1

NOESIS
CONSULTING

CONCEPTOS FUNDAMENTALES DE GESTIÓN DE RIESGOS

NOESIS CONSULTING

INTRODUCCIÓN A LA GESTIÓN DE RIESGOS DE TI

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI

El riesgo se define como la combinación de la probabilidad de un evento y su consecuencia.

A menudo, el riesgo se considera un evento adverso que puede amenazar los activos de una organización o explotar vulnerabilidades y causar daños.

Se consideran varios factores al evaluar el riesgo, tales comocomo:

- la misión de la organización
- los activos
- las amenazas
- las vulnerabilidades
- probabilidad e impacto.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
Gobierno y gestion de riesgos

La gobernanza es la responsabilidad de proteger los activos de una organización.

Durante la última década, el término "gobernanza" se ha puesto a la vanguardia del pensamiento empresarial en respuesta a ejemplos que demuestran la importancia de la buena gobernanza y, en el otro extremo de la escala, los percances comerciales globales.

El gobierno corporativo de TI es el sistema mediante el cual se evalúa, dirige y controla el uso actual y futuro de TI.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
Gobierno y gestion de riesgos

La creación de valor se compone de la realización de beneficios, la optimización de riesgos y la optimización de recursos.

La optimización del riesgo es, por lo tanto, una parte esencial de cualquier sistema de gobierno y no puede verse aisladamente de la obtención de beneficios u optimización de recursos.

La gobernanza responde cuatro preguntas:

- ¿Estámos haciendo las cosas correctas?
- ¿Los estamos haciendo de la manera correcta?
- ¿Los estamos haciendo bien?
- ¿Estamos obteniendo los beneficios?

NOESIS CONSULTING

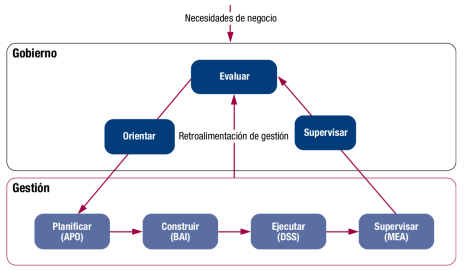
Introducción a la gestión de riesgos de TI
Gobierno y gestion de riesgos

- Existe una clara distinción entre gobernanza y gestión.
- La administración se enfoca en la planificación, construcción, ejecución y monitoreo dentro de las direcciones establecidas por el sistema de gobierno para crear valor mediante el logro de objetivos.
- La gestión de riesgos prevé los desafíos para lograr estos objetivos e intenta reducir las posibilidades y los impactos de que ocurran.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
Gobierno y gestion de riesgos

Figura 15—Las Áreas Clave de Gobierno y Gestión de COBIT 5



Introducción a la gestión de riesgos de TI
Gobierno y gestion de riesgos

La gobernanza eficaz del riesgo ayuda a garantizar que las prácticas de gestión del riesgo estén integradas en la empresa, lo que le permite garantizar un rendimiento óptimo ajustado al riesgo.

La gobernanza del riesgo tiene cuatro objetivos principales:

1. Establecer y mantener una visión común del riesgo.
2. Integrar la gestión de riesgos en la empresa.
3. Tomar decisiones comerciales conscientes del riesgo.
4. Asegúrese de que los controles de gestión de riesgos se implementen y funcionen correctamente

Introducción a la gestión de riesgos de TI

- La gestión de riesgos se define como las actividades coordinadas para dirigir y controlar una empresa con respecto al riesgo.
- En términos simples, el riesgo puede considerarse como un desafío para lograr los objetivos.
- Por lo tanto, la gestión de riesgos puede considerarse como la actividad realizada para prever dificultades y reducir las posibilidades de que ocurran esos desafíos y su impacto.
- La gestión eficaz del riesgo también puede ayudar a maximizar las oportunidades.

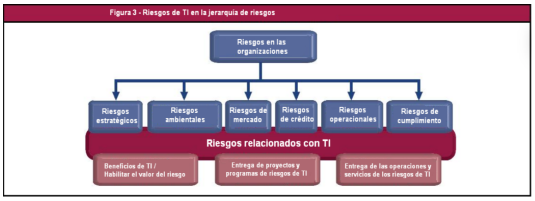
Introducción a la gestión de riesgos de TI
El contexto

- La gestión de riesgos comienza con la comprensión de la organización, pero la organización es principalmente un servidor del entorno o contexto en el que opera.
- Evaluar el contexto de la organización incluye evaluar la intención y la capacidad de las amenazas; el valor relativo y la confianza requerida en los activos; y la relación respectiva de vulnerabilidades que las amenazas podrían explotar para interceptar, modificar o fabricar datos en activos de información.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
El contexto

- La estrategia de la organización impulsará las líneas de negocio individuales que componen la organización, y cada línea de negocio desarrollará sistemas de información que respalden su función comercial.



NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
El Proceso

La gestión de riesgos es un proceso cíclico, como se muestra en la figura

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
El contexto

El primer paso en el proceso de gestión de riesgos de TI es la identificación del riesgo de TI, que incluye la determinación del contexto de riesgo y el marco de riesgo, y el proceso de identificación y documentación del riesgo.

- El esfuerzo de identificación de riesgos debe dar como resultado el listado y la documentación del riesgo.

Este paso se alinea con la siguiente fase del proceso de gestión de riesgos de TI: la evaluación de riesgos de TI.

El esfuerzo por evaluar el riesgo, incluida la priorización del riesgo, proporcionará a la gerencia los datos necesarios para su consideración como factor clave en la siguiente fase, la respuesta al riesgo y la mitigación.

La respuesta al riesgo y la mitigación abordan el apetito y la tolerancia al riesgo de la organización y la necesidad de encontrar formas rentables de abordar el riesgo

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
El contexto

La fase final de la gestión de riesgos de TI es la supervisión e informes de los riesgos y sus controles.

En esta fase, se supervisan los controles y los esfuerzos de gestión de los riesgos, así como el estado actual del riesgo, y los resultados se informan a la alta gerencia, quien determinará la necesidad de volver a cualquiera de las fases anteriores del proceso.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
El contexto

El proceso de gestión de riesgos de TI se basa en el ciclo completo de todos los elementos.

Si no se realiza una de las fases de manera completa y exhaustiva, el proceso de gestión de riesgos será ineficaz.

Una falla en cualquier paso del ciclo puede causar una deficiencia que afectará las otras fases.

Al igual que con todos los ciclos de vida, el ciclo de vida de la gestión de procesos se repite y mejora continuamente, cuanto más efectivo sea el esfuerzo de gestión de riesgos de TI y se obtendrán resultados consistentes.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
Importancia y Beneficios

Importancia de la gestión de riesgos de TI

Los beneficios de la gestión de riesgos de TI incluyen:

- Mejor supervisión de los activos de la organización.
- Pérdida minimizada
- Identificación de amenazas, vulnerabilidades y riesgos.
- Priorización de los esfuerzos de respuesta al riesgo
- Cumplimiento legal y regulatorio
- Mayor probabilidad de éxito del proyecto
- Rendimiento mejorado y la capacidad de alcanzar objetivos comerciales
- Aumento de la confianza de los interesados
- Creación de una cultura consciente del riesgo.
- Mejor gestión de incidentes y continuidad del negocio.
- Controles mejorados
- Mejor monitoreo e informes
- Toma de decisiones mejorada
- Capacidad para cumplir con el objetivo comercial

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
Riesgo empresarial versus riesgo de TI

El riesgo es una parte crítica de los negocios.

A menos que una empresa esté dispuesta a correr riesgos, no podrá darse cuenta de los beneficios asociados con el riesgo.

Sin embargo, tomar demasiado riesgo puede conducir a una mayor probabilidad de fracaso del negocio y pérdida de inversión.

Cada negocio enfrenta la decisión de cuánto riesgo tomar y qué oportunidades perder.

Esta es una decisión que refleja el nivel de aceptación del riesgo de la alta gerencia.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
Riesgo empresarial - continuidad del negocio

La gestión de riesgos de TI está estrechamente relacionada con la continuidad del negocio, y la evaluación de riesgos de TI suele ser un precursor de un análisis de impacto empresarial (BIA).

En muchos sentidos, la continuidad del negocio comienza donde la gestión de riesgos termina.

A través de la gestión de riesgos de TI, la organización intenta reducir todos los riesgos de TI a un nivel aceptable.

El riesgo es que el plan de continuidad del negocio (BCP) puede no ser adecuado o preciso, lo que lleva a una falla en la recuperación efectiva de un incidente.

NOESIS CONSULTING

Introducción a la gestión de riesgos de TI
Riesgo de TI y seguridad de la información

La seguridad de la información debe estar basada en el riesgo.

El Instituto Nacional de Estándares y Tecnología (NIST) establece que una organización debe proporcionar controles rentables y basados en el riesgo.

El profesional de riesgos debe ser capaz de demostrar el propósito de cada control y explicar el razonamiento detrás de la selección y ejecución del control.

- Control de riesgo
- Cambiar el riesgo

Riesgos de seguridad

Tratamiento del Riesgo

Evitar riesgos
Evitar significa salir de las actividades o de las condiciones que dan lugar a riesgo. Este es el caso cuando: No hay ninguna otra respuesta rentable que puede tener éxito y el riesgo no puede ser compartido o transferido.

Reducción de Riesgos / Mitigación
La reducción significa, que medidas están tomadas para detectar el riesgo, seguido por la acción para reducir la frecuencia y/o el impacto de un riesgo. Las maneras más comunes de respuesta al riesgo incluyen la Introducción de una serie de medidas de control o planes de acción y su monitoreo.

Compartido / Transferencia
Compartir significa reducir la frecuencia de riesgo o impacto mediante la transferencia o distribución de una parte del riesgo. Las técnicas más comunes son los seguros y la subcontratación.

Aceptación del riesgo
Aceptación significa que no se tomen medidas relativas con un riesgo particular, y la pérdida es aceptada cuando y si se produce. Esto es diferente de ignorar el riesgo, aceptar el riesgo supone que el riesgo es conocido, es decir, una decisión informada se ha aceptado por la dirección.

Introducción a la gestión de riesgos de TI Resumen

Hay muchas variables que un análisis de riesgos de TI debe considerar y muchas decisiones que debe tomar, pero el éxito del esfuerzo de gestión de riesgos de TI generalmente se basa en tener una perspectiva amplia de la organización de la gestión de riesgos, siguiendo una metodología estructurada y reuniendo la información correcta.

Es a través del éxito del esfuerzo de gestión de riesgos de TI que un los responsables de riesgos de TI podrán agregar valor, recomendar controles apropiados e informar el estado del perfil de riesgo a la gerencia y a todas las partes interesadas relevantes.

