**Repaso de todas las pruebas**

**Modulo #1**

**DESCRIPCIÓN**

En esta asignatura se pretende enseñar y dar la formación de los conceptos de la Auditoría Informática aplicado en los entornos informáticos. Comprende la evaluación de todas o algunas de sus áreas, los estándares y procedimientos, su calidad y el cumplimiento de ellos, de los objetivos fijados, de los contratos y las normas legales aplicables; el grado de satisfacción de usuarios y directivos; los controles existentes y un análisis de los riesgos.

**OBJETIVO GENERAL**

Orientar a los alumnos en la planificación, implementación y administración de un proyecto de auditoría de sistemas y a establecer las directrices generales de los procesos de auditoría informática en las organizaciones, bajo el marco del proceso de la auditoría, señaladas en sus Normas Generales, así como, determinar los diseños para los enfoques de auditoría más adecuados, considerando la identificación y la evaluación de los riesgos que pueden existir en las organizaciones, asegurando su integridad, oportunidad y confiabilidad de los procesos informáticos.

**Objetivos Específicos:**

1.  Interpretar y comprender los propósitos de la auditoria informática.

2.  Conocer métodos y técnicas de auditoría.

3.  Formar un criterio para la evaluación de riesgos de control.

4.  Conocer cómo usar adecuadamente el recurso informático en la auditoria.

5.  Identificar la función del auditor informático y reflexionar respecto de su misión.

Función de la informática en la empresa.

La **informática**, también llamada **computación**, ​ es una [ciencia](https://es.wikipedia.org/wiki/Ciencia) que administra métodos, técnicas y procesos con el fin de almacenar, procesar y transmitir [información](https://es.wikipedia.org/wiki/Informaci%C3%B3n) y [datos](https://es.wikipedia.org/wiki/Dato) en formato [digital](https://es.wikipedia.org/wiki/Electr%C3%B3nica_digital).

No existe una definición consensuada sobre el término, lo cual puede comprenderse a través de las Discusiones que acompañan esta página. Sin embargo, la Asociación de Docentes de Informática y Computación de la República Argentina han tomado una posición, definiéndola de la siguiente manera:

"La Informática es la disciplina o campo de estudio que abarca el conjunto de conocimientos, métodos y técnicas referentes al tratamiento automático de la información, junto con sus teorías y aplicaciones prácticas, con el fin de almacenar, procesar y transmitir datos e información en formato digital utilizando sistemas computacionales. Los datos son la materia prima para que, mediante su proceso, se obtenga como resultado información.  Para ello, la informática crea y/o emplea sistemas de procesamiento de datos, que incluyen medios físicos (hardware) en interacción con medios lógicos (software) y las personas que los programan y/o los usan (humanware). ​"

Es por lo que se hace distinción entre este término y las [Ciencias de la computación](https://es.wikipedia.org/wiki/Ciencias_de_la_computaci%C3%B3n), puesto que el segundo engloba la parte más teórica mientras que informática se refiere a la aplicabilidad de esta anterior en datos usando dispositivos electrónicos. De hecho se definen cinco subdisciplinas del campo de la informática: [**Ciencias de la computación**](https://es.wikipedia.org/wiki/Ciencias_de_la_computaci%C3%B3n)**,**[**ingeniería informática**](https://es.wikipedia.org/wiki/Ingenier%C3%ADa_inform%C3%A1tica)**,**[**sistemas de información**](https://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n)**,**[**tecnología de la información**](https://es.wikipedia.org/wiki/Tecnolog%C3%ADas_de_la_informaci%C3%B3n_y_la_comunicaci%C3%B3n)**e**[**ingeniería de software**](https://es.wikipedia.org/wiki/Ingenier%C3%ADa_de_software)**.**

**Funciones, Responsabilidades y Atribuciones:**

 a. Asegurar la operación eficiente de la plataforma de sistemas de información ERP que soportan los procesos de negocio, generando una ejecución eficiente, precisa, integral y confiable de la data e información que manejan y comparten.

 b. Apoyar los requerimientos de las Gerencias, que son usuarias de la información del sistema ERP, aplicando un concepto de servicio al cliente, basado en las necesidades y los problemas del negocio.

c. Apoyar al control de gestión, a través de la generación de información que permita realizar una evaluación permanente del desempeño del negocio.

d. Generar propuestas de modernización de la plataforma informática de la Empresa, para asegurar su actualización permanente y captar las oportunidades que plantea la innovación en materias informáticas.

e. Participar en la evaluación técnica de los proyectos de inversión en tecnologías de la información y comunicaciones, aportando antecedentes para su evaluación económica.

 f. Asegurar el perfeccionamiento continuo del personal en todas las áreas del conocimiento asociadas al trabajo en tecnologías de información y comunicaciones.

 g. Desarrollar las gestiones periódicas y necesarias para mantener permanentemente actualizadas las aplicaciones de las diferentes organizaciones en la Intranet y también de la página Web de la Empresa.

h. Apoyar directamente al Gerente de Planificación y Desarrollo en la gestión del Comité Informático. i. Velar por la correcta utilización de los sistemas de información con que cuenta la empresa.

## ¿Qué es la auditoria? Definiciones

Es un proceso formal que es llevado adelante por especialistas en auditoría y en informática a efectos de verificar y asegurar que los recursos y procesos involucrados en la construcción y explotación de los sistemas de información cumplen con los procedimientos establecidos y se ajustan a criterios de integridad, eficiencia, seguridad, efectividad y legalidad.

## Clases de auditoria

**• Auditoría contable:** Es el examen independiente de los estados financieros de una entidad con la finalidad de expresar una opinión sobre ellos. En este marco el auditor investiga críticamente los estados contables de una organización para formarse un juicio sobre la veracidad de tal información y comunicarlo a la comunidad.

**• Auditoría administrativa**: Es el control de la actividad desarrollada por los administradores de una organización; evalúa el desempeño de los mismos como ejecutivos, el cumplimiento de las metas programadas, la eficiencia en el uso de los recursos disponibles, el éxito o fracaso en las misiones encomendadas.

**• Auditoría Social:** Es el examen o evaluación sistemática sobre algún campo de acción significativo, definible, de actividades con repercusión social. • Auditoría médica Es el examen o evaluación de la calidad de los servicios médicos efectuados por los prestadores de salud. En Argentina este tipo de auditorías es efectuada por profesionales especializados vinculados a las obras sociales.

**• Auditoría informática:** En este marco, podemos adelantar el concepto de auditoría informática: es el estudio que se realiza para comprobar la fiabilidad de la herramienta informática y la utilización que se hace de ella en una organización. En forma más amplia se analiza la aplicación de recursos informáticos a los sistemas de información existentes en las empresas, en especial los orientados a automatizar las tareas administrativo-contables, financieras, de gestión, de soporte de decisiones, etc.

**• Auditoría interna**: Es una función de evaluación interna, ejercida por personal perteneciente a los cuadros de la empresa. Actúa como un servicio independiente de la línea jerárquica corriente, por lo que depende directamente de la Dirección de la organización. La auditoría interna mide y evalúa la confiabilidad y eficacia del sistema de control interno de la entidad con miras a lograr su mejoramiento.

**• Auditoría externa**: Es una función de evaluación externa, ejecutada por un ente externo e independiente de la línea jerárquica establecida. Actúa controlando algún aspecto particular de las operaciones o procedimientos establecidos en la organización.

