sea confiable
- ➔ Confidencialidad: solo conocida por quienes deban
- ➔ Disponibilidad: acceder cuando se necesite

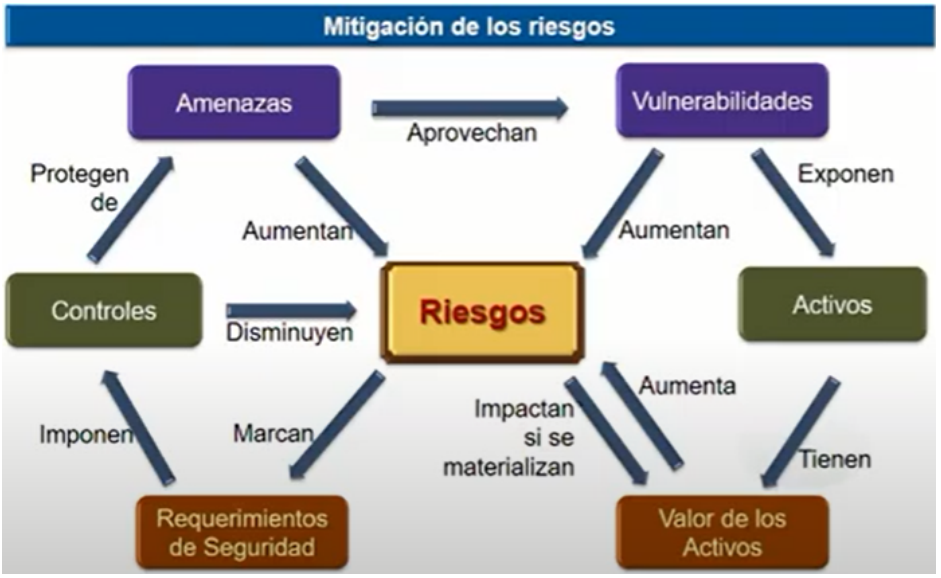
Amenazas

- ➔ Hacking: los piratas informáticos acceden a sistemas informáticos para alterarlos.
- ➔ Trashing: rastreo en los papeles información, contraseñas, directorios, etc.
- ➔ Wardriving: búsquedas de redes inalámbricas desde vehículos móviles.
- ➔ Desastres: naturales, accidentales, intencionales.

El 30% de los incidentes de seguridad corresponden a incidentes externos, como por ejemplo los virus. El resto de incidentes internos, como pueden ser errores de usuarios.

La Seguridad de la Información involucra a organizaciones de todos los tamaños y todos los sectores. No importa cuán segura y bien protegida aparente ser una organización, la información más sensible puede ser atacada sin que nos demos cuenta.

La información de todas las áreas, ya sea en discos de computadoras, papel, o en la cabeza de las personas está expuesta a amenazas.



Gestión de riesgos:

La Gestión de la Seguridad Informática involucra a la gestión de riesgos, es decir la identificación, medición, control y minimización de pérdidas asociadas con determinados eventos o “Riesgos”.

El Riesgo implica “Probabilidad” e “Incertidumbre” ya que se analiza la probabilidad de ocurrencia de un evento indeseable, como así también su magnitud.

El Riesgo CERO o la Seguridad absoluta no existen, esto significa que hay que aprender a convivir con el riesgo: riesgo residual o riesgo aceptado.

Sistemas de Gestión de la Seguridad de la Información
ISO/IEC 27001:2013
Cómo manejar los Riesgos: Gestión de Riesgos

1. **Planificar:**

a. Determinar el **alcance**: La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información. Así también la organización debe determinar las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información; y los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.
b. Definir la **política**: La alta dirección debe establecer una política de seguridad de la información que:
    i. sea adecuada al propósito de la organización;
    ii. Incluya objetivos de seguridad de la información o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información;
    iii. Incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información;
    iv. Incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.
c. **Metodología:** La organización debe planificar:
    i. Las acciones para tratar estos riesgos y oportunidades; y
    ii. La manera de integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información.
    iii. La manera de evaluar la eficacia de estas acciones.

2. Identificar activos, amenazas y vulnerabilidades:

La organización debe definir y aplicar un proceso de **apreciación de riesgos** de seguridad de la información que:

a. establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:
    i. los criterios de aceptación de los riesgos, y
    ii. los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información;
b. asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;
c. identifique los riesgos de seguridad de la información:
    i. Llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,
    ii. Identificando a los dueños de los riesgos;

3. Analizar los Riesgos

a. Identificar amenaza: valorar las posibles consecuencias que resultarían si los riesgos llegasen a materializarse.
b. Determinar frecuencia: valorar de forma realista la probabilidad de ocurrencia de los riesgos identificados.
c. Análisis del impacto: determinar los niveles de riesgo;

Además se deben evaluar los **riesgos de seguridad** de la información:

d. Comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos.
e. Priorizar el tratamiento de los riesgos analizados. La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información.

4. Decidir:

a. **Tratamiento** del riesgo: La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para:
    i. Seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos;
    ii. Determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

iii. Comprobar que no se han omitido controles necesarios.
b. Análisis del costo: cuánto puede costar
c. Análisis del costo/beneficio: es costo efectivo?

Acciones que se pueden llevar adelante ante un Riesgo:

- ➔ **Aceptación:** se documenta la información de dejar que el riesgo se materialice.
- ➔ **Mitigación:** Se deben seleccionar controles, luego estructurarlo a partir de una arquitectura orientada a servicios, para finalmente implementar las acciones necesarias para disminuir el impacto de los riesgos.
- ➔ **Transferencia:** refiere a delegar el riesgo para que sea asumido o tratado por un tercero, como por ejemplo seguros o proveedores.
- ➔ **Evitar:** se toman acciones que tienden al cese de las actividades que originan el riesgo. Esto permite disminuir la probabilidad de ocurrencia del riesgo.