NOESIS CONSULTING

Cuestionario

- Analisis de Riesgos de TI
- Toolkit 4

NOESIS CONSULTING

NOESIS
CONSULTING

AUDITORIA BASADA EN RIESGOS

NOESIS CONSULTING

Objetivos del Entrenamiento

- Conceptos de Auditoría Basada en Riesgos
- Conceptos fundamentales de Gestión de Riesgos
  - ¿Que es la Gestión Integral del Riesgo?.
  - ¿Cuales son las responsabilidades al interior de la Empresa?
  - ¿Quienes participan?
- Proceso de la Gestión de Riesgos
  - Riesgo – Clasificación – Actividades de Control – Probabilidad – Impacto – Riesgo Inherente – Riesgo Residual.
- Estructura general del modelo de Gestión de Riesgos
- Base Normativa
- Controles Internos

NOESIS CONSULTING

¿Qué es?

La Auditoria Basada en Riesgos es una forma de conducir auditorias de diferentes tipos:

- De procesos
- De sistemas de información
- Operativa
- De sistemas de gestión
- De Estados Financieros

NOESIS CONSULTING

¿Qué es?

Basa su planeación y desarrollo en los riesgos críticos, es decir, los que pudieran causar el mayor impacto negativo en la consecución de los **objetivos de la organización**:

- Objetivos estratégicos
- Objetivos operacionales
- Objetivos de información
- Objetivos de cumplimiento

NOESIS CONSULTING

Objetivos Estratégicos

La misión de una entidad establece en amplios términos lo que se aspira a alcanzar. Es importante que la dirección con la ayuda del consejo establezca expresamente la razón de ser de la entidad. A partir de esto, la dirección fija los objetivos estratégicos, formula la estrategia y establece los correspondientes objetivos operativos, de información y de cumplimiento para la organización.

Los objetivos estratégicos son de alto nivel, están alineados con la misión y visión de la entidad y le dan su apoyo. Reflejan la opción que ha elegido la dirección en cuanto a cómo la entidad creará valor para sus grupos de interés.

NOESIS CONSULTING

Objetivos operativos

Se refieren a la eficacia y eficiencia de las operaciones de la entidad e incluyen otros sub-objetivos orientados a mejorar ambas características mediante la movilización de la empresa hacia sus metas finales.

Los objetivos operativos deben reflejar los entornos empresarial, sectorial y económico en los que actúa la entidad.

Un conjunto claro de objetivos operativos, vinculados a subjetivos, es esencial para el éxito. Los objetivos operativos proporcionan un punto de focalización para orientar la asignación de recursos.

NOESIS CONSULTING

Objetivos de información

Se refieren a la fiabilidad de la información. Incluyen la información interna y externa e implican la financiera y no financiera. Una información fiable proporciona a la dirección datos seguros y completos, adecuados para la finalidad pretendida, y le presta apoyo en su toma de decisiones y en el seguimiento de las actividades y rendimiento de la entidad.

La información también está relacionada con los documentos preparados para su difusión externa, como es el caso de los estados financieros y sus notas de detalle, los comentarios y análisis de la dirección y los informes presentados a entidades reguladoras.

NOESIS CONSULTING

Objetivos de cumplimiento

Se refieren al cumplimiento de leyes y normas relevantes. Dependen de factores externos y tienden a ser similares entre entidades, en algunos casos, y sectorialmente, entre otros.

Las entidades deben llevar a cabo sus actividades y a menudo acciones concretas de acuerdo con las leyes y normas relevantes. Las leyes y normas aplicables establecen pautas mínimas de conducta, que la entidad integra en sus objetivos de cumplimiento.

El historial de cumplimiento de una entidad puede afectar positiva o negativamente a su reputación en la comunidad y el mercado.

NOESIS CONSULTING

¿Para qué ?

Confirma si las operaciones, los productos o servicios se ajustan a lo establecido en la Misión, la Visión, los objetivos estratégicos, las reglas del negocio, las buenas y mejores practicas de control interno y seguridad y las normas legales aplicables.

NOESIS CONSULTING

Objetivo Principal

La Auditoria Basadas en Riesgos evalúa y verifica que los procesos auditados satisfagan los objetivos y necesidades de la organización de manera eficaz, eficiente y segura, enfatizando en que los activos y recursos utilizados en las operaciones del negocio estén provistos de los controles y seguridades necesarias para reducir los riesgos inherentes a niveles aceptables de riesgo residual.

NOESIS CONSULTING

Objetivo 1

La auditorias “basadas en riesgos” satisfacen dos grandes objetivos: el primero es evaluar la “efectividad” del control interno en los procesos (operativos y TIC).

Es decir, determinar la capacidad de los controles establecidos para reducir los riesgos potenciales críticos a niveles aceptables de riesgo residual.

Los resultados de esta evaluación son la base para determinar la naturaleza y extensión de las pruebas de auditoría necesarias (de cumplimiento y sustantivas)

NOESIS CONSULTING

Prueba de Auditoria Tradicional Vs ABR

Practice Name	Activity
Manage physical access to IT assets.	1. Manage the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorised by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access.
	2. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.
	3. Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.
	4. Instruct all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorisation.
	5. Require visitors to be escorted at all times while on-site. If an unaccompanied, unfamiliar individual who is not wearing staff identification is identified, alert security personnel.
	6. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. Ensure that the devices record entry and trigger an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners.
	7. Conduct regular physical security awareness training.

Practice Name	Activity
Manage physical access to IT assets.	
	2. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.
	4. Instruct all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorisation.
	5. Require visitors to be escorted at all times while on-site. If an unaccompanied, unfamiliar individual who is not wearing staff identification is identified, alert security personnel.
	6. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. Ensure that the devices record entry and trigger an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners.

NOESIS CONSULTING

Objetivo 2

El segundo objetivo es verificar el cumplimiento de los controles para los riesgos críticos que presenten efectividad “Apropiada” (pruebas de cumplimiento) y verificar los objetivos que pudieran ser impactados por los eventos de riesgo que presentan debilidades de control (pruebas sustantivas). Las pruebas se realizan individualmente para una muestra de las áreas organizacionales y terceros que intervengan en el proceso y que requieran pruebas.

NOESIS CONSULTING

Planificación

Entradas

- Administración (ejecutiva y Unidades)
- Proyectos clave y cambios en los negocios
- Fraude y errores
- Externos / problemas de la industria
- Auditoría Externa Ethical hacking

Entendimiento de la situación actual y resultados anteriores de auditoría

Identificar Riesgos

- Estrategia
- Operaciones
- Cumplimiento
- Financiero

Definir Riesgos

Entrevistas
Análisis
Talleres

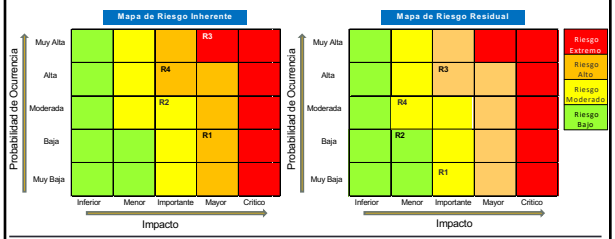
Priorizar

Los esfuerzos de evaluación de riesgos necesitan enfocarse en los problemas que tienen mayor impacto en los objetivos estratégicos:

NOESIS CONSULTING

Planificación

SERVICIOS DE TI



#	Detalle del Riesgo
R1	Pérdida de confidencialidad de la información transmitida a través de las redes de telecomunicaciones
R2	Pérdida de integridad de la información transmitida a través de las redes de telecomunicaciones
R3	No disponibilidad de las redes de telecomunicaciones
R4	Aplicaciones obsoletas con errores operativos

NOESIS CONSULTING

Planificación

Un proceso de definición de un plan de auditoría debe contemplar por lo menos:

- Riesgos priorizados desde la evaluación de riesgos
- Expectativas de la administración y el Comité de Auditoría
- Cumplimiento Normativo
- Proyectos especiales y auditorías no planeadas

Priorización

Asignación contra recursos

Priorización con el comité de Auditoría

Dentro del Plan

NOESIS CONSULTING

Plan de Auditoría de TI basada en riesgos

- Estrategia de la orgranización (Interno/Externo)
- Entorno legal y regulatorio
- Procesos críticos
- Estrategia de TI
- Estrategia de SI
- Application Maturity Assessment
- Análisis de BIA / IT
- Entrevistas
- Gestión de Problemas e Incidentes

- Taller final

NOESIS CONSULTING

Plan de Auditoría de TI basada en riesgos

El gerente de auditoría de TI debe reunirse con el director de información (CIO) y los miembros principales de la administración de TI para obtener su opinión y concurrencia con la evaluación de riesgos de los procesos de TI en el universo de auditoría.

Si hay un comité directivo de TI, el universo de auditoría también debe revisarse con él. Esto ayudará a garantizar la alineación entre TI, negocios y auditoría en las áreas clave de riesgo.

La reunión con el CIO y los gerentes de TI también debe presentar al personal de auditoría y comunicar el alcance, los objetivos, el cronograma y el proceso de comunicación que se utilizará durante todo el trabajo.

Esta también es una oportunidad para una discusión abierta sobre la percepción de la administración de TI de las áreas de riesgo, cambios significativos en el área bajo revisión e identificación de contactos apropiados en TI.

NOESIS CONSULTING

42

Auditoría Basada en Riesgos

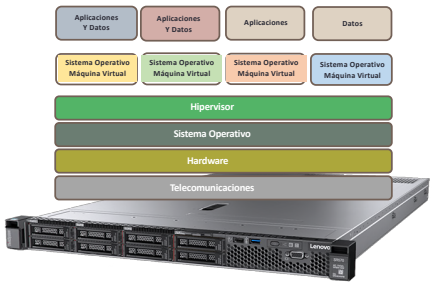
Beneficios para el área de Auditoria

- Soporta el logro de los objetivos de la auditoria
- Estandarización en el método de trabajo
- Integración del concepto de control en las políticas organizacionales
- Mayor efectividad en la planeación general de Auditoria.
- Evaluaciones enfocadas en riesgos
- Mayor cobertura de la administración de riesgos
- Auditorias más efectivas y con mayor valor agregado

NOESIS CONSULTING

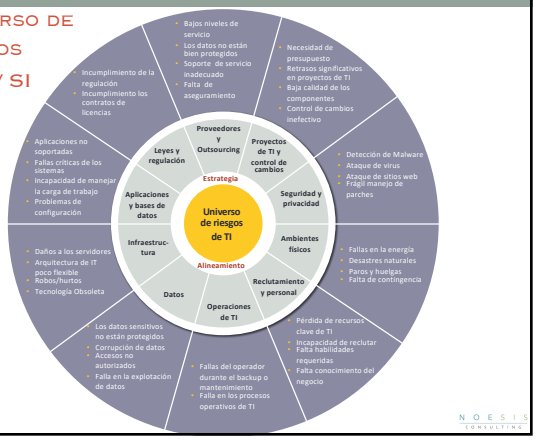
COMPLEJIDAD ACTUAL

Server tecnológico actual



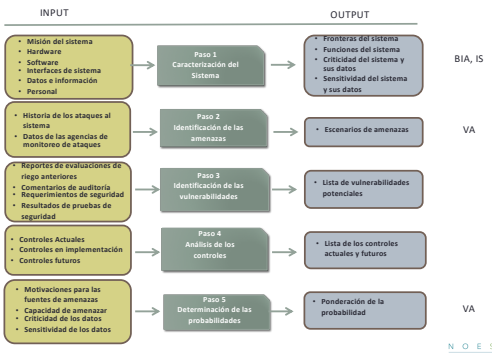
UNIVERSO DE RIESGOS

Universo de riesgos de TI / SI

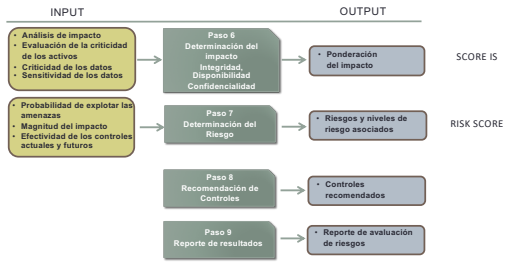


EVALUACION DE RIESGOS

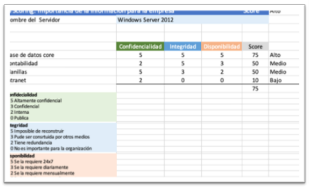
Evaluación de riesgos de Sistemas de TI



Evaluación de riesgos de SI



Ejemplo: Scoring Servidor Principal



Ejercicio

Análisis de la planificación
Toolkit 5

IT GENERAL CONTROLS
APPLICATION CONTROLS
END USER APPLICATIONS

Controles Generales de IT (ITGC)