**Modulo #2**

## Fases de una auditoria

## Desarrollo de una [auditoría](https://www.monografias.com/trabajos14/auditoria/auditoria.shtml) de calidad

**Fases de una auditoría de**[**calidad**](https://www.monografias.com/trabajos11/conge/conge.shtml)**:**

**1. Establecer los**[**objetivos**](https://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml)**de la auditoría de calidad:** En la [política](https://www.monografias.com/Politica/index.shtml) de calidad de [la organización](https://www.monografias.com/trabajos6/napro/napro.shtml) hay que incluir las [auditorías](https://www.monografias.com/trabajos14/auditoria/auditoria.shtml) de calidad como instrumento de [gestión](https://www.monografias.com/trabajos15/sistemas-control/sistemas-control.shtml). Con su [empleo](https://www.monografias.com/trabajos36/teoria-empleo/teoria-empleo.shtml) se debe perseguir el [objetivo](https://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml) de [poder](https://www.monografias.com/trabajos35/el-poder/el-poder.shtml) reconocer a [tiempo](https://www.monografias.com/trabajos901/evolucion-historica-concepciones-tiempo/evolucion-historica-concepciones-tiempo.shtml) las desviaciones respecto a las especificaciones establecidas y poder aplicar las medidas apropiadas. Antes de comenzar a realizar una determinada auditoría hay que establecer qué desea lograrse con ella. Los objetivos concretos perseguidos ayudarán a establecer el tipo de auditoría más adecuado, además de su campo y profundidad.

**2. Establecer el campo y profundidad:**Consiste en definir el objeto de la auditoría (si va a ser de [producto](https://www.monografias.com/trabajos12/elproduc/elproduc.shtml), [proceso](https://www.monografias.com/trabajos14/administ-procesos/administ-procesos.shtml#PROCE) o [sistema](https://www.monografias.com/trabajos11/teosis/teosis.shtml)) así como decidir si es interna o externa.

**3. Establecer la frecuencia:** Dado que el objetivo de las auditorías de calidad es la mejora continua, no tendría sentido no realizarlas de modo regular. Pero la periodicidad con que deben hacerse dependen del objeto de la auditoría. Por ejemplo, las auditorías de producto suelen repetirse con mucha frecuencia, incluso puede ser diaria. Sin embargo, la auditoría de certificación según la [ISO 9001](https://www.monografias.com/trabajos6/inso/inso.shtml) se realiza una vez cada tres años con una revisión anual.

**4. Designar a los auditores:**El número y cualificación de los auditores depende del tipo y frecuencia con que se vayan a llevar a cabo. Si se precisa de un equipo auditor, es preciso nombrar a un jefe del equipo que tendrá la [responsabilidad](https://www.monografias.com/trabajos33/responsabilidad/responsabilidad.shtml) del mismo.

**5. Cualificación de los auditores:** Depende del tipo de auditoría hará falta conseguir una especial cualificación para las personas que vayan a llevar a cabo las auditorías. Sobre la formación específica para los auditores, se habla con más en detalle en el apartado "Requisitos de los auditores".

**6. Preparar el**[**plan**](https://www.monografias.com/trabajos7/plane/plane.shtml)**de auditoría:**el plan de la auditoría se emplea como base para proceder de una forma estructurada; en él se especifican todos los aspectos organizativos de las auditorías como por ejemplo las entidades afectadas, orden del [procedimiento](https://www.monografias.com/trabajos13/mapro/mapro.shtml), [distribución](https://www.monografias.com/trabajos11/travent/travent.shtml) de tareas, fechas, definición de responsabilidades.

**7. Recoger**[**información**](https://www.monografias.com/trabajos7/sisinf/sisinf.shtml)**sobre las entidades objeto de la auditoría:**Esta recogida de información es sobre todo de vital importancia cuando se trata de auditorías externas, ya que con ello se logra que el equipo auditor tome contacto con la [filosofía](https://www.monografias.com/trabajos910/en-torno-filosofia/en-torno-filosofia.shtml) y metas de [la empresa](https://www.monografias.com/trabajos11/empre/empre.shtml), sus [productos](https://www.monografias.com/trabajos12/elproduc/elproduc.shtml) y [procesos](https://www.monografias.com/trabajos14/administ-procesos/administ-procesos.shtml#PROCE), la [organización](https://www.monografias.com/trabajos6/napro/napro.shtml) de la [empresa](https://www.monografias.com/trabajos11/empre/empre.shtml), las tareas concretas y funcionamiento del área objeto de la auditoría, y relaciones con [clientes](https://www.monografias.com/trabajos11/sercli/sercli.shtml) externos e internos y con los [proveedores](https://www.monografias.com/trabajos6/lacali/lacali.shtml#influencia).

**8. Clasificación de la**[**documentación**](https://www.monografias.com/trabajos11/ladocont/ladocont.shtml)**:**Se desarrolla en [función](https://www.monografias.com/trabajos7/mafu/mafu.shtml) del tipo de auditoría del que se trate. Hay que comprobar que los [documentos](https://www.monografias.com/trabajos14/comer/comer.shtml) necesarios están disponibles.

**9. Preparar Checklist o lista de chequeo:**Al terminar la fase de [planificación](https://www.monografias.com/trabajos34/planificacion/planificacion.shtml) de la auditoría hay que elaborar las Checklist que se van a emplear en la auditoría. En algunos casos no será necesario preparar dichas Checklist porque ya estarán disponibles de auditorías previas. Las entidades de certificación y otras [organizaciones](https://www.monografias.com/trabajos6/napro/napro.shtml) publican checklist que pueden emplearse como base y [modelo](https://www.monografias.com/trabajos/adolmodin/adolmodin.shtml) por las [empresas](https://www.monografias.com/trabajos11/empre/empre.shtml).

La checklist o lista de chequeo consiste en un listado con los todos los aspectos que se van a revisar en la auditoría.

## Evaluación de los sistemas

**Sistemas de información**El objetivo principal de los sistemas de información es procesar la información que entra a una organización, permitir su análisis, almacenamiento y presentación, proveyendo a las directivas de una organización la información necesaria facilitando la gestión de la organización. Un sistema de información debe estar diseñado para poder cumplir con los objetivos estratégicos de la organización.

**Evaluación de los Sistemas**

Los progresos realizados en un sistema deben ser medidos o evaluados para conocer las deficiencias y problemas que éste presenta. Aunque una evaluación cualitativa puede resultar útil en las etapas iniciales del desarrollo del sistema, medidas cuantitativas bajo unas mismas condiciones resultan de vital importancia para ver el progreso real del sistema y compararlo consigo mismo o con otros. Los números no aportan información si se desconoce de dónde proceden, es decir, qué representan. La evaluación de cualquier tecnología debe ir acompañada de un conjunto de medidas estándar propuestas para tal fin. La disponibilidad de bases de datos y de protocolos o procedimientos para la evaluación de estos sistemas ha sido un componente muy importante, casi fundamental, en el progreso alcanzado en este campo y ha permitido compartir nuevas ideas, e incluso compararlas con otras ya consolidadas. Los progresos en la evaluación de sistemas de comprensión del lenguaje hablado están comenzando. Así vamos a mencionar a continuación diferentes acuerdos alcanzados [PRI90] en la evaluación de sistemas:

## *Conjuntos de Datos de Entrenamiento y de Prueba Independientes.* La importancia de disponer de conjuntos de datos independientes para el entrenamiento/desarrollo y para la evaluación de sistemas de reconocimiento de habla viene siendo aceptada desde hace bastante tiempo por la comunidad científica. Sigue siendo igual de importante para el desarrollo y evaluación de los sistemas de comprensión de habla, aunque para estos últimos nos interesará tener datos de prueba dónde aparezcan el mayor número de fenómenos del habla posibles (son importantes las construcciones gramaticales, los efectos propios del habla espontánea, etc.), para colocar al sistema en el mayor número de situaciones (léxicas, sintácticas y semánticas) posible. Sin embargo, es conveniente resaltar que el proceso de evaluación no deja de ser parte del proceso de entrenamiento, pues en muchos casos los resultados de la misma sirven para depurar o mejorar el comportamiento final del sistema. Por tanto, es importante que exista un conjunto de datos independiente y realista, tan grande como sea posible, con el que se evalúe definitivamente un sistema y con cuyos resultados no se intente seguir desarrollando (mejorando) el sistema.