Responsables e involucrados con la Seguridad de la Información

Todas las personas que interactúan con la organización se conciben como involucrados en la Seguridad de la Información: alta dirección, socios/inversores, clientes, proveedores y contratistas, empleados, gobierno.

Instrumentar la Seguridad de la Información

Se debe lograr un cambio en la cultura organizacional, que provenga de la alta dirección, instrumentando varios medios para hacer llegar el mensaje que provoque el cambio y lo haga perdurar en el tiempo. Esto se puede llevar adelante a partir de

- ➔ Divulgación y capacitación
- ➔ Mensajes y carteles
- ➔ Premios y castigos
- ➔ Conformación de un Grupo de Seguridad, para instrumentar los controles y auditar el cumplimiento de los mismos

Aspectos Tecnológicos: implementación de controles preventivos, directivos y correctivos: antivirus/antispam, firewall, manejo de eventos y paquetes de información, detección de intrusos, VPN.
Aspectos Funcionales: definición de la Política de Seguridad, implementación de Procedimientos, Seguimiento de Registros.
Política de seguridad: contiene las directivas de la Alta Dirección para crear un programa de seguridad de la información, establecer sus objetivos, mediciones y asignar responsabilidades.

Sistema de Gestión de Seguridad de la Información (SGSI)

El propósito de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, controlados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno, y las tecnologías.
El SGSI ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con el objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.
Con un SGSI la organización conoce los riesgos y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora continuamente.

Proceso de implementación de la norma ISO 27001

1. Adquirir el estándar
2. Establecer capacitación
3. Reunir el equipo de trabajo
4. Definir el alcance
5. Identificar activos de la información
6. Determinar el valor de los activos
7. Determinar los riesgos

8. Determinar el grado de Aseguramiento y controles
9. Identificar los objetivos de control y controles
10. Definir las políticas y procedimientos y controles a implantar
11. Implantar las políticas, procedimientos y controles
12. Completar los requerimientos del SGSI
13. Auditoría y revisión del SGSI
14. Seleccionar un ente certificador
15. Acuerdo con el ente Certificador
16. Etapa 1: revisión de documento
17. Etapa 2: auditoría implantación
18. Certificación
19. Evaluación periódica

Etapas del proceso de implementar un Sistema de Gestión de la Seguridad Informática

1 - Planificar

- ➔ Definir la política de seguridad
- ➔ Establecer el alcance del SGSI
- ➔ Realizar el análisis de riesgo
- ➔ Seleccionar los controles
- ➔ Definir competencias
- ➔ Establecer un mapa de procesos
- ➔ Definir autoridades y responsabilidades

2 - Hacer

- ➔ Implantar el plan de Gestión de Riesgos
- ➔ Implantar el SGSI
- ➔ Implantar los controles

3 - Verificar

- ➔ Revisar externamente el SGSI
- ➔ Realizar auditorías internas del SGSI
- ➔ Poner en marcha indicadores y métricas
- ➔ Hacer una revisión por parte de la dirección

4 - Actuar

- ➔ Adoptar acciones correctivas
- ➔ Adoptar acciones de mejora

Pasos claves de la implementación de ISO 27001

- ➔ Lograr el compromiso de alta dirección
- ➔ Definir la conformación del comité de seguridad
- ➔ Organizar el grupo de trabajo y acordar la estrategia de trabajo
- ➔ Nombrar al oficial de seguridad
- ➔ Capacitar al personal directamente involucrado (o tercerizar los recursos)
- ➔ Definir el alcance del SGSI
- ➔ Evaluar la brecha entre los requisitos de la ISO 27001 y la situación actual
- ➔ Armar el Plan de Trabajo para alinearse con los requisitos de la ISO 27001
- ➔ Determinar los activos de información, sus valores y propietarios
- ➔ Realizar el análisis y la evaluación de Riesgos

Razones para adoptar estándares:
Establecer medidas de seguridad de acuerdo al tipo de negocio. Mejorar los controles sobre los riesgos de TI y su gestión. Identificación de peligros y reducir los incidentes de seguridad de la información. Optimizar los costos mediante medidas de seguridad de TI que preserven la operatividad de la empresa. Demostrar al mercado la responsabilidad y compromiso en materia de seguridad de la información, logrando competitividad.

Ventajas:
Disminución de los riesgos. Implementación de controles efectivos. Protección de los activos de la organización y de los clientes. Continuidad operativa y del negocio. Prevención y atención inmediata de incidentes. Cumplimiento de normas y regulaciones. Concientización sobre el valor de la información de la organización. Gerenciamiento optimizado ante normas, políticas y procedimientos.

Conclusiones
La seguridad en TIC es un proceso que afecta a toda la Organización
Las organizaciones deben definir una estrategia de seguridad basada en el negocio y no en la tecnología.
La seguridad que proporciona un SGSI es permanente, puesto que es un proceso y no acciones puntuales.
El enfoque de la seguridad debe ser integral, si no puede conducir a una falsa sensación de seguridad y al fracaso.
La seguridad de la información se basa en las personas.
Un problema de seguridad es todo aquello que manifiesta un riesgo en los activos de las organizaciones.
El escenario de riesgos en las organizaciones se agudiza vertiginosamente.
Toda organización está expuesta a amenazas.
La tecnología representa tantas ventajas evolutivas como peligros latentes (vulnerabilidades).
Sin un adecuado sistema de gestión de riesgos la seguridad por lo general es incompleta.
La implementación y/o certificación de normas permite a las organizaciones mantener un entorno confiable y proactivo alineado con los objetivos de la Alta Dirección.