ITGC representa la base de la estructura de control de TI. Ayudan a garantizar la fiabilidad de los datos generados por los sistemas de TI y respaldan la afirmación de que los sistemas funcionan según lo previsto y que la salida es confiable. ITGC generalmente incluye los siguientes tipos de controles:

Entorno de control, o aquellos controles diseñados para dar forma a la cultura corporativa.
Procedimientos de gestión de cambios: controles diseñados para garantizar que los cambios cumplan con los requisitos comerciales y estén autorizados.
Procedimientos de control del código fuente / versión del documento: controles diseñados para proteger la integridad del código del programa
Estándares del ciclo de vida del desarrollo de software: controles diseñados para garantizar que los proyectos de TI se gestionen de manera efectiva.
Políticas, estándares y procesos de acceso lógico: controles diseñados para administrar el acceso según las necesidades de negocio.

Controles Generales de IT (ITGC)

Políticas y procedimientos de gestión de incidentes: controles diseñados para abordar los errores de procesamiento operativo.
Políticas y procedimientos de gestión de problemas: controles diseñados para identificar y abordar la causa raíz de los incidentes.
Políticas y procedimientos de soporte técnico: políticas para ayudar a los usuarios a desempeñarse de manera más eficiente e informar problemas.
Configuración, instalación, prueba, estándares de gestión, políticas y procedimientos de hardware / software.
Recuperación ante desastres / procedimientos de respaldo y recuperación, para permitir el procesamiento continuo a pesar de las condiciones adversas.
Seguridad física: controles para garantizar la seguridad física de la tecnología de la información de los individuos y de los riesgos ambientales.

Controles de Aplicaciones de TI

Los controles de aplicaciones o programas de TI están completamente automatizados (es decir, los sistemas los ejecutan automáticamente) diseñados para garantizar el procesamiento completo y preciso de los datos, desde la entrada hasta la salida. Estos controles varían según el propósito comercial de la aplicación específica. Estos controles también pueden ayudar a garantizar la privacidad y seguridad de los datos transmitidos entre aplicaciones. Las categorías de controles de aplicaciones de TI pueden incluir:

Verificaciones de integridad: controles que garantizan que todos los registros se procesaron desde el inicio hasta la finalización.
Verificaciones de validez: controles que garantizan que solo se ingresen o procesen datos válidos.
Identificación: controles que garantizan que todos los usuarios estén identificados de forma única e irrefutable.
Autenticación: controles que proporcionan un mecanismo de autenticación en el sistema de la aplicación.
Autorización: controles que garantizan que solo los usuarios comerciales aprobados tengan acceso al sistema de aplicación.
Controles de entrada: controles que garantizan la integridad de los datos alimentados desde diferentes fuentes al sistema de aplicación.
Controles de registro (log): control que garantiza que las actividades dentro de la aplicación son registradas (usuario, acción, datos, etc.).

NOESIS CONSULTING

End User Applications (EUA)

Las hojas de cálculo o las bases de datos basadas en PC a menudo se utilizan para proporcionar datos críticos o cálculos relacionados con áreas negocio. Las hojas de cálculo financieras a menudo se clasifican como herramientas informáticas para el usuario final (EUC) que históricamente han estado ausentes de los controles de TI tradicionales. Pueden admitir cálculos complejos y proporcionar una flexibilidad significativa. Sin embargo, con flexibilidad y poder viene el riesgo de errores, un mayor potencial de fraude y mal uso de hojas de cálculo críticas que no siguen el ciclo de vida de desarrollo de software (diseño, desarrollo, pruebas, validación, implementación). Para remediar y controlar hojas de cálculo, las organizaciones pueden implementar controles tales como:

- Inventario y hojas de cálculo de con clasificación de riesgo
- Análisis basado en el riesgo para identificar errores lógicos en la hoja de cálculo
- Asegúrese de que los cálculos de la hoja de cálculo funcionen según lo previsto.
- Asegúrese de que los cambios en los cálculos clave estén debidamente aprobados.

La responsabilidad del control sobre las hojas de cálculo es una responsabilidad compartida con los usuarios comerciales y TI. La organización de TI generalmente se preocupa por proporcionar un disco compartido seguro para el almacenamiento de las hojas de cálculo y la copia de seguridad de datos. El personal comercial es responsable del resto.

NOESIS CONSULTING

Ejercicio

Selección de Controles
Toolkit 6

NOESIS CONSULTING

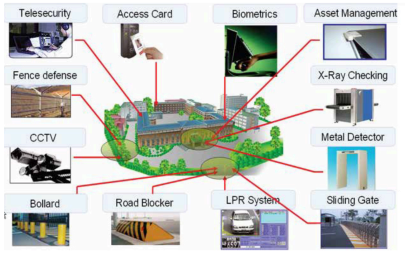
1

N O E S I S
C O N S U L T I N G

CONCEPTOS DE SEGURIDAD DE LA INFORMACION

2

Cómo proteger un tesoro



CONTROLES

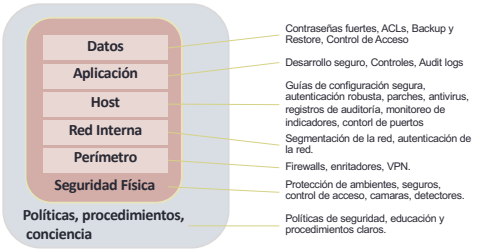
Físicos/lógicos

Tipos

- Disuasivos
- Preventivos
- Detectivos
- Ccorrectivos

3

La seguridad de la información – por capas



4

Seguridad de la Información

La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada

La información puede estar:

- Impresa o escrita en papel.
- Almacenada electrónicamente (PC, Server, Base de datos, Pendrive, etc).
- Mostrada en filmes.
- Difundida en una conversación.

Carácter de la información
- Financiera
- Estratégica
- Operacional
- Personal
- …

La información puede ser:
- creada
- almacenada
- destruida
- usada
- transmitida

NOESIS CONSULTING

5

Objetivos de la Seguridad de la información

El objetivo de la seguridad de la información es proteger los intereses de los negocios que dependan de la información.

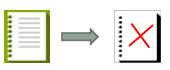
Los objetivos de la seguridad de la información se cumplen cuando se preserva:

- **LA CONFIDENCIALIDAD:** La información es accedida solo por aquellas personas que están debidamente autorizadas.
- **LA INTEGRIDAD**: La información es completa, precisa y protegida contra modificaciones no autorizadas.
- **LA DISPONIBILIDAD**: La información esta disponible y utilizable cuando se requiere.

NOESIS CONSULTING

6

Incidentes de seguridad de la información



Interruppcion - Disponibilidad

Intercepción - Confidencialidad

Modificación - Integridad

Producción - Integridad

NOESIS CONSULTING

7

¿Contra qué se debe proteger la información?

- Eventos de orden fortuito (destruccion parcial o total por incendio, inundaciones, eventos electricos, etc
- Eventos de orden deliberado (fraude, espionaje, sabotaje, vandalismo,etc.)

NOESIS CONSULTING

8

¿Qué es una amenaza?

Una amenaza es una probable violación de la seguridad. No es necesario que haya ocurrido para que la amenaza exista.

- Amenazas Naturales: Incendios, terremotos, Inundaciones
- Amenazas Humanas:
  - Maliciosas de origen Interno o Externo,
  - No maliciosas de origen de errores humanos

NOESIS CONSULTING

9

Amenazas

NOESIS CONSULTING

10

Más Amenazas!!

NOESIS CONSULTING

11

¿QUÉ ES VULNERABILIDAD?

Es una debilidad en un activo o en un procedimiento que establece la seguridad del activo. La amenazas explotan las vulnerabilidades

- Inadecuado compromiso de la direcció□n.
- Personal inadecuadamente capacitado y concientizado.
- Inadecuada asignacio□n de responsabilidades.
- Ausencia de poli□ticas/ procedimientos.
- Ausencia de controles (fi□sicos/lo□gicos) / (disuasivos/preventivos/detectivos/correctivos)
- Ausencia de reportes de incidentes y vulnerabilidades.
- Inadecuado seguimiento y monitoreo de los controles.

NOESIS CONSULTING

12

TIPOS DE EVALUACIONES DE SEGURIDAD

Exploraciones de vulnerabilidades

- Se enfoca en las debilidades conocidas
- Se puede automatizar
- No requiere experiencia necesariamente

Pruebas de penetración

- Se enfoca en las debilidades conocidas y desconocidas
- Requiere probadores altamente capacitados
- Lleva una carga legal tremenda en ciertos países/organizaciones

Auditoría en la Seguridad Informática

- Se enfoca en las políticas y procedimientos de seguridad
- Se utiliza para proporcionar evidencia para las normas de la industria

NOESIS CONSULTING

13

Riesgos de seguridad

NOESIS CONSULTING

14

¿Cómo establecer los Requerimientos de Seguridad de la Información?

Es esencial que la Organización identifique sus requisitos de seguridad.
La primer fuente procede de la valoración de los riesgos de la Organización. Con ella:

- Se identifican las amenazas a los activos,
- Se evalúa la vulnerabilidad y la probabilidad de su ocurrencia.
- Se estima su posible impacto

La segunda fuente es el conjunto de requisitos legales, estatutarios, regulatorios y contractuales que debe satisfacer:

- la Organización,
- sus socios comerciales,
- los contratistas
- los proveedores de servicios.

La tercera fuente está formada por los principios, objetivos y requisitos que la Organización ha desarrollado para apoyar sus operaciones.

NOESIS CONSULTING

Ejercicio

Análisis de Vulnerabilidades
Toolkit 7

NOESIS CONSULTING

16

ISO 27001/27002

NOESIS CONSULTING

17

Que es ISO 27001 / 27002

Son un estándar internacional que se ocupan de la gestión de seguridad de la información, y el principal es ISO27001: 2005.