## *Evaluación del Sistema como Caja Negra.* La evaluación de los componentes de un sistema es una tarea importante durante el desarrollo del mismo, aunque no es especialmente útil para comparar sistemas entre sí, al menos que los sistemas a comparar sean muy similares, lo que no suele ser el caso. La motivación para evaluar los componentes de un sistema es puramente interna, por tanto, no es absolutamente necesario llegar a acuerdos en la comunidad internacional sobre la metodología de evaluación de los mismos. Las medidas de evaluación de los componentes internos de un sistema pueden utilizarse para evaluar las tecnologías empleadas en cada componente como una función de sus parámetros de diseño; por ejemplo, el funcionamiento de un módulo de reconocimiento acústico puede ser evaluado como una función de la perplejidad alofónica y sintáctica, el funcionamiento de un analizador sintáctico (parser) como una función de la calidad (errores) de la secuencia de palabras (frase) de entrada. Además, estas medidas son útiles para evaluar el progreso conseguido, y cómo los cambios en varios componentes afectan al resto de los mismos.

## *Evaluación Cuantitativa vs. Cualitativa.* Una evaluación cualitativa de un sistema (p. ej. lo que parece gustar a los usuarios del sistema) puede ser animador, pero mucho más convincente para aquellos que no pueden observar el sistema son las medidas cuantitativas llevadas a cabo de forma automática. Las medidas deberían ser estandarizadas en la medida de lo posible, y ser reproducibles, para considerarlas significativas. El proceso automatizado evita errores humanos debido a fatiga, falta de atención, malas intenciones, etc. y además, permite capturar muchos más datos que en un caso manual, y sacar conclusiones sobre el funcionamiento de ciertos procesos o hechos que ocurren, con una mayor fiabilidad.

## *Captura de Datos para Evaluación.* Para capturar los datos que necesitamos para evaluar los sistemas de lenguaje hablado, se han desarrollado técnicas y sistemas especiales conocidos como *PNAMBIC* (“Pay No Attention to the Man Behind the Curtain”) o *Mago de Oz*(Wizard of Oz), que implica la existencia de un experto cooperando con un sistema más o menos automático y completo, pero del que no es consciente el usuario, quién piensa que interacciona sólo con un sistema completamente automático. Realmente, el “mago” introduce las peticiones del usuario transcribiendo la frase hablada a texto y enviándosela a la pantalla del usuario, así como interaccionando con un sistema de información (p.e. de gestión de bases de datos), para conseguir las respuesta a la pregunta o petición del usuario y poder mandársela. No se permite que el “mago” realice tareas complejas, sólo puede enviar los datos obtenidos de la base de datos, o frases que indiquen ciertos problemas, indicaciones al usuario, como “su pregunta requiere un proceso que sobrepasa las posibilidades del sistema”. En general, la actuación del “mago” viene condicionada por el hecho de que comprenda o no la pregunta del usuario y sobre su conocimiento sobre las posibilidades de la base de datos. Los datos deben ser analizados a posteriori para determinar si la actuación del “mago” fue o no correcta.

## *Convenios sobre las Transcripciones.* La transcripción de las sesiones, es decir, las frases que se muestran al usuario, representan el habla natural de ese locutor. Para llevar a cabo evaluaciones automáticas, debemos llegar a un cierto acuerdo sobre los convenios a utilizar para representar lo que el usuario ha dicho, y se deben implementar procedimientos que aseguren que estos convenios son realmente utilizados.

## *Respuestas Canónicas y Obtención de Medidas.* Las respuestas canónicas son, en general, las respuestas enviadas al usuario bajo el control del “mago”. Estas respuestas deberán ser modificadas si el “mago” comete un error, o si la respuesta depende del contexto en que fue generada debido a la posible cooperación (diálogo) entre el “mago” y el usuario. La obtención de medidas se lleva a cabo con programas estándar y convenios para las entradas y salidas.

## Investigación preliminar

**Si un proyecto de sistema parece ser viable y tiene suficiente prioridad, se comienza la investigación preliminar. Esta investigación requiere uno o más analistas de sistemas analizando el “system request” para determinar la verdadera naturaleza y alcance del problema y recomendar si es que se debe continuar con el proyecto. El propósito de la investigación preliminar es buscar información suficiente para determinar si se debe continuar con el Ciclo de Vida del Desarrollo del Sistema. La investigación no es una actividad de recolección de datos; no se espera que se definan todos los problemas ni que se propongan todas las posibles soluciones.**

**La investigación preliminar debe cumplir con los siguientes cinco objetivos:**

**1.      *Entender la naturaleza del problema***– Es el primer objetivo de la investigación preliminar. Muchas veces, el problema presentado en el “system request” no es el problema real, sino un síntoma. Al interaccionar con los usuarios, se debe evitar el uso de la palabra problema, ya que puede generar una impresión negativa. Es mejor hablar sobre mejoras que necesita el sistema.

**2.      *Definir el alcance y las restricciones o limitaciones del sistema***– El alcance del proyecto es la extensión del proyecto o del sistema, o sea, hasta dónde se debe llegar. Se debe determinar quién es afectado por el problema o por la solución.  También es importante definir las limitaciones del sistema. Una limitación es una condición, restricción o requisito que el sistema debe satisfacer. La limitación puede tener que ver con el equipo, programas, tiempo, leyes, costos y otros.

**3.      *Identificar los beneficios que se obtendrían si el sistema propuesto es completado*** – Se debe identificar los beneficios tangibles e intangibles que se esperan como resultado del “system request”. Estos beneficios, junto a los estimados de costo, serán usado por la gerencia para decidir si se continúa con el proyecto. Los beneficios tangibles son aquellos que se pueden expresar en términos de dinero. Los beneficios intangibles son difíciles de contabilizar en dólares y centavos, pero son igualmente importantes. Tienen que ver con la satisfacción del empleado, mayor información disponible para tomar decisiones, mejorar la imagen de la compañía y otros aspectos que no se miden en término de dinero.

**4.      *Especificar un estimado de tiempo y costo para las próximas fases de desarrollo***– Se debe presentar un estimado del tiempo que tomará realizar cada uno de las siguientes fases del desarrollo del sistema y del costo que la compañía debe incurrir para completar el sistema. Se debe incluir los costos de desarrollo – costos que ocurren una sola vez – y los costos continuos – costos pagados periódicamente.

**5.      *Presentar un informe a la gerencia describiendo el problema y detallando****si se recomienda continuar con la fase de análisis del sistema* – Debe incluir la evaluación del “system request”, estimado de tiempo y costo-beneficios y las recomendaciones.

**Pasos para realizar la investigación preliminar:**

1.      Obtener la autorización de la gerencia.

2.      Identificar la información necesaria para el proyecto para cumplir con los cinco objetivos de la investigación (ya mencionados).

3.      Realizar las acciones que sean necesarias para conseguir la información, como por ejemplo:

         a.       Analizar el organigrama para conocer la estructura de los departamentos y las personas claves para el sistema.

         b.      Realizar entrevistas a los usuarios, éste es el método principal de obtener información.

         c.       Revisar la documentación actual, verificando con los usuarios si la documentación es correcta y completa.

         d.      Observar la operación actual para identificar fuentes de Input y Output.

         e.       Realizar encuestas, método usado cuando se necesita información de muchas personas.

4.      Analizar la información obtenida, identificando alternativas con sus costos y beneficios y recomendando la acción que se debe tomar.

5.      Presentar los resultados y recomendaciones a la gerencia.

## Personal involucrado en la auditoria en informática.

**Una de las partes más importantes dentro de la planeación de la auditoría en informática es el personal que deberá participar y sus características.**

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

**Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:**

• Técnico en informática.

• Experiencia en el área de informática.

• Experiencia en operación y análisis de sistemas.

• Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

Una vez que se ha hecho la planeación, se puede utilizar el formato donde  figura el organismo, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días/hombre estimado. El control del avance de la auditoría lo podemos llevar mediante el anexo en el cual nos permite cumplir con los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación.

**Modulo #3**

## Recopilación de la información organizacional.

**Recopilación de la información organizacional**

Una vez elaborada la planeación de la auditoría, la cual servirá como plan maestro de los tiempos, costos y prioridades, y como medio de control de la auditoría, se debe empezar la recolección de la información.