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

- El SGSI (Sistema de Gestión de la Seguridad de la Ingormación o ISMS: Information Security Managemet System).
- La Valoración de riegos (Risk Assesment)
- Los Controles (ISO 27002:2013)

NOESIS CONSULTING

18

¿Como se implementa un SGSI?

Esta norma define un enfoque de proyecto para ayudar al diseño y la implementación de un SGSI, y utiliza el reconocido modelo Plan-Do-Check-Act (P-D-C-A) para estructurar las tareas requeridas para introducir un SGSI efectivo.

El ciclo P-D-C-A se puede resumir como:

- **Planifique** lo que necesita hacer para lograr el objetivo (que incluye definir cuál es ese objetivo).
- **Haz** lo que planeaste.
- **Verifique** que lo que ha hecho logre lo que había planeado para lograrlo e identifique cualquier brecha o déficit (es decir, verifique si ha cumplido los objetivos).
- **Actúe** sobre los resultados de la fase del plan para abordar las brechas y / o mejorar la eficiencia y la eficacia de lo que tiene en su lugar.

NOESIS CONSULTING

19

Controles ISO 27001:2005 - Anexo A

A.5 Política de seguridad
A.6 Organización de la seguridad de la información
A.7 Administración de activos
A.8 Seguridad de los recursos humanos
A.9 Seguridad física y del entorno
A.10 Administración de las comunicaciones y operaciones
A.11 Control de accesos
A.12 Adquisición de sistemas de información, desarrollo y mantenimiento
A.13 Administración de los incidentes de seguridad
A.14 Administración de la continuidad de negocio
A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

NOESIS CONSULTING

20

A.5 Política de seguridad

Este grupo está constituido por dos controles

- Existencia de la Política de Seguridad (Nivel político o estratégico de la organización): Es la mayor línea rectora, la alta dirección. Define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.
- Revisión de la Política de Seguridad de la información

Sus controles

5.1	**Política de Seguridad de la información**
5.1.1	Documento de Política de Seguridad de la Información
5.1.2	Revisión de la política de seguridad de la información

NOESIS CONSULTING

21

A.6 Organización de la SI

Este segundo grupo de controles abarca once de ellos y se subdivide en:

- **Organización Interna:** Compromiso de la Dirección, coordinaciones, responsabilidades, autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad, revisiones independientes.
- **Partes externas:** Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios de negocio.

Lo más importante a destacar de este grupo son dos cosas fundamentales que abarcan a ambos subgrupos:

- Organizar y Mantener actualizada la lista de actores involucrados (internos y externos), con el mayor detalle posible (Personas, responsabilidades, activos, necesidades, acuerdos, riesgos, etc.).
- Derechos y obligaciones de cualquiera de los involucrados.

NOESIS CONSULTING

22

A.6 Organización

6.1 Organización Interna

6.1.1 Compromiso de la Dirección con la seguridad de la información

6.1.2 Coordinación de la seguridad de la información

6.1.3 Asignación de responsabilidades relativas a la seguridad de la información

6.1.4 Proceso de autorización de recursos para el tratamiento de la información

6.1.5 Acuerdos de confidencialidad

6.1.6 Contacto con las autoridades

6.1.7 Contacto con grupos de especial interés

6.1.8 Revisión independiente de la seguridad de la información

NOESIS CONSULTING

23

A.6 Organización

6.2 Terceros

6.2.1 Identificación de los riesgos derivados del acceso de terceros

6.2.2 Tratamiento de la seguridad en la relación con los clientes

6.2.3 Tratamiento de la seguridad en contratos con terceros

NOESIS CONSULTING

24

A.7 Administracion de activos

Este grupo cubre cinco controles y también se encuentra subdividido en:

- Responsabilidad en los recursos: Inventario y propietario de los recursos, uso aceptable de los mismos.
- Clasificación de la información: Guías de clasificación y Denominación, identificación y tratamiento de la información.

Este grupo es eminentemente procedimental, en cuanto a que todo recurso debe estar perfectamente inventariado y que toda la información deberá ser tratada de acuerdo a su nivel.

NOESIS CONSULTING

25

A.7 ADMINISTRACION DE ACTIVOS

7.1 Responsabilidad sobre los activos
7.1.1 Inventario de activos
7.1.2 Propiedad de los activos
7.1.3 Uso aceptable de los activos

7.2 Clasificación de la información
7.2.1 Directrices de clasificación
7.2.2 Etiquetado y manipulado de la información

NOESIS CONSULTING

26

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

Por un lado las personas son el activo más importante en una organización pero a su vez podemos considerar que los errores humanos son normalmente el mayor riesgo para la seguridad de la información.

Los controles para la seguridad de la información que se consideran en este capítulo abordan las medidas para la seguridad a abordar en la fase de contratación, durante el empleo y en la fase de término o finalización del empleo.

NOESIS CONSULTING

27

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo 1: Previo al empleo

Asegurar que los empleados y contratistas entulturaiendan sus responsabilidades y que sean aptos para los roles para los cuales están siendo considerados

Controles:

8.1.1 Funciones y responsabilidades
8.1.2 Investigación de antecedentes
8.1.3 Términos y condiciones de contratación

NOESIS CONSULTING

28

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo 2: Durante el empleo

Asegurar que los empleados y contratistas sean conscientes de y cumplan con las responsabilidades de seguridad de la información

Controles:

8.2.1 Responsabilidades de la dirección

8.2.2 Concientización, educación y formación en seguridad de la información

8.2.3 Proceso disciplinario

29

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo 3: Finalización o cambio de la relación laboral o empleo

Controles:

8.3.1 Responsabilidad del cese o cambio

8.3.2 Devolución de activos

8.3.3 Retirada de los derechos de acceso

30

A.9. SEGURIDAD FÍSICA Y AMBIENTAL

El estándar parece centrarse en el CPD pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos.

Prevenir acceso no autorizado, daño o interferencia a los edificios y por ende a la información.

Establecer procedimientos para prevenir daño y perdida de información, equipos y bienes tal que no afecten las actividades adversamente.

Prevenir extracción de información (robo) y mantener la integridad de la información y sus premisas donde se procesa información, mediante revisiones y chequeos periódicos.

31

A.9. SEGURIDAD FÍSICA Y AMBIENTAL

9.1 Areas seguras

9.1.1 Perímetro de seguridad física
9.1.2 Controles físicos de entrada
9.1.3 Seguridad de oficinas, despachos e instalaciones
9.1.4 Protección contra las amenazas externas y de origen ambiental
9.1.5 Trabajo en áreas seguras
9.1.6 Áreas de acceso público y de carga y descarga

NOESIS CONSULTING

32

A.9. SEGURIDAD FÍSICA Y AMBIENTAL

9.2 Seguridad de los equipos

9.2.1 Emplazamiento y protección de equipos
9.2.2 Instalaciones de suministro
9.2.3 Seguridad del cableado
9.2.4 Mantenimiento de los equipos
9.2.5 Seguridad de los equipos fuera de las instalaciones
9.2.6 Reutilización o retirada segura de equipos
9.2.7 Retirada de materiales propiedad de la empresa

NOESIS CONSULTING

Ejercicio

Análisis de la Seguridad de la Información
Toolkit 8

NOESIS CONSULTING

34

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

- Documente procedimientos, normas y directrices de seguridad de la información
- Supervisión de terceros proveedores de servicios y sus respectivas entregas de servicio.
- Adopte procesos estructurados de planificación de capacidad TI, desarrollo seguro, pruebas de seguridad, criterios de aceptación en producción.
- Combine controles tecnológicos (p. ej., software antivirus) con medidas no técnicas (educación, concienciación y formación).
- Implante procedimientos de backup y recuperación
- Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS.

NOESIS CONSULTING

35

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

Asegure los medios y la información en tránsito no solo físico sino electrónico (a través de las redes).

Encripte todos los datos sensibles o valiosos antes de ser transportados.

Considere las medidas necesarias para asegurar el intercambio de información como canales de comunicación, mensajería, utlilizando medios, etc.

Incorpore requisitos de seguridad de la información en los proyectos e-business. proyectos e-business.

Auditar Logs que registren actividad, excepciones y eventos de seguridad y realizar revisiones periódicas.

NOESIS CONSULTING

36

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Responsabilidades y procedimientos de operación

10.1.1 Documentación de los procedimientos de operación

10.1.2 Gestión de cambios

10.1.3 Segregación de tareas

10.1.4 Separación de los recursos de desarrollo, prueba y operación

10.2 Gestión de la provisión de servicios por terceros

10.2.1 Provisión de servicios

10.2.2 Supervisión y revisión de los servicios prestados por terceros

10.2.3 Gestión del cambio en los servicios prestados por terceros

NOESIS CONSULTING

37

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.3 Planificación y aceptación del sistema
10.3.1 Gestión de capacidades
10.3.2 Aceptación del sistema
10.4 Protección contra el código malicioso y descargable
10.4.1 Controles contra el código malicioso
10.4.2 Controles contra el código descargado en el cliente
10.5 Copias de seguridad
10.5.1 Copias de seguridad de la información

NOESIS CONSULTING

38

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.6 Gestión de la seguridad de las redes
10.6.1 Controles de red
10.6.2 Seguridad de los servicios de red
10.7 Manipulación de los soportes
10.7.1 Gestión de soportes extraíbles
10.7.2 Retirada de soportes
10.7.3 Procedimientos de manipulación de la información
10.7.4 Seguridad de la documentación del sistema

NOESIS CONSULTING

39

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.8 Intercambio de información
10.8.1 Políticas y procedimientos de intercambio de información
10.8.2 Acuerdos de intercambio
10.8.3 Soportes físicos en tránsito
10.8.4 Mensajería electrónica
10.8.5 Sistemas de información empresariales
10.9 Servicios de comercio electrónico
10.9.1 Comercio electrónico
10.9.2 Transacciones en línea
10.9.3 Información públicamente disponible

NOESIS CONSULTING

40

A.10 Gestión de comunicaciones y operaciones

10.10 Supervisión

10.10.1 Registros de auditoría
10.10.2 Supervisión del uso del sistema
10.10.3 Protección de la información de los registros
10.10.4 Registros de administración y operación
10.10.5 Registro de fallos
10.10.6 Sincronización del reloj

NOESIS CONSULTING

41

A.11 Control de Accesos

Establecer niveles de seguridad de acuerdo con el nivel de riesgo de los activos y sus propietarios.

Un procedimiento de registro y revocación de cuentas de usuarios, una adecuada administración de los privilegios y de las contraseñas de cada uno de ellos, realizar periódicas revisiones a intervalos regulares.

Definir y documentar las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo.

Establecer una política de uso de contraseñas, de cuidado y protección de la información en sus escritorios, medios removibles y pantallas.

NOESIS CONSULTING

42

A.11 Control de Accesos

Establecer una política de uso de servicios de red.

Establecer medidas de autenticación sobre los accesos remotos.

Seguridad en la validación de usuarios del sistema operativo, empleo de identificadores únicos de usuarios, correcta administración de contraseñas, control y limitación de tiempos en las sesiones.

Implante estándares de seguridad básica para todas las aplicaciones y middleware.

Tenga políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, laptops, PDAs, etc.), sino, en mayor medida, de la información almacenada en ellos.

NOESIS CONSULTING

43

A.11 Control de Accesos

11.1 Requisitos de negocio para el control de acceso
11.1.1 Política de control de acceso
11.2 Gestión de acceso de usuario
11.2.1 Registro de usuario
11.2.2 Gestión de privilegios
11.2.3 Gestión de contraseñas de usuario
11.2.4 Revisión de los derechos de acceso de usuario
11.3 Responsabilidades de usuario
11.3.1 Uso de contraseñas
11.3.2 Equipo de usuario desatendido
11.3.3 Política de puesto de trabajo despejado y pantalla limpia

NOESIS CONSULTING

44

A.11 Control de Accesos

11.4 Control de acceso a la red
11.4.1 Política de uso de los servicios en red
11.4.2 Autenticación de usuario para conexiones externas
11.4.3 Identificación de los equipos en las redes
11.4.4 Diagnóstico remoto y protección de los puertos de configuración
11.4.5 Segregación de las redes
11.4.6 Control de la conexión a la red
11.4.7 Control de encaminamiento (routing) de red

NOESIS CONSULTING

45

A.11 Control de Accesos

11.5 Control de acceso al sistema operativo
11.5.1 Procedimientos seguros de inicio de sesión
11.5.2 Identificación y autenticación de usuario
11.5.3 Sistema de gestión de contraseñas
11.5.4 Uso de los recursos del sistema
11.5.5 Desconexión automática de sesión
11.5.6 Limitación del tiempo de conexión

NOESIS CONSULTING

46

A.11 Control de Accesos

11.6 Control de acceso a las aplicaciones y a la información

11.6.1 Restricción del acceso a la información

11.6.2 Aislamiento de sistemas sensibles

11.7 Ordenadores portátiles y teletrabajo

11.7.1 Ordenadores portátiles y comunicaciones móviles

11.7.2 Teletrabajo

47

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

Incluir requerimientos de seguridad de las aplicaciones involucrando a los propietarios de la información, Riesgos (SI), Auditoría.

Utilice librerías y funciones estándar para necesidades corrientes como validación de datos de entrada, restricciones de rango y tipo, integridad referencial, etc.

Para mayor confianza con datos vitales, construya e incorpore funciones adicionales de validación y chequeo cruzado (p. ej., sumas totalizadas de control).

Desarrolle y use herramientas -y habilidades- de prueba automatizadas y manuales, para comprobar cuestiones habituales como desbordamientos de memoria, inyección SQL, etc

Utilice estándares formales de encriptación.

48

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

Definir directorios que deben y no deben cambiar, utilizar control de software operacional, test de esos datos y controlar el acceso al código fuente.

Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios.

Haga un seguimiento de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática siempre que sea posible.

49

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

12.1 Requisitos de seguridad de los sistemas de información
12.1.1 Análisis y especificación de los requisitos de seguridad

12.2 Tratamiento correcto de las aplicaciones
12.2.1 Validación de los datos de entrada
12.2.2 Control del procesamiento interno
12.2.3 Integridad de los mensajes
12.2.4 Validación de los datos de salida

NOESIS CONSULTING

50

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

12.3 Controles criptográficos
12.3.1 Política de uso de los controles criptográficos
12.3.2 Gestión de claves

12.4 Seguridad de los archivos del sistema
12.4.1 Control del software en explotación
12.4.2 Protección de los datos de prueba del sistema
12.4.3 Control de acceso al código fuente de los programas

NOESIS CONSULTING

51

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

12.5 Seguridad en los procesos de desarrollo y soporte
12.5.1 Procedimientos de control de cambios
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
12.5.3 Restricciones a los cambios en los paquetes de software
12.5.4 Fugas de información
12.5.5 Externalización del desarrollo de software

12.6 Gestión de la vulnerabilidad técnica
12.6.1 Control de las vulnerabilidades técnicas

NOESIS CONSULTING

52

A.13 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Establecer procedimientos de reporte de incidentes de seguridad y problemas de seguridad.

Analizar y tomar las medidas correctivas

NOESIS CONSULTING

53

A.13 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información

13.1.1 Notificación de eventos de seguridad de la información

13.1.2 Notificación de puntos débiles de seguridad

13.2 Gestión de incidentes de seguridad de la información y mejoras

13.2.1 Responsabilidades y procedimientos de operación

13.2.2 Aprendizaje de los incidentes de seguridad de la información

13.2.3 Recopilación de evidencias

NOESIS CONSULTING

54

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Contrarrestrar interrupciones a las actividades de la empresa y sus procesos de los efectos creados por un desastre o falla de sistema(s) de comunicación / informática implementando un plan de continuidad del negocio.

"La gestión de la continuidad comienza donde la gestión de riesgos acaba"

NOESIS CONSULTING

55

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

14.1.2 Continuidad del negocio y evaluación de riesgos

14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

14.1.4 Marco de referencia para la planificación de la continuidad del negocio

14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio

NOESIS CONSULTING

56

A.15 CUMPLIMIENTO

Prevenir brechas de seguridad por actos criminales o violación de ley civil, regulatoria, obligaciones contractuales u otros aspectos de impacto a la seguridad.

Asegurar un sistema de gestión cumpliendo con políticas de seguridad y normativas (ISO27002, ISO 9001 y otras)

NOESIS CONSULTING

57

A.15 CUMPLIMIENTO

15.1 Cumplimiento de los requisitos legales

15.1.1 Identificación de la legislación aplicable

15.1.2 Derechos de propiedad intelectual (IPR)

15.1.3 Protección de los documentos de la organización

15.1.4 Protección de datos y privacidad de la información de carácter personal

15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información

15.1.6 Regulación de los controles criptográficos

NOESIS CONSULTING

58

A.15 Cumplimiento

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

15.2.1 Cumplimiento de las políticas y normas de seguridad

15.2.2 Comprobación del cumplimiento técnico

15.3 Consideraciones sobre la auditoría de los sistemas de información

15.3.1 Controles de auditoría de los sistemas de información

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

NOESIS CONSULTING

59

Controles ISO 27001:2013 - Anexo A

A.5 Políticas de seguridad de la Información
A.6 Organización de la seguridad de la información
A.7 Seguridad de los Recursos Humanos
A.8 Gestión de recursos
A.9 Control de Acceso
A.10 Criptografía
A.11 Seguridad física y ambiental.
A.12 Seguridad Operacional
A.13 Seguridad de las Comunicaciones
A.14 Adquisición, desarrollo y mantenimiento de Sistemas
A.15 Relaciones con los proveedores
A.16 Gestión de Incidentes en Seguridad de la Información
A.17 Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio
A.18 Cumplimiento

NOESIS CONSULTING

Ejercicio

Análisis de la Operación de TI
Toolkit 9

NOESIS CONSULTING

61

SANS

SANS INSTITUTE TOP 20 CONTROLS

https://www.sans.org/

NOESIS CONSULTING

62

INVENTARIO DE DISPOSITIVOS AUTORIZADOS Y NO AUTORIZADOS

Cada vez que se instala un nuevo dispositivo en una red, existen riesgos de exponer la red a vulnerabilidades desconocidas o impedir su funcionamiento. El código malicioso puede aprovechar el nuevo hardware que no está configurado y parchado con las actualizaciones de seguridad adecuadas en el momento de la instalación. Los atacantes pueden usar estos sistemas vulnerables para instalar puertas traseras antes de que se endurezcan. Al automatizar el control crítico 1, es fundamental que todos los dispositivos tengan un sistema de control de inventario preciso y actualizado. Se debe prohibir que cualquier dispositivo que no esté en la base de datos se conecte a la red. Algunas organizaciones mantienen inventarios de activos utilizando productos comerciales empresariales específicos a gran escala o utilizando soluciones gratuitas para rastrear y barrer la red periódicamente.

Para evaluar la implementación del Control 1 de forma periódica, se conectará sistemas de prueba a al menos 10 ubicaciones en la red. Esto incluirá una selección de subredes asociadas con DMZ, estaciones de trabajo y servidores

NOESIS CONSULTING

63

INVENTARIO DE SOFTWARE AUTORIZADO Y NO AUTORIZADO

Una organización sin la capacidad de inventariar y controlar los programas instalados de sus computadoras hace que sus sistemas sean más vulnerables a los ataques. Además, es más probable que las máquinas mal controladas ejecuten software innecesario, lo que presenta posibles fallas de seguridad. Los sistemas comprometidos se convierten en un punto de partida para que los atacantes recopilen información confidencial. Para combatir esta amenaza potencial, una organización debe escanear una red e identificar aplicaciones conocidas. Las herramientas de inventario de activos están ampliamente disponibles. Las mejores herramientas proporcionan una verificación de inventario de cientos de aplicaciones comunes, obteniendo información sobre el nivel de parche de cada programa instalado. Esto garantiza que sea la última versión y que aproveche los nombres de aplicaciones estandarizados, como los que se encuentran en la especificación Common Platform Enumeration (CPE). Además de las comprobaciones de inventario, las herramientas implementan las listas blancas (permitir) y las listas negras (denegar).

Para evaluar la implementación del Control 2 de forma periódica, el equipo debe mover un programa de prueba de software benigno que no esté incluido en la lista de software autorizado en 10 sistemas de la red. El equipo debe verificar que el software esté bloqueado y no pueda ejecutarse

NOESIS CONSULTING

64

Configuraciones seguras para hardware y software en computadoras portátiles, estaciones de trabajo y servidores

Las configuraciones predeterminadas de software a menudo están orientadas a la facilidad de implementación y facilidad de uso y no a la seguridad, dejando a algunos sistemas explotables en su estado predeterminado. Los atacantes intentan explotar tanto los servicios accesibles a la red como el software del cliente utilizando diversas formas de malware. Sin la capacidad de inventario y control instalado y en funcionamiento, las empresas hacen que sus sistemas sean más vulnerables. Las organizaciones pueden implementar este control desarrollando una serie de imágenes y servidores de almacenamiento seguros para alojar estas imágenes estándar. Las herramientas de administración de la configuración se pueden emplear para medir la configuración del software instalado y buscar desviaciones de las configuraciones de imagen estándar utilizadas por la organización.

Para evaluar la implementación del Control 3 de forma periódica, el auditor debe configurar un sistema de prueba benigno, (uno que no contenga la imagen oficial endurecida, pero que contenga servicios adicionales, puertos y cambios en los archivos de configuración) a la red. El equipo de evaluación debe verificar que los sistemas generan una alerta con respecto a los cambios en el software.

NOESIS CONSULTING

65

Evaluación continua de vulnerabilidades y remediación

Poco después de que los investigadores o vendedores de seguridad descubren e informan nuevas vulnerabilidades, los atacantes diseñan el código y lo lanzan contra objetivos de interés. Cualquier retraso significativo en la búsqueda o reparación de software con vulnerabilidades críticas ofrece una amplia oportunidad para que los atacantes persistentes se abran paso y ganen el control de las máquinas vulnerables. Una gran cantidad de herramientas de escaneo de vulnerabilidades están disponibles para evaluar la configuración de seguridad de los sistemas. Las herramientas de escaneo de vulnerabilidades más efectivas comparan los resultados del escaneo actual con escaneos anteriores para determinar cómo las vulnerabilidades en el entorno han cambiado con el tiempo. Todas las máquinas identificadas por el sistema de inventario de activos deben analizarse en busca de vulnerabilidades.