**La revisión sistematizada del área se realiza a través de los siguientes elementos:**

**A) Revisión de la estructura orgánica.**\* Jerarquías  - Estructura Orgánica - Funciones – Objetivos

**B) Se deberá revisar la situación de los**[**recursos humanos**](http://www.wikiteka.com/trabajos/planeacion-de-personal/)**.**

**C) Entrevistas con el personal de procesos electrónicos:**

•Jefatura  - Análisis - Programadores - Personal de base de datos - Personal de comunicación y redes.

**D) Se deberá conocer la situación en cuanto a:**

•Presupuesto - Recursos financieros - Recursos materiales - Mobiliario y equipo Costos

**E) Se hará el levantamiento del censo de recursos humanos y análisis de su situación en cuanto a**:

\*Número de personas y distribución por área - Movimientos salariales – Conocimientos - Escolaridad.

**F) Se deberá revisar el grado de cumplimiento de los documentos administrativos.**

\*Organización - Normas y políticas - Planes de trabajos - Controles – Estándares- Procedimientos

PRINCIPALES PLANES QUE SE REQUIEREN DENTRO DE LA ORGANIZACIÓN DE INFORMÁTICA

**Estudio de viabilidad:**Investiga los costos y beneficios de los usos a largo plazo de las computadoras, y recomienda cuándo deben o no usarse.

**Planeación de cambios, modificación y actualización:**Especifica las metas y actividades que se deben realizar para lograr los cambios y modificaciones, su independencia, tiempos, responsables y restricciones, cuando la organización toma la decisión de hacer cambios sustanciales de software, hardware, comunicación o equipos periféricos.

**Actividades típicas de este plan:**

•Especificación completa de hardware, software, comunicación, equipos periféricos.  •Evaluación y selección. •Planeación física y preparación del lugar.

•Pruebas finales de aceptación.

**Plan Maestro:**Define los objetivos a largo plazo y las metas necesarias para lograrlo. Una de las principales obligaciones del área de gerencia en informática es la construcción de un plan maestro.

**Puede comprender cuatro sub-planes:**

A) El plan estratégico de organización.

B) El plan estratégico de sistemas de información.

C) El plan de requerimientos.

D) El plan de aplicaciones de sistemas de información.

**Plan de Proyectos:**Consiste en el plan básico para desarrollar determinado sistema y para asegurarse que el proyecto es consistente con las metas y objetivos de la organización y con aquellos señalados en el plan maestro.

**Actividades básicas que debe contener:**

A) Identificar las tareas a realizar

B) Identificar las relaciones entre tareas

C) Determinar los recursos necesarios para cada tarea.

D) Determinar la secuencia de actividades.

**Plan de Seguridad:**seguros, contingencias y recuperación en caso de siniestro.

**Razones por las que puede estar expuesta una instalación informática a un desastre:**

 Huracanes, fuego, inundaciones, terremotos, sabotaje, fraude, problemas de equipo.

3.2 [EVALUACIÓN DE LOS RECURSOS HUMANOS](https://itla.edu.do/virtual/cv/mod/page/view.php?id=71483)

**El desarrollo del personal implica:**

•Establecer promociones y oportunidades de desarrollo.

•Educación y capacitación. Estas actividades mantienen la moral y las habilidades de los empleados en un nivel adecuado para cumplir con los objetivos y metas encomendadas.

3.3 ENTREVISTAS CON EL PERSONAL DE INFORMÁTICA

**La entrevista nos servirá para determinar:**

•Grado de cumplimiento de la estructura organizacional administrativa.

•Grado de cumplimiento de las políticas y los procedimientos administrativos.

•Satisfacción e insatisfacción.

•Capacitación.  •Observaciones generales.

**Presupuestos**: Se obtendrá información presupuestal y financiera del departamento, así como del número de equipos y características para hacer un análisis de su situación desde un punto de vista económico.

**Entre esta información se encuentra:**

•Costos del departamento, desglosado por áreas y controles.

•Presupuesto del departamento, desglosado por áreas.

•Características de los equipos, número de ellos y contratos.

**Recursos Financieros**: Para abordar el tema de los recursos financieros, se sugiere formular las siguientes preguntas.

**Recursos Materiales:**con la finalidad de poder obtener información, se recomienda la elaboración de las preguntas, tomando en consideración los siguientes rubros:

## Evaluación de la estructura orgánica

## EVALUACION DE LA ESTRUCTURA ORGANICA

* Organigrama con jerarquías
* Funciones
* Objetivos y políticas
* Análisis, descripción y evaluación de puestos
* Manual de procedimientos
* Manual de normas
* Objetivos de la dirección
* Políticas y normas de la dirección

##### ESTRUCTURA ORGANICA

Los auditores deben contar con:  
  
Independencia funcional.  
Libertad de acción.  
Facultad para la toma de decisiones  
Negociación con los niveles gerenciales  
Involucramiento en proyectos de alto impacto en el negocio

**FUNCIONES**

Evaluación, verificación e implantación oportuna de los controles y procedimientos que se requieren para el aseguramiento del buen uso y aprovechamiento de la función de informática.  
Aseguramiento permanente de la existencia y cumplimiento de los controles y procedimientos que regulan las actividades y utilización de los recursos de informática de acuerdo con las políticas de la organización.

**Evaluar las áreas de riesgo de la función de informática y justificar su evaluación con la alta dirección del negocio.**

Elaborar un plan de auditoría en informática en los plazos determinados por el responsable de la función.  
Obtener la aprobación formal de los proyectos del plan y difundidos entre los involucrados para su compromiso.  
Administrar o ejecutar de manera eficiente los proyectos contemplados en el plan de la auditoría en informática.

**OBJETIVOS**

· Asegurar que la función de auditoría cubra y proteja los mayores riesgos y exposiciones existentes en el medio informático en el negocio.

·Asegurar que los recursos de informática (hardware, software, telecomunicaciones, servicios, personal, etc.) sean orientados al logro de los objetivos y las estrategias de las organizaciones.

· Asegurar la formulación, elaboración y difusión formal de las políticas, controles y procedimientos inherentes a la auditoría en informática que garanticen el uso y aprovechamiento óptimo y eficiente de cada uno de los recursos de informática en el negocio.

·Asegurar el cumplimiento formal de las políticas, controles y procedimientos definidos en cada proyecto de auditoría en informática mediante un seguimiento oportuno.

**ANÁLISIS DE ORGANIZACIONES**

Agrupar funciones similares y relacionarlas entre sí.  
Agrupar funciones que sean compatibles.  
Localizar la actividad cerca de la función a la que sirva.   
Localizar la actividad cerca o dentro de la función mejor preparada para realizarla.  
No asignar la misma función a dos personas o entidades diferentes.  
Separar las funciones de control y aquellas que serán objeto del mismo.  
Ningún puesto debe tener dos o más líneas de dependencia jerárquica.  
El tramo de control no debe ser exagerado, ni muy numerosos los niveles jerárquicos.﻿

## Evaluación de los recursos humanos

## Patrones de evaluación y control en recursos humanos.

La auditoria de recursos humanos puede definirse como el análisis de las políticas y prácticas de personal de una empresa y la evaluación de su funcionamiento actual, seguida de sugerencias para mejorar. El propósito principal de la auditoria de recursos humanos es mostrar como está funcionado el    programa, localizando prácticas y condiciones que son perjudiciales par la empresa o que no están justificando su costo, o prácticas y condiciones que deben incrementarse.

La auditoria es un sistema de revisión y control para informar a la administración sobre la eficiencia y la eficacia del programa que lleva a cabo.

El sistema de administración de recursos humanos necesita patrones capaces de permitir una continua evaluación y control sistemático de su funcionamiento.

Patrón en in criterio o un modelo que se establece previamente para permitir la comparación con los resultados o con los objetivos alcanzados. Por medio de la comparación con el patrón pueden evaluarse los resultados obtenidos y verificar que ajustes y correcciones deben realizarse en el sistema, con el fin de que funcione mejor.

**Se utilizan varios patrones, esto pueden ser:**

1) Patrones de cantidad: son los que se expresan en números o en cantidades, como número de empleados, porcentaje de rotación de empleados, numero de admisiones, índice de accidentes, etc.