Para evaluar la implementación del Control 4 periódicamente, el auditor debe verificar que las herramientas de escaneo hayan completado con éxito sus escaneos semanales o diarios.

NOESIS CONSULTING

66

Uso controlado de privilegios administrativos

El método más común que usan los atacantes para infiltrarse en una empresa objetivo es a través del mal uso de los privilegios de administrador por parte de un empleado. Un atacante puede convencer fácilmente a un usuario de la estación de trabajo para que abra un archivo adjunto de correo electrónico malicioso, descargue y abra un archivo desde un sitio malicioso, o navegue a un sitio que descargue automáticamente contenido malicioso. Si el usuario ha iniciado sesión como administrador, el atacante tiene acceso completo al sistema. Las características integradas del sistema operativo pueden extraer listas de cuentas con privilegios de superusuario, tanto localmente en sistemas individuales como en controladores de dominio generales. Estas cuentas deben ser monitoreadas y rastreadas muy de cerca.

Para evaluar la implementación del Control 5 de manera periódica, el auditor debe verificar que se aplique la política de contraseñas de la organización y que las cuentas del administrador se controlen cuidadosamente. El equipo de evaluación hace esto creando una cuenta de prueba de privilegios limitados, temporal, deshabilitada en diez sistemas diferentes. Luego intenta cambiar la contraseña de la cuenta a un valor que no cumple con la política de contraseña de la organización.

NOESIS CONSULTING

67

MANTENIMIENTO, MONITOREO Y ANÁLISIS DE REGISTROS DE AUDITORÍA

En ocasiones, los registros de auditoría proporcionan la única evidencia de un ataque exitoso. Muchas organizaciones mantienen registros de auditoría para fines de cumplimiento, pero rara vez los revisan. Cuando no se revisan los registros de auditoría, las organizaciones no saben que sus sistemas se han visto comprometidos. Los atacantes confían en esto. La mayoría de los sistemas operativos, servicios de red y tecnologías de firewall gratuitos y comerciales ofrecen capacidades de registro de auditoría. Dicho registro debe activarse y los registros deben enviarse a los servidores de registro centralizados. El sistema debe ser capaz de registrar todos los eventos en la red. El registro debe validarse tanto en la red como en los sistemas host.

Para evaluar la implementación del Control 6 periódicamente, el auditor debe revisar los registros de seguridad de varios dispositivos de red, servidores y hosts.

NOESIS CONSULTING

68

PROTECCIONES DE CORREO ELECTRÓNICO Y NAVEGADOR WEB

Los navegadores web y los clientes de correo electrónico son puntos de entrada y ataque muy comunes debido a su alta complejidad técnica y flexibilidad, y su interacción directa con los usuarios y dentro de los otros sistemas y sitios web. El contenido se puede diseñar para atraer a los usuarios falsos a tomar medidas que aumenten en gran medida el riesgo y permitan la introducción de código malicioso, la pérdida de datos valiosos y otros ataques. Las organizaciones deben minimizar la superficie de ataque y las oportunidades para que los atacantes manipulen el comportamiento humano a través de su interacción con navegadores web y sistemas de correo electrónico.

Para evaluar la implementación del Control 7 periódicamente, el auditor debe revisar que los firewalls bloqueen sitios inseguros y que las máquinas tienen instalados antimalware y antivirus

NOESIS CONSULTING

69

DEFENSAS DE MALWARE

El software malicioso es un aspecto integral y peligroso de las amenazas de Internet. Se dirige a usuarios finales y organizaciones a través de la navegación web, archivos adjuntos de correo electrónico, dispositivos móviles y otros vectores. El código malicioso puede alterar el contenido de un sistema, capturar datos confidenciales y propagarse a otros sistemas. Para garantizar que las firmas antivirus estén actualizadas, las organizaciones eficaces utilizan la automatización. Utilizan las funciones administrativas integradas de las suites de seguridad de endpoints empresariales para verificar que las funciones de antivirus, antispyware y sistemas de detección de intrusiones (IDS) basadas en host estén activas en cada sistema administrado. También realizan evaluaciones automáticas diariamente y revisan los resultados para encontrar y mitigar los sistemas que han desactivado tales protecciones o no tienen las últimas definiciones de malware. El sistema debe identificar cualquier software malicioso que se haya instalado, intentado instalar, ejecutar o intentado ejecutar en un sistema informático.

Para evaluar la implementación de Control 8 de forma periódica, el auditor debe instalar un programa de prueba de software benigno que parezca ser malware en un sistema y asegurarse de que se descubra y repare adecuadamente.

NOESIS CONSULTING

70

Limitación y control de puertos de red, protocolos y servicios

Los atacantes buscan servicios de red accesibles de forma remota que sean vulnerables a la explotación. Muchos paquetes de software instalan servicios automáticamente y los activan como parte de la instalación del paquete de software principal. Cuando esto ocurre, el software rara vez informa a un usuario que los servicios se han habilitado. Las herramientas de escaneo de puertos se utilizan para determinar qué servicios están escuchando en la red para una gama de sistemas de destino. Además de determinar qué puertos están abiertos, se pueden configurar escáneres de puertos efectivos para identificar la versión del protocolo y el servicio de escucha en cada puerto abierto descubierto. El sistema debe ser capaz de identificar cualquier puerto de red de escucha no autorizado que esté conectado a la red.

Para evaluar la implementación de Control 9 de forma periódica, el auditor debe instalar servicios de prueba reforzados con escuchas de red en diez ubicaciones de la red, incluida una selección de subredes asociadas con DMZ, estaciones de trabajo y servidores.

NOESIS CONSULTING

71

Capacidad de recuperación de datos (validado manualmente)

Cuando los atacantes comprometen las máquinas, a menudo realizan cambios significativos en las configuraciones y el software. A veces, los atacantes también hacen alteraciones sutiles de los datos almacenados en máquinas comprometidas, lo que puede poner en peligro la eficacia de la organización con información contaminada.

Para evaluar la implementación de Control 9 de forma periódica, una vez por trimestre, un equipo de evaluación debe evaluar una muestra aleatoria de las copias de seguridad del sistema al intentar restaurarlas en un entorno de banco de pruebas. Los sistemas restaurados deben verificarse para garantizar que el sistema operativo, la aplicación y los datos de la copia de seguridad estén intactos y funcionales.

NOESIS CONSULTING

72

Configuraciones seguras para dispositivos de red como cortafuegos, enrutadores y switches

Los atacantes penetran las defensas buscando agujeros electrónicos en los cortafuegos, enrutadores y conmutadores. Una vez que estos dispositivos de red han sido explotados, los atacantes pueden obtener acceso a las redes objetivo, redirigir el tráfico en esa red (a un sistema malicioso disfrazado de un sistema confiable) e interceptar y alterar la información durante la transmisión. Las organizaciones pueden usar herramientas comerciales que evaluarán el conjunto de reglas de los dispositivos de filtrado de red, que determinan si son consistentes o están en conflicto y proporcionan una verificación automática de los filtros de red. Además, estas herramientas comerciales buscan errores en conjuntos de reglas. Dichas herramientas deben ejecutarse cada vez que se realicen cambios significativos en los conjuntos de reglas de firewall, las ACL del enrutador u otras tecnologías de filtrado.

Para evaluar la implementación del Control 11 de forma periódica, el auditor debe realizar un cambio en cada tipo de dispositivo de red conectado a la red. Como mínimo, los enrutadores, conmutadores y firewalls deben ser probados. Si existen, se deben incluir IPS, IDS y otros dispositivos de red.

NOESIS CONSULTING

73

DEFENSA DE PERÍMETRO

Al atacar los sistemas orientados a Internet, los atacantes pueden crear un punto de retransmisión para entrar en otras redes o sistemas internos. Las herramientas automatizadas se pueden utilizar para explotar puntos de entrada vulnerables en una red. Para controlar el flujo de tráfico a través de las fronteras de la red y buscar ataques y evidencia de máquinas comprometidas, las defensas de límites deben ser de varias capas. Estos límites deben consistir en firewalls, servidores proxy, redes perimetrales DMZ y sistemas de prevención de intrusos y sistemas de detección de intrusos basados en la red. Las organizaciones deben probar regularmente estos sensores lanzando herramientas de escaneo de vulnerabilidades. Estas herramientas verifican que el tráfico del escáner active una alerta apropiada. Los paquetes capturados de los sensores del Sistema de detección de intrusiones (IDS) deben revisarse utilizando un script automatizado cada día, lo que garantiza que los volúmenes de registro estén dentro de los parámetros esperados, estén formateados correctamente y no hayan sido dañados.

Para evaluar la implementación del Control 12 de forma periódica, el auditor debe probar los dispositivos de perímetro. Esto se realiza enviando paquetes desde fuera de una red confiable, lo que garantiza que solo los paquetes autorizados se permitan a través del límite. Todos los demás paquetes deben descartarse.

NOESIS CONSULTING

74

PROTECCIÓN DE DATOS

La pérdida de datos protegidos y confidenciales es una grave amenaza para las operaciones comerciales y, potencialmente, para la seguridad nacional. Si bien algunos datos se filtran o se pierden como resultado de robo o espionaje, la gran mayoría de estos problemas son el resultado de protección de datos poco conocidas. Estos incluyen, entre otros, la falta de arquitecturas de políticas efectivas y el error del usuario. La frase "Prevención de pérdida de datos" (DLP) se refiere a un enfoque integral que abarca personas, procesos y sistemas que identifican, monitorean y protegen los datos en uso (por ejemplo, acciones de punto final), datos en movimiento (por ejemplo, acciones de red) y datos en reposo (p. ej., almacenamiento de datos) a través de una inspección profunda de contenido y con un marco de gestión centralizado. Las soluciones comerciales de DLP están disponibles para buscar intentos de exfiltración y detectar otras actividades sospechosas asociadas con una red protegida que contiene información confidencial. El sistema debe ser capaz de identificar datos no autorizados que salen de los sistemas de la organización

Para evaluar la implementación del Control 13 de forma periódica, el auditor debe intentar mover los conjuntos de datos de prueba (que activan los sistemas DLP pero no contienen datos confidenciales) fuera del entorno informático confiable a través de transferencias de archivos de red y medios extraíbles.

NOESIS CONSULTING

75

ACCESO CONTROLADO BASADO EN LA NECESIDAD DE SABER

Algunas organizaciones no identifican y separan con cuidado los datos confidenciales de la información menos sensible y públicamente disponible dentro de una red interna. En muchos entornos, los usuarios internos tienen acceso a toda o la mayoría de la información en la red. Una vez que los atacantes han penetrado en dicha red, pueden encontrar y extraer fácilmente información importante con poca resistencia. Este control a menudo se implementa utilizando la separación integrada de las cuentas de administrador de las cuentas que no son de administrador. El sistema debe poder detectar todos los intentos de los usuarios de acceder a los archivos sin los privilegios apropiados y debe generar una alerta o un correo electrónico para el personal administrativo. Esto incluye información sobre sistemas locales o recursos compartidos de archivos accesibles en red.