2) Patrones de calidad: son los que se relacionan con aspectos no cuantificables, como métodos de selección de empleados, resultados de entrenamiento, funcionamiento de la evaluación del desempeño. Etc.,

3) Patones de tiempo: consisten en la rapidez con que se integra e personal recién admitido, la permanencia promedio del empleado en la empresa, el tiempo de procesamiento de la requisiciones de personal, etc.

4) Patones de costo: son los costos, directos e indirectos, de la rotación de personal, de los accidentes en el trabajo, de los beneficios sociales, de las obligaciones sociales, de la relación costo-beneficio del entrenamiento.

**Los patrones permiten la evaluación y el control por medio de la comparación con:**

1) Resultados finales: cuando la comparación entra el patrón y la variable se hace después de realizada la operación. La medición se realiza en términos de algo rápido y acabado, en el fin de la línea, lo cual presenta el inconveniente de mostrar los aciertos y las fallas de una operación ya terminada, una especie de partida de defunción de algo que ya sucedió.

2) Desempeño: cuando la comparación entre el patrón y la variable se hace simultáneamente con la operación, es decir, cuando la comparación acompaña ala ejecución de la operación. La medición es concomitante con el procesamiento de operación. A pesar de que se realiza en forma simultanea, lo que quiere decir es que es actual, la medición se realiza sobre una operación en proceso y no terminada aún.

La comparación es la función de verificar el grado de concordancia entra una variable u su patrón. La ARH se encarga de planear, organizar y controlar las actividades relacionadas con la vida del personal en la empresa. Parte de la ejecución de estas actividades al realizan los organismos de recursos humanos, en tantos que alguna parte de ella la realizan diversos organismos de línea. De este modo las actividades de recursos humanos planeadas y organizadas con antelación muestran durante su ejecución y control algunas dificultades y distorsiones que requieren ser diagnosticadas y superadas, con el fin de evitar mayores problemas. La rapidez con que esto se haga depende de una revisión y auditoria permanentes, capaces de suministrar una adecuada retroalimentación para que los aspectos positivos puedan mejorarse y los negativos, corregirse y ajustarse.

La función de auditoria no es solo señalar las fallas y los problemas, sino también presentar sugerencias y soluciones. En este sentido, el papel de la auditoria de recursos humanos es fundamentalmente educativo.

**Modulo #4**

**Modulo #5**

## Introducción a la seguridad

La **seguridad informática** es la [disciplina](https://www.monografias.com/trabajos14/disciplina/disciplina.shtml) que se Ocupa de diseñar las normas, procedimientos,[métodos](https://www.monografias.com/trabajos11/metods/metods.shtml) y [técnicas](https://www.monografias.com/trabajos6/juti/juti.shtml), orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

consiste en asegurar que los recursos del [sistema](https://www.monografias.com/trabajos11/teosis/teosis.shtml) de información (material informático o [programas](https://www.monografias.com/Computacion/Programacion/)) de una [organización](https://www.monografias.com/trabajos6/napro/napro.shtml) sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los [límites](https://www.monografias.com/trabajos6/lide/lide.shtml) de su autorización.

**Principios de Seguridad Informática:**

Para lograr sus [objetivos](https://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml) la seguridad informática se fundamenta en tres [principios](https://www.monografias.com/trabajos6/etic/etic.shtml), que debe cumplir todo sistema informático:

**Confidencialidad:** Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en [sistemas distribuidos](https://www.monografias.com/trabajos16/sistemas-distribuidos/sistemas-distribuidos.shtml), es decir, aquellos en los que los usuarios , computadores y datos residen en localidades diferentes , pero están [física](https://www.monografias.com/Fisica/index.shtml) y lógicamente interconectados.

**Integridad:** Se refiere a la validez y consistencia de los elementos de información almacenados y [procesador](https://www.monografias.com/trabajos5/sisope/sisope.shtml) en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los [procesos](https://www.monografias.com/trabajos14/administ-procesos/administ-procesos.shtml#PROCE) de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios , computadores y procesos comparten la misma información.

**Disponibilidad:** Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar [servicio](https://www.monografias.com/trabajos14/verific-servicios/verific-servicios.shtml) permanente.

## Tipos de seguridad informática.

La **seguridad informática** se rige por diferentes aspectos y es crucial conocer los diferentes tipos para evitar ataques informáticos que pongan en riesgo los datos o el prestigio de las empresas. Cada día más, Internet es el canal por el cual se introducen virus en las organizaciones que pueden suponer costes millonarios. Para evitar este tipo de ataques lo primero que hay que hacer es conocer los diferentes tipos de seguridad informática que hay. Veámoslos.

**Seguridad informática de red**

¿Te suenan los virus, los gusanos o los hackers? ¿El robo de identidad o el software espía? Todos ellos son fallos en la seguridad informática de red y pueden combatirse con antivirus y antispyware, cortafuegos o las redes privadas virtuales o VPN.

La [seguridad de red](https://plataformavirtual.itla.edu.do/mod/page/view.php?id=17630) pretende proteger a la red informática de todas las amenazas que pueden entrar o difundirse en una red de dispositivos. Al mismo tiempo que debe minimizar el mantenimiento de la misma.

Las estrategias de protección más comunes que utiliza el [administrador de sistemas informáticos en red](http://fp.uoc.edu/estudios-fp/administracion-sistemas-informaticos-red/) son utilizar diferentes niveles de seguridad, para que trabajando al mismo tiempo siempre haya alguna funcionando. Incluyen la seguridad de hardware y software. Un buen sistema de [seguridad de red](https://plataformavirtual.itla.edu.do/mod/page/view.php?id=17630) minimiza el mantenimiento de la misma y **mejora la seguridad a todos los niveles**.

**Seguridad informática de hardware**

El cortafuegos o los firewalls de hardware y los llamados [servidores proxy](http://fp.uoc.edu/blog/servidor-proxy-informatica/) son elementos que controlan el tráfico de red y forman parte de la seguridad informática de hardware. Son los encargados de ofrecer una seguridad más potente y segura y protegen al mismo tiempo otros sistemas como las redes, por ejemplo. Los HSM, o módulos de seguridad de hardware, protegen el cifrado o la autenticación para diferentes sistemas mediante claves criptográficas.

Pero la seguridad informática de hardware va más allá, y también se ocupa de la **seguridad de los equipos informáticos**. Por ejemplo, conocer si existen errores de seguridad desde su configuración o el código que ejecuta el hardware, así como los dispositivos de entrada y salida de datos que tiene. Todo influye en la seguridad de hardware y debe ser tenido en cuenta para evitar intrusos no deseados.

**Seguridad informática de software**

La seguridad de software o la construcción de un software seguro es algo relativamente nuevo. Los desarrolladores trabajan para construir software que sean cada vez más seguros desde el momento uno.

El objetivo es **proteger al software de errores frecuentes relacionados con la seguridad** como errores de implementación, defectos de diseño, desbordamiento de buffer…Estos defectos de software pueden servir de entrada para virus o hackers. Por ello, trabajar en un software seguro desde la creación del mismo es crucial para la seguridad del mismo.

## Seguridad lógica y confidencial

**Seguridad lógica y confidencial**

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de una computadora, así como de controlar el mal uso de la información.

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación.

Identifica individualmente a cada usuario y sus actividades en el sistema, y restringe el acceso a datos, a los programas de uso general, de uso especifico, de las redes y terminales.

La falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

Cambio de los datos antes o cuando se le da entrada a la computadora.

Copias de programas y /o información.

Código oculto en un programa

Entrada de virus

**La seguridad lógica**puede evitar una afectación de perdida de registros, y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden al usuario una contraseña antes de permitirle el acceso a información confidencial. Sin embargo, los paquetes de control de acceso basados en componentes pueden ser eludidos por delincuentes sofisticados en computación, por lo que no es conveniente depender de esos paquetes por si solos para tener una seguridad adecuada.

El sistema integral de seguridad debe comprender:

Elementos administrativos.

Definición de una política de seguridad.

Organización y división de responsabilidades.

Seguridad lógica

Tipos de usuarios:

Propietario. Es el dueño de la información, el responsable de ésta, y puede realizar cualquier función. Es responsable de la seguridad lógica, en cuanto puede realizar cualquier acción y puede autorizar a otros usuarios de acuerdo con el nivel que desee darles.

Administrador. Sólo puede actualizar o modificar el software con la debida autorización, pero no puede modificar la información. Es responsable de la seguridad lógica y de la integridad de los datos.

Usuario principal. Está autorizado por el propietario para hacer modificaciones, cambios, lectura y utilización de los datos, pero no puede dar autorización para que otros usuarios entren.

Usuario de explotación. Puede leer la información y utilizarla para explotación de la misma, principalmente para hacer reportes de diferente índole.

Usuario de auditoría. Puede utilizar la información y rastrearla dentro del sistema para fines de auditoria.

Los usuarios pueden ser múltiples, y pueden ser el resultado de la combinación de los antes señalados. Se recomienda que exista sólo un usuario propietario, y que el administrador sea una persona designada por la gerencia de informática.

Para conservar la integridad, confidencialidad y disponibilidad de los sistemas de información se debe tomar en cuenta lo siguiente:

La integridad es la responsabilidad de los individuos autorizados para modificar datos o programas o de los usuarios a los que se otorgan acceso a aplicaciones de sistema o funciones fuera de sus responsabilidades normales de trabajo.

La confidencialidad es responsabilidad de los individuos autorizados para consultar o para bajar archivos importantes para microcomputadoras.

La responsabilidad es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema operativo, al sistema manejador de base de datos, al monitoreo de teleproceso o al software de telecomunicaciones.

**La seguridad lógica abarca las siguientes áreas:**

Rutas de acceso.

Claves de acceso.

Software de control de acceso.

Encriptamiento.

Rutas de acceso

Cada uno de los sistemas de información tiene una ruta de acceso, la cual puede definirse como la trayectoria seguida en el momento de acceso al sistema.

Los tipos de restricciones de acceso son:

Sólo lectura

Sólo consulta

Lectura y consulta

Lectura escritura para crear, actualizar, borrar, ejecutar o copiar

El esquema de las rutas de acceso sirve para identificar todos los puntos de control que pueden ser usados para proteger los datos en el sistema. El autor debe conocer las rutas de acceso para el evaluación de los puntos de control apropiados.

Claves de acceso

Un área importante en la seguridad lógica de las claves de acceso de los usuarios. Existen diferentes métodos de identificación para el usuario:

Un password, código o llaves de acceso. Las claves de acceso pueden ser usadas para controlar al acceso a la computadora, a sus recursos, así como definir nivel de acceso o funciones específicas.

Las llaves de acceso deben tener las siguientes características:

- El sistema debe verificar primero que el usuario tenga una llave de acceso válida.

- La llave de acceso debe ser de una longitud adecuada para ser un secreto.

- La llave de acceso no debe ser desplegada cuando es tecleada.

- Las llaves de acceso deben ser encintadas.

- Las llaves de acceso deben de prohibir el uso de nombres, palabras o caracteres difíciles de retener, además el password no debe ser cambiado por un valor pasado. Se recomienda la combinación de caracteres alfabéticos y numéricos.

Una credencial con banda magnética. La banda magnética de las credenciales es frecuentemente usada para la entrada del sistema. Esta credencial es como una bancaria, pero se recomienda que tenga fotografía y firma.

Algo especifico del usuario. Es un método para identificación del usuario, que es implantado con tecnología biométrica (características propias). Algunos de los dispositivos biométricos son:

- Las huellas dactilares.

- La retina

- La geometría de la mano.

- La firma.

- La voz.

Software de control de acceso

El software de control de acceso, tiene las siguientes funciones:

Definición de usuarios.

Definición de las funciones del usuario después de accesar el sistema.

Jobs

Establecimiento de auditoría a través del uso del sistema.

La mayor ventaja del software de seguridad es la capacidad para proteger los recursos de acceso no autorizados, incluyendo los siguientes:

Procesos en espera de modificación por un programa de aplicación.

Accesos por editores en línea.

Accesos por utilerías de software.

Accesos a archivos de las bases de datos, a través de un manejador de base de datos.

Acceso de terminales o estaciones no autorizadas.

Estos paquetes pueden restringir el acceso a los recursos, reduciendo así el riesgo de accesos no autorizados.

Otra característica de estos paquetes es que se pueden detectar las violaciones de seguridad, tomando las siguientes medidas:

Terminaciones de procesos.

Forzar a las terminales a apagarse.

Desplegar mensajes de error.

Escribir los riesgos para la auditoría.

Otros tipos de software de control de acceso

Algunos tipos de software son diseñados con características que pueden ser usadas para proveerles seguridad. Sin embargo, es preferible usar un software de control de acceso para asegurar el ambiente total y completar las características de seguridad con u software especifico.

a) Sistemas operativos. Se trata de una serie de programas que se encuentran dentro de los sistemas operativos, los cuales manejan los recursos de las computadoras y sirven como interfase entre software de aplicaciones y el hardware. Estos programas proporcionan seguridad ya que, internamente, dentro de los sistemas operativos manejan y controlan la ejecución de programas de aplicación y proveen los servicios que estos programas requieren, dependiendo del usuario y del sistema que esté trabajando.

b) Software manejador de base de datos. Es un software cuya finalidad es la de controlar, organizar y manipular los datos. Provee múltiples caminos para accesar los datos en una base de datos. Maneja la integridad de datos entre operaciones, funciones y tareas de la organización.

c) Software de consolas o terminales maestras. El software de consolas o terminales maestras puede ser definido como varios programas del sistema operativo que proveen soporte y servicio para que las terminales en línea acceden a los programas en aplicación.

d) Software de librerías. El software de librerías consta de datos y programas específicos escritos para ejecutar una función de la organización. Los programas en aplicación pueden ser guardados en archivos en el sistema, y el acceso a estos programas puede ser controlado por medio del software usado para controlar el acceso a estos archivos.

e) Software de utilerías. Existen dos tipos de utilerías. El primero es usado en los sistemas de desarrollo para proveer productividad. El desarrollo de programas y los editores en línea son los ejemplos de este tipo de software. El segundo es usado para asistir en el manejo de operaciones de la computadora. Monitoreos, calendarios de trabajo, sistema manejador de disco y cinta son ejemplos de este de software.

## POLÍTICAS DE SEGURIDAD INFORMÁTICA

**ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA.**

 Como una política de seguridad debe orientar las decisiones que se tomen en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considere importante. Las políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

· Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

 · Objetivos de la política y descripción clara de los elementos involucrados en su definición. Responsabilidades por cada uno de los servicios y recursos informáticos aplicados a todos los niveles de la organización.

 · Requerimientos mínimos para la configuración de la seguridad de los sistemas que abarca el alcance de la política.

**PLAN DE TRABAJO PARA ESTABLECER POLÍTICAS DE SEGURIDAD.**

• Agendar reunión con los coordinadores o jefes de departamentos.

• Destacar en que nos afecta a todos la perdida de información.

 • Asumir el compromiso de las buenas prácticas en la manipulación de datos de la red informática.

• Establecer en la reunión las propuestas para definir las medidas de seguridad aplicadas a los coordinadores y personas a su cargo.

• Medidas de seguridad:

• Acceso a Internet

• Respaldo de la información

**Personal de sistemas:**

 a. El control de los equipos tecnológicos deberá estar bajo la responsabilidad del área de TIC´S, así como la asignación de usuarios y la ubicación física.

 b. En el área de TIC´S se deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

 c. El área de TIC´S será la encargada de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

 d. Las licencias de uso de software estarán bajo custodia del área de TIC´S. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

e. El área de TIC´S es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

 f. Todas las publicaciones que se realicen en el sitio WEB de la entidad, deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

**DEFINICIONES**

 Para los efectos del presente manual, se adoptarán las siguientes definiciones:

**Acceso físico**: La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.

**Acceso lógico:** Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.

**Activos de Información:** Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

**Cableado estructurado:** Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.

**Cifrado de datos:** Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.

**Configuración Lógica:** conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

**Copia de respaldo o backup:** Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

**Contenido**: Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, vídeo, diseños, software, animaciones, etc.

**Contraseñas:** Clave cristalográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

**Correo electrónico institucional:**Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos, que se encuentra alojado en un hosting de propiedad de la Entidad.