Para evaluar la implementación del Control 14 de forma periódica, el equipo de evaluación debe crear cuentas de prueba con acceso limitado y verificar que la cuenta no pueda acceder a la información controlada.

NOESIS CONSULTING

76

Control de Dispositivo Inalámbrico

Los atacantes que obtienen acceso inalámbrico a una organización desde estacionamientos cercanos han iniciado robos de datos importantes. Esto permite a los atacantes el acceso a largo plazo dentro de un objetivo. Las organizaciones eficaces ejecutan herramientas de detección, detección y detección inalámbricas comerciales, así como sistemas de detección de intrusos inalámbricos comerciales. El sistema debe ser capaz de identificar dispositivos o configuraciones inalámbricos no autorizados cuando estén dentro del alcance de los sistemas de la organización o estén conectados a sus redes.

Para evaluar la implementación del Control 15 de forma periódica, el auditor debe configurar clientes inalámbricos no autorizados pero reforzados y puntos de acceso inalámbrico a la red de la organización. También debe intentar conectarlos a las redes inalámbricas de la organización. Estos puntos de acceso deben detectarse y repararse de manera oportuna.

NOESIS CONSULTING

77

Monitoreo y control de cuentas

Los atacantes frecuentemente se hacen pasar por usuarios legítimos a través de cuentas de usuario inactivas. Este método dificulta que los observadores de red identifiquen el comportamiento de los atacantes. Aunque la mayoría de los sistemas operativos incluyen capacidades para registrar información sobre el uso de la cuenta, estas funciones a veces están deshabilitadas de manera predeterminada. El personal de seguridad puede configurar sistemas para registrar información más detallada sobre el acceso a la cuenta y utilizar scripts propios o herramientas de análisis de registros de terceros para analizar esta información. El sistema debe ser capaz de identificar cuentas de usuarios no autorizados cuando existan en el sistema.

Para evaluar la implementación del Control 16 de forma periódica, el auditor debe verificar que la lista de cuentas bloqueadas, cuentas deshabilitadas, cuentas con contraseñas que exceden la antigüedad máxima de la contraseña y cuentas con contraseñas que nunca caducan se han identificado con éxito diariamente .

NOESIS CONSULTING

78

Evaluación de habilidades de seguridad y capacitación adecuada para llenar brechas (validado manualmente)

Una organización que espera encontrar y responder a los ataques depende efectivamente de sus empleados y contratistas para encontrar las b rechas y corregirlas. Un programa sólido de evaluación de habilidades de seguridad puede proporcionar información procesable a los tomadores de decisiones sobre dónde debe mejorarse la conciencia de seguridad. También puede ayudar a determinar la asignación adecuada de recursos limitados para mejorar las prácticas de seguridad. La clave para mejorar las habilidades es la medición, no con exámenes de certificación, sino con evaluaciones que muestran tanto al empleado como al empleador dónde el conocimiento es suficiente y dónde hay lagunas. Una vez que se han identificado las brechas, se puede recurrir a los empleados que tienen el conocimiento requerido para que asesoren a los empleados que no. La organización también puede desarrollar programas de capacitación que mantengan preparados a los empleados.

Para evaluar la implementación del Control 17 de forma periódica, el auditor debe verificar el programa de capacitación, el control de las capacitciones de cada empleado y el resultado de las pruebas de conocimiento

NOESIS CONSULTING

79

Seguridad del Software de Aplicación

Las organizaciones criminales con frecuencia atacan vulnerabilidades tanto en software de aplicaciones basadas en la web como no basadas en la web. De hecho, es una prioridad para los delincuentes. El software de aplicación es vulnerable al acciones remotas de tres maneras:

- No verifica correctamente el tamaño de la entrada (input) del usuario
- No puede sanitizar la entrada del usuario al filtrar secuencias de caracteres potencialmente maliciosas
- No inicializa y borra las variables correctamente

Para evitar ataques, el software de aplicación desarrollado internamente y de terceros debe probarse cuidadosamente para encontrar fallas de seguridad. Las herramientas de prueba de código fuente, las herramientas de escaneo de seguridad de aplicaciones web y las herramientas de prueba de código de objeto han demostrado ser útiles para proteger el software de la aplicación. administrativo de la empresa.

Para evaluar la implementación de Control 18 mensualmente, el auditor debe usar un escáner de vulnerabilidad de aplicaciones web para probar fallas de seguridad del software.

NOESIS CONSULTING

80

Respuesta y gestión de incidentes (validado manualmente)

Sin un plan de respuesta a incidentes, una organización puede no descubrir un ataque en primer lugar. Incluso si se detecta el ataque, la organización puede no seguir los procedimientos adecuados para contener el daño, erradicar la presencia del atacante y recuperarse de manera segura. Por lo tanto, el atacante puede generar un impacto mucho mayor en la organización objetivo, causando más daño, infectando más sistemas y posiblemente extrayendo datos más confidenciales de lo que de otro modo sería posible. Después de definir procedimientos detallados de respuesta a incidentes, el equipo de respuesta a incidentes debe participar en capacitación periódica basada en escenarios. Esto incluye, entre otros, trabajar a través de una serie de escenarios de ataque que se ajustan a las amenazas y vulnerabilidades que enfrenta la organización.

Para evaluar la implementación de Control 19 se deben simular incidentes para validar las acciones de respuesta y los tiempos de respuesta de acuerdo al incidente.

NOESIS CONSULTING

81

Control crítico 20: Pruebas de penetración y ejercicios del equipo rojo (validados manualmente)

Los atacantes penetran en redes y sistemas a través de la ingeniería social y explotando software y hardware vulnerables. Las pruebas de penetración implican imitar las acciones de los atacantes informáticos y explotarlos para determinar qué tipo de acceso puede obtener un atacante. Cada organización debe definir un alcance claro y las reglas de participación para las pruebas de penetración y los análisis del equipo rojo. El alcance de tales proyectos debe incluir, al menos, sistemas con la información de mayor valor y la funcionalidad de procesamiento de producción.

Para evaluar la implementación de Control 20 se deben verificar que se realizaron las pruebas de penetración y revisar los resultados documentales.

NOESIS CONSULTING

82

COBIT

NOESIS CONSULTING

83

Figura 16—Modelo de Referencia de Procesos de COBIT 5

NOESIS CONSULTING

1

N O E S I S
C O N S U L T I N G

REQUERIMIENTOS LOCALES (NAGA, ASFI)
REQUERIMIENTOS NIA
NIA 315

2

Quiz

¿ Porque la norma de gobierno de la ASFI se denomina REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ?

¿ Que conocemos de las NIAs ?

¿ Que conocemos de las NAGAs?

¿ Qué conocemos de COBIT ?

¿ Qué conocemos de ISO27001, ISO 27002?

Requerimientos ASFI sobre Auditoría

SECCIÓN 5: UNIDAD DE AUDITORÍA INTERNA

Artículo 1° - (Características de la Unidad de Auditoría Interna) La Unidad de Auditoría Interna debe cumplir mínimamente con los siguientes aspectos:

a. Depender orgánica, funcional y administrativamente del Directorio a través del Comité de Auditoría;

b. Desempeñar sus funciones y cumplir sus objetivos de modo oportuno, independiente y eficiente. Las evaluaciones, revisiones o cualquier función que realice la Unidad de Auditoría Interna debe efectuarse con base en lo dispuesto en el presente Reglamento. Para las situaciones no previstas en éste, se aplicarán las Normas de Auditoría Generalmente Aceptadas en Bolivia (NAGA), Normas Internacionales de Auditoría (NIA) y el Código de Ética del Auditor Internacionalmente aplicable;

Requerimientos NAGA Bolivia
NA No.3 Planificación del Trabajo de Auditoría

1. OBJETIVOS

1.1 El proceso de Planificación descrito en estas recomendaciones, permitirá que los profesionales encargados de realizar exámenes de auditoria sobre información financiera, realicen una auditoria efectiva, de manera eficiente y oportuna. La planificación debe basarse en el conocimiento del negocio de la entidad auditada. La planificación debe hacer para, entre otras cosas:

a) Adquirir conocimiento del sistema de contabilidad de la entidad, de las políticas y procedimientos de control interno.
b) Establecer el grado de confianza que se espera tener en el control interno.
c) Determinar y programar la naturaleza, la oportunidad y el alcance de los procedimientos de auditoria que se llevarán a cabo.
d) Coordinar el trabajo que habrá de efectuarse.

1.2 Asimismo…

NOESIS CONSULTING

Requerimientos NAGA Bolivia
NA No.3 Planificación del Trabajo de Auditoría

2. AMBITO DE APLICACIÓN Y ALCANCE

2.1 El proceso de planificación se aplica en la auditoria tanto de estados financieros como de otra información financiera. La presente norma se enmarca en el contexto de auditorias recurrentes. En una auditoria que se efectúa por primera vez. El auditor puede requerir extender el proceso de planificación más allá de los aspectos mencionados en esta recomendación.

2.2 El alcance de la planificación variará de acuerdo con el tamaño y la complejidad de la auditoria, de las experiencias previas del auditor con la entidad y considerando el conocimiento de su negocio.

NOESIS CONSULTING

Requerimientos NAGA Bolivia
NA No.3 Planificación del Trabajo de Auditoría

3. ETAPAS DE LA PLANIFICACION

3.1 La planificación debe ser continua durante la auditoria y deberá incluir:

- El conocimiento del negocio de la entidad.
- El desarrollo de un plan general que incluya el alcance y dirección esperados de la auditoria, y
- La preparación de un programa de auditoria que incluya la naturaleza, oportunidad y alcance de los procedimientos de auditoria.

3.2 Los cambios …

NOESIS CONSULTING

Requerimientos NAGA Bolivia
NA No.3 Planificación del Trabajo de Auditoría

4. CONOCIMIENTO DEL NEGOCIO DE LA ENTIDAD

4.1 El auditor necesita tener cierto nivel de conocimiento de la actividad y el negocio de la entidad, que le permita identificar los eventos, transacciones y practicas que, a su juicio pueden tener un efecto significativo sobre la información financiera. Puede obtener dicho conocimiento de:

a) Los informes anuales de la entidad a sus accionistas

b) …

f) Discusiones con la gerencia de la entidad, las cuales pudieron incluir asuntos tales como:

- Cambios en la administración, en la estructura organizacional o en las actividades de la entidad.