**Cuenta de acceso:** Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

**Dispositivos/Periféricos:** Aparatos auxiliares e independientes conectados al computador o la red.

**Dominio:** Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

**Modulo #6**

La forma de proteger un sistema **contra** un ataque de **virus** es utilizando un programa de **protección**. Los programas antivirus están diseñados para operar permanentemente, por lo que el usuario normalmente no está consciente de que al menos surja un problema.

## Que es un Virus de Computadora?

Los Virus Informáticos son sencillamente programas maliciosos (malwares) que “infectan” a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo “víctima” (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección. Su nombre lo adoptan de la similitud que tienen con los virus biológicos que afectan a los humanos, donde los antibióticos en este caso serían los programas Antivirus.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad, son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

## ¿Cuál es el funcionamiento básico de un virus?

1. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario.

2. El código del virus queda residente (alojado) en la memoria RAM del computador, aun cuando el programa que lo contenía haya terminado de ejecutarse.

3. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables (.exe., .com, .scr, etc) que sean llamados para su ejecución.

4. Finalmente se añade el código del virus al programa.

## ¿Cómo eliminar un virus informático?

Si sospecha haber sido víctima de un virus o malwares en su equipo, puede informar al área de Tecnología y Sistemas de Información y ellos le orientaran sobre la manera cómo puede verificar si existen infecciones, cuales son y el mecanismo para eliminarlos. Si la sospecha es sobre el equipo de cómputo de su casa le recomendamos tener instalado un buen antivirus de preferencia con licencia; pues los antivirus gratuitos muchas veces vienen con otras intenciones menos la de protegerlo.

**Modulo #7**

Ciberseguridad en las empresas (1/4)

La ciberseguridad implica que **las empresas deban estar preparadas** para cualquier ataque que reciba, tenga planes de cómo reaccionar y qué acción tomar para que “no les pille por sorpresa”. Esta seguridad debe involucrar a base de datos, metadatos, archivos, hardwares, computadoras y todo aquello que sea susceptible de correr riesgo por pérdida de información o robo.

Las amenazas provocadas por los ataques **pueden venir provocadas por**:

* “**Hackers**” que, bajo servicio o sin él, tratan de buscar cierta información de los usuarios de una página web porque los requiere o busca una retribución por su venta.
* Programas maliciosos o perjudiciales. Suelen tener la misma función, pero rescatan la información a través de un programa informático que se instala en las bases de datos de los hardwares de las empresas.
* **Errores de programación**. Un fallo puede provocar que se desequilibre algunos datos o acciones en una web.
* Fallos electrónicos, siniestros o catástrofes que, por razones externas, perjudican la información de los usuarios.

Ciberseguridad en las empresas (1/4)

La ciberseguridad implica que **las empresas deban estar preparadas** para cualquier ataque que reciba, tenga planes de cómo reaccionar y qué acción tomar para que “no les pille por sorpresa”. Esta seguridad debe involucrar a base de datos, metadatos, archivos, hardwares, computadoras y todo aquello que sea susceptible de correr riesgo por pérdida de información o robo.

Las amenazas provocadas por los ataques **pueden venir provocadas por**:

* “**Hackers**” que, bajo servicio o sin él, tratan de buscar cierta información de los usuarios de una página web porque los requiere o busca una retribución por su venta.
* Programas maliciosos o perjudiciales. Suelen tener la misma función, pero rescatan la información a través de un programa informático que se instala en las bases de datos de los hardwares de las empresas.
* **Errores de programación**. Un fallo puede provocar que se desequilibre algunos datos o acciones en una web.
* Fallos electrónicos, siniestros o catástrofes que, por razones externas, perjudican la información de los usuarios.

**Modulo #8**

## Prevención

Dentro del enfoque global que se ha mencionado anteriormente, la prevención ha de ser abordada por el usuario y la empresa desde varias perspectivas. Por un lado, es importante estar informado de la evolución de las amenazas, de las posibles estafas y de qué soluciones existen contra ellas. Por ello, la formación constante es un elemento esencial en la prevención. Es recomendable adquirir una serie de conocimientos sobre seguridad que son necesarios poner en marcha con una actitud de prudencia y utilizar con la mayor eficacia y eficiencia posibles todos los medios a nuestro alcance. Por otro lado, es necesario conocer el funcionamiento de las herramientas o productos de seguridad, sus características y su forma de actuar para sacarle el mayor partido posible y conseguir la protección más efectiva. También es necesaria la protección física de las instalaciones para garantizar que nadie sin autorización pueda manipular los terminales, los accesos a la red o conectar dispositivos no autorizados3 . Como puede verse en el gráfico anterior, la prevención tiene tres procesos críticos: control de accesos y gestión de identidades, [prevención de fugas de datos](https://plataformavirtual.itla.edu.do/mod/page/view.php?id=17629) y seguridad de la red. Brevemente se describirán cada uno de estos procesos.

## Ciberdefensa-Ciberseguridad Riesgos y Amenazas

**Diferencias en las definiciones**

• Ciberguerra: Conflicto en el Ciberespacio.

• Ciberdefensa: Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y           negarlo al enemigo o a otras inteligencias en oposición.

 • Ciberseguridad: Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros

. • Cibercrimen: Acciòn criminal en el ciberespacio.

 • Ciberterrorismo: Acción terrorista en el ciberespacio.

**Definición de Ciberdefensa Ciberdefensa** es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informaticos y teleinformaticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.

**Caracterización de las Amenazas Amenazas por el origen**

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute(CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas: **Amenazas externas Amenazas Internas.**

**Amenazas internas**: Generalmente estas amenazas pueden ser más serias que las externas Los usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos. Los sistemas de [prevención](https://plataformavirtual.itla.edu.do/mod/page/view.php?id=17626) de intrusos o IPS, y firewalls son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno.

**Amenazas Externas** • Se originan fuera de la red local.  
• Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla.  
• La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.  
• Para clasificarlo como externo debe ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red: rosetas, switches o Hubs accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

**Amenazas por el efecto** El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en: Robo de información. Destrucción de información. Anulación del funcionamiento de los sistemas o efectos que tiendan a ello. Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc. Robo de dinero, estafas,..

**Amenazas por el medio utilizado** Se pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque Aquí se clasifican acciones como • Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

• Worms

• BOTs

• Adware

• Cookies

• Phishing.

• Ingeniería social.

 • Denegación de servicio.

• Spoofing : de DNS, de IP, de DHCP , etc.

## Control de accesos y gestión de identidades

Dos procesos importantes para la ciberseguridad en una empresa son el control de accesos y la gestión de identidades. Estos dos conceptos, aunque diferentes, se dan la mano el uno con el otro para desarrollar sus funciones, que son básicamente controlar los accesos a los sistemas, tanto físicos como informáticos. La gestión de identidades es un proceso relevante a la hora de prevenir ataques, ya que consiste en asignar a una identidad concreta un rol o una serie de permisos o credenciales para acceder a ciertos sistemas o recursos, especialmente a las aplicaciones críticas y zonas restringidas. En todas las organizaciones existen zonas donde se almacena información confidencial o de suma importancia. Por eso es recomendable implementar una serie de políticas de control sobre quiénes podrán acceder a los activos críticos para minimizar el riesgo, y esto se realiza mediante las herramientas que nos ofrecen el control de accesos y la gestión de identidades.

Para la correcta gestión de los controles y las identidades, es necesario llevar a cabo acciones de inventariado y catalogado y establecer los criterios de acceso. Estos criterios de acceso deben regirse por la máxima de que una persona debe tener disponibilidad de las aplicaciones críticas o zona restringida solo cuando el ejercicio de su trabajo lo requiera4 . En numerosas ocasiones, la gestión de identidades, y por tanto el control de accesos, es llevada a cabo mediante procedimientos manuales. Sin embargo, los expertos en el ámbito de la gestión de identidades advierten de que uno de los principales problemas que acarrean los procesos manuales en este ámbito es su ineficiencia5 . Adicionalmente a este problema los principales retos que la gestión de identidades plantea a las organizaciones son la previsión, la gestión de cuentas huérfanas y la adaptación a la normativa vigente. El primer gran reto es poseer en las organizaciones un sistema organizado de previsión, de modo que cada persona tenga sus credenciales en tiempo y forma. Adoptando sistemas de previsión se evitarían muchos problemas de seguridad, especialmente cuando existen cambios de roles dentro de una organización; como que una persona con el rol equivocado acceda a funciones o zonas para las que no está autorizada. Por eso es necesario ser ágil a la hora de realizar estos cambios y hay que tener un protocolo eficaz para asignar las claves y los usuarios que cada rol requiera. El segundo reto de la gestión de identidades es lo que se da en llamar las cuentas huérfanas. En muchos casos, una persona deja una organización y hay que gestionar que la cuenta de ese trabajador quede totalmente anulada. El problema es que en numerosas ocasiones el trabajador es dado de baja en aquellos aspectos que se encuentran reglados en el protocolo interno de la empresa, pero puede que existan aspectos ligados a la seguridad que estén siendo gestionados por un tercero; por ejemplo, el control de los tornos de entrada en un edificio, y que no están contemplados en el protocolo interno, por lo que su gestión es más lenta. Por último, el gran reto en cuanto a la gestión de identidades es el de las normativas de seguridad aplicables.

## Prevención de fugas de datos

La fuga de datos es uno de los principales problemas de seguridad y uno de los retos a los que se enfrentan usuarios, empresas y organizaciones. Ejemplos de esta amenaza los encontramos en la fuga de datos que sufrió eBay y que pudo afectar a un total de 128 millones de usuarios , o la que experimentó el Gobierno de Estados Unidos en junio de 2015, que se estima que afectó a 4 millones de empleados de la Administración federal10. Los incidentes de este tipo son complejos debido a la diversidad y a las graves consecuencias que pueden acarrear. Muchas de las fugas de datos tienen un componente humano y organizativo. Para afrontar este reto, empresas y organizaciones cuentan con una amplia oferta de herramientas y medidas que de una forma eficaz ayudan a minimizar y prevenir la temida fuga de datos. Estas medidas y herramientas se pueden agrupar en tres grupos diferentes. En el primer grupo se englobarían todas las medidas técnicas; en el segundo, las de carácter organizativo, y en el tercero, las medidas legales. Entre las medidas técnicas se hallan: control de acceso e identidad, soluciones antimalware y antifraude, seguridad perimetral y protección de las comunicaciones, control de contenidos y control de tráfico, copias de seguridad, control de acceso a los recursos, actualizaciones de seguridad y parches y, por último, otras medidas de seguridad derivadas del cumplimiento de legislación, gestión de eventos e inteligencia de seguridad.

## Seguridad de red

La seguridad de red hace referencia a todas aquellas acciones encaminadas y diseñadas para proteger una red de sistemas u ordenadores y recursos de acceso de red. Esencialmente estas actividades se encaminan a proteger el uso de las redes, el grado de fiabilidad, la integridad y la seguridad de las redes y de los datos que se transmiten a través de ellas. Una seguridad efectiva de la red se dirige a la protección de una amplia variedad de amenazas y a evitar su entrada en la red o que se expanda por ella, por lo que es un elemento esencial de una correcta política de [prevención](https://plataformavirtual.itla.edu.do/mod/page/view.php?id=17626) en materia de ciberseguridad.

## Detección

En el campo de la ciberseguridad, otro proceso destacado es la detección de incidencias. La detección puede ocurrir mientras se está produciendo el ataque o pasado un tiempo desde el mismo. La detección de un ataque o amenaza en tiempo real suele producirse gracias a la detección del malware por parte de un antivirus. Si por el contrario se da la segunda circunstancia, los problemas son mayores porque los hackers han podido actuar libremente durante un largo período de tiempo. Se estima que el período medio entre el momento en que se produce una brecha de seguridad y su detección fue en 2014 de 205 días. Afortunadamente, se puede afirmar que las herramientas de ciberseguridad existentes en la actualidad realizan de forma eficaz la detección de patrones de ataque conocidos si se encuentran instaladas correctamente. El problema lo encontramos con los ataques con patrones desconocidos y cuando la detección no se ha producido en tiempo real y ha pasado un período largo hasta que finalmente se produce la detección.

## Sistemas de recuperación

Los sistemas de recuperación son una función que permite al usuario devolver el estado de su equipo y las aplicaciones al punto de partida anterior a que se haya producido un problema y así solucionarlo.

Uno de los sistemas operativos pioneros en incluir esta función fue Microsoft en sus sistemas operativos de Windows. En la primera versión que se incluyó fue en Windows ME y, a partir de entonces, se ha introducido en todas las versiones del sistema operativo que le han seguido. En las primeras versiones, este sistema se basaba en un filtro de archivos que observaba los cambios que sufrían las diferentes extensiones, copiando los archivos antes de ser sobrescritos. Posteriormente, en las versiones a partir de Windows Vista, utiliza un Shadow System de restaurado que permite cambios de bloque en archivos ubicados en cualquier directorio de forma que reciben apoyo y son monitorizados con independencia de su ubicación. También permite realizar recuperaciones si la versión de Windows instalada no consigue limpiar el sistema. Otro sistema operativo que ha introducido esta función ha sido Android. El recovery se basa en una partición con propiedades de arranque. Se ejecuta separado y paralelo al sistema operativo principal de Android. Las particiones en que se dividen son boot/kernel y root/ system. Estas particiones se encuentran separadas del sistema de recuperación que contiene su propio kernel de Linux.

**Modulo # 9**

## ¿Qué son las NORTIC?

Las NORTIC  son normas de tecnologías de la información y comunicación, creadas por el Departamento de estandarización, Normativa y Auditoria Técnica (ENAT), en el 2013, las cuales tienen como objetico principal el establecimiento de estándares generales, relacionados con aspectos tecnológicos.

**Alcance**

Las NORTIC fueron concebidas con el fin de normalizar, estandarizar, y tener una herramienta de auditoría para el efectivo uso e implementación de las TIC en el Gobierno Dominicano, con el fin de llegar a la completa homogeneidad entre los organismos gubernamentales.

**Categorización**

Se han definido 5 categorías o tipos de normas, según el alcance de estas, para ser difundidas e implementadas en toda la administración pública, como se presenta a continuación:

##### Categoría A (normas universales)**, para las normas que aplican para todos los organismos gubernamentales.**

##### Categoría B (normas para los departamentos de TIC)**, para las normas que aplican específicamente para los distintos viceministerios, direcciones, departamentos, divisiones o áreas de Tecnologías de la Información (TIC) de los organismos gubernamentales.**

##### Categorías C (normas municipales)**, para las normas que aplican para las iniciativas de TIC de los ayuntamientos en sus respectivos municipios.**

##### Categorías D (normas para embajadas)**, para las normas que aplican únicamente para las iniciativas de TIC de las embajadas, consulados y misiones en el extranjero.**

##### Categorías E (normas especiales)**, para las normas que aplican a organismos gubernamentales con características específicas dependiendo de sus funciones y estructura orgánica, así como para iniciativas, proyectos o programas de gobierno, en el cual se haga uso de las TIC.**

**Nomenclatura**

La nomenclatura utilizada en el nombramiento de las NORTIC es de la siguiente manera; el nombre NORTIC, seguido de la categoría que engloba la norma, más el número de secuencia de creación y por último, el año de creación. De modo que el caso de la norma para la creación y administración de portales web del gobierno dominicano, por tener un alcance universal, pertenece a la categoría A; mientras que por ser la segunda NORTIC elaborada y ha sido lanzada en el año 2013, su denominación sería NORTIC A2:2013.