NOESIS CONSULTING

Requerimientos NAGA Bolivia
NA No.3 Planificación del Trabajo de Auditoría

- Disposiciones legales vigentes del gobierno que afecten a la entidad.
- Evaluaciones actuales de los negocios que afecten a la entidad.
- Dificultades financieras o problemas de contabilidad actual o pendiente.
- Existencia de partes relacionadas.
- Cambios recientes en la tecnología, en tipos de productos o servicios y en métodos de producción o distribución.
- Cambios en el sistema de contabilidad y en el sistema de control interno

NOESIS CONSULTING

NIA 315

IDENTIFICACIÓN Y VALORACIÓN DE LOS RIESGOS DE INCORRECCIÓN MATERIAL MEDIANTE EL CONOCIMIENTO DE LA ENTIDAD Y DE SU ENTORNO

NOESIS CONSULTING

REQUERIMIENTOS DE LA NIA 315

NIA 315

Alcance: Esta NIA trata de la responsabilidad que tiene el auditor de identificar y valorar los riesgos de incorrección material en los estados financieros, mediante el conocimiento de la entidad y de su entorno, incluido el control interno de la entidad.

Objetivo: Identificar y valorar los riesgos de incorrección material, debida a fraude o error, tanto en los estados financieros como en las afirmaciones, mediante el conocimiento de la entidad y de su entorno, incluido su control interno, con la finalidad de proporcionar una base para el diseño y la implementación de respuestas a los riesgos valorados de incorrección material

Requerimientos de la NIA 315

1. Procedimientos de valoración del riesgo y actividades relacionadas
2. El conocimiento requerido de la entidad y su entorno, incluido su control interno
3. Identificación y valoración de los riesgos de incorrección material

Definiciones

Afirmaciones. Manifestaciones de la dirección, explícitas o no, incluidas en los estados financieros y tenidas en cuenta por el auditor al considerar los distintos tipos de incorrecciones que puedan existir.

Riesgo de negocio. Riesgo derivado de condiciones, hechos, circunstancias, acciones u omisiones significativos que podrían afectar negativamente a la capacidad de una entidad para conseguir sus objetivos y ejecutar sus estrategias o derivado del establecimiento de objetivos y estrategias inadecuados

Definiciones

Control interno. Proceso diseñado, implementado y mantenido por los responsables del gobierno corporativo de la entidad, la dirección y otro personal, con la finalidad de proporcionar una seguridad razonable sobre la consecución de los objetivos de la entidad relativos a la fiabilidad de la información financiera, la eficacia y eficiencia de las operaciones, así como sobre el cumplimiento de las disposiciones legales y reglamentarias aplicables. El término "controles" se refiere a cualquier aspecto relativo a uno o más componentes del control interno.

Riesgo significativo. Riesgo identificado y valorado de incorrección material que, a juicio del auditor, requiere una consideración especial en la auditoría.

Definiciones

Representación Errónea de Importancia Relativa: El concepto de una representación errónea de importancia relativa, se refiere a que podría haber algún error pero de poca importancia relativa; es decir, si ha habido un error en la clasificación de un gasto de mil dólares en una empresa que vende 20 millones de dólares, posiblemente ese error no modifique la opinión o interpretación de cualquier analista o interesado en la empresa

Definiciones

Incorrecciones materiales. Las incorrecciones se originan cuando se detecta que existe diferencia entre la cantidad, clasificación, presentación o información revelada, y la cantidad, clasificación, presentación o revelación de información requerida por cierta partida; es decir, las incorrecciones hacen referencia a aquellos errores de correspondencia que se presente entre la información revelada y la realidad o las condiciones determinadas por la normatividad vigente aplicable para el proceso del reconocimiento y revelación de un suceso.

NOESIS CONSULTING

PROCEDIMIENTOS DE VALORACION DEL RIESGO Y ACTIVIDADES RELACIONADAS

NOESIS CONSULTING

Tipos de riesgos significativos en la auditoría de estados financieros

En la auditoría de estados financieros, un riesgo significativo ocurre cuando el riesgo valorado de incorrección material es tan alto que, a juicio del auditor, requiere una consideración especial de auditoría. La existencia de riesgos significativos se determina después de identificar y valorar los riesgos de negocio y de fraude.

Los riesgos significativos se valoran antes de considerar cualquiera de los controles de mitigación. Además, los riesgos significativos se basan en el riesgo inherente y no en el riesgo combinado —que comprende tanto los riesgos inherentes como los de control interno.

Existen varios tipos de riesgos que un auditor puede llegar a considerar significativos en una auditoría de estados financieros, entre ellos están: actividades de alto riesgo, transacciones grandes con partes vinculadas, transacciones inusuales significativas, asuntos de juicio importantes que requieren intervención de la dirección, riesgos significativos de transacciones y potencial de fraude.

NOESIS CONSULTING

Tipos de riesgos significativos

Actividades de alto riesgo:

- Transacciones grandes con partes vinculadas
- Transacciones inusuales significativas
- Asuntos de juicio importantes que requieren intervención de la dirección
- Riesgos significativos de transacciones
- Potencial de fraude

Procedimientos de evaluación de riesgos:

a) **Indagaciones ante la dirección y otras personas de la entidad***. que, a juicio de auditor, puedan disponer de información que pueda facilitar la identificación de los riesgos de incorrección material, debida a fraude o error (incluye evaluación de fraude, políticas contables utilizadas, continuidad de la entidad como negocio en marcha, transacciones con afiliadas).

(*) 1. Responsables de la información financiera, 2. Encargados del gobierno corporativo, 3. Auditoría interna 4. Empleados involucrados en el inicio, procesamiento o registro de transacciones complejas o inusuales y, 5. Otras áreas de negocios (abogados internos, personal de mercadotecnia, ventas, etc.

Procedimientos de evaluación de riesgos

b) Procedimientos analíticos. (financiera y no financiera, por ej. razones simples, identificaciones de transacciones inusuales, tendencias).

c) Observación e inspección. Asimismo, se debe considerar la información del proceso de aceptación y/o continuidad con el cliente y en su caso, la experiencia acumulada.

EL CONOCIMIENTO REQUERIDO DE LA ENTIDAD Y SU ENTORNO, INCLUIDO SU CONTROL INTERNO

La entidad y su entorno

El conocimiento de la entidad y su entorno, por parte del auditor, incluye conocer información sobre los siguientes temas:

1. Factores de la industria, regulación y otros externos.
2. Naturaleza de la entidad.
3. Selección y aplicación de políticas contables.
4. Objetivos, estrategias y riesgos relacionados al negocio.
5. Medición y revisión del desempeño financiero de la entidad.
6. Control Interno

La entidad y su entorno

Factores de la industria, regulación y otros externos.

- Entorno competitivo, relaciones con proveedores y clientes, el mercado, la competencia, demanda, capacidad, precios, actividad cíclica o de temporada, tecnología de los productos, suministro y costo de energía, riesgos de la industria, experiencia y conocimiento sobre la misma.
- Prácticas contables de la industria, legislación y regulación, impuestos, políticas, restricciones y apoyos gubernamentales y requisitos ambientales.
- Condiciones económicas generales, tasas de interés o disponibilidad de financiamiento, inflación y tipo de cambio.

La entidad y su entorno

Naturaleza de la entidad.

- Operaciones del negocio: fuentes de ingresos, productos o servicios, ventas, métodos de producción, alianzas, negocios conjuntos, outsourcing, segmentación, almacenes, oficinas, ubicaciones, clientes, proveedores y sindicatos
- Inversiones y actividades de inversiones: adquisiciones, valores y capital de trabajo.
- Financiamiento y actividades de financiamiento: asociadas, subsidiarias, deuda, financiamiento, derivados y socios.
- Información financiera: reglas contabilidad y prácticas de la industria (ingresos, transacciones complejas)

NOESIS CONSULTING

La entidad y su entorno

Selección y aplicación de políticas contables.

- Registro de transacciones importantes e inusuales.
- Políticas contables en áreas controversiales o emergentes en las que faltan lineamientos autorizados o consenso.
- Cambios en las políticas contables y normas de información financiera, leyes y regulaciones que son nuevas.

NOESIS CONSULTING

La entidad y su entorno

Objetivos, estrategias y riesgos del negocio.

Desarrollos de la industria, nuevos productos y servicios, expansión del negocio, IT. Otras condiciones que pueden indicar la existencia de riesgo de error material son:

- Devaluación, inflación, mercados volátiles, regulación compleja, órganos gubernamentales o de regulación, transacciones no rutinarias / no sistemáticas.
- Negocios en marcha, restricciones en capital y crédito, refinanciamientos, cadena de suministro, nuevas localidades, reorganizaciones , salida de ejecutivos clave.
- Deficiencias en control interno, errores del pasado.

NOESIS CONSULTING

La entidad y su entorno

Medición y revisión del desempeño financiero.

- Indicadores clave del desempeño (financiero y no financiero), proporciones, tendencias y estadísticas.
- Análisis periodo-sobre-periodo del desempeño financiero.
- Presupuestos, pronósticos, análisis de variaciones, información de segmentos /divisiones /departamentos, etc.
- Medidas y políticas de compensación por incentivos.
- Comparaciones del desempeño de una entidad con el de los competidores.

NOESIS CONSULTING

Ejercicio

- Realizar una evaluación del entorno
- Toolkit 1

NOESIS CONSULTING

CONTROL INTERNO

NOESIS CONSULTING

Entorno de Control Interno

El ambiente de Control Interno (COSO Committee of Sponsoring Organizations of the Treadway Commission)

Componentes del control interno:

1) Entorno de control.
2) Proceso de evaluación de riesgos.
3) Sistemas de información.
4) Actividades de control.
5) Monitoreo de controles.

Entorno de Control Interno

El auditor deberá obtener un entendimiento del ambiente del control. Como parte de este entendimiento, el auditor deberá evaluar si:

a) La administración, bajo la supervisión de los encargados del gobierno corporativo de la entidad, ha creado y mantenido una cultura de honestidad y conducta ética; y
b) Las fortalezas de los elementos del entorno de control proporcionan, en conjunto, una base adecuada para los otros componentes del control interno, y si esos otros componentes resultan afectados de modo negativo por las debilidades en el ambiente del control.

Entorno de Control Interno (Apendice 2)

El entorno de control engloba los siguientes elementos:

a) Comunicación y vigilancia de la integridad y valores éticos.
b) Compromiso con la competencia.
c) Participación de los responsables del gobierno de la entidad.
d) Filosofía y estilo operativo de la administración.
e) Estructura organizacional.
f) Asignación de autoridad y responsabilidad.
g) Políticas y prácticas de recursos humanos.

Proceso de evaluación del riesgo de la entidad

El auditor deberá obtener un entendimiento de si la entidad tiene establecido un proceso para:

a) Identificar los riesgos de negocios relevantes para el logro de los objetivos de información financiera;
b) Estimar la importancia de los riesgos.
c) Evaluar la probabilidad de su ocurrencia.
d) Decidir sobre las acciones para hacer frente a esos riesgos.

Proceso de evaluación del riesgo de la entidad (Anexo 1)

Los riesgos pueden surgir o variar debido a circunstancias como las siguientes:

a) Cambios en el entorno operativo.
b) Nuevo personal.
c) Sistemas de información nuevos o actualizados.
d) Crecimiento rápido.
e) Nueva tecnología.
f) Nuevos modelos de negocio, productos o actividades.
g) Reestructuraciones corporativas.
h) Expansión de las operaciones en el extranjero.
i) Nuevos pronunciamientos contables.

Condiciones y eventos que pueden indicar riesgos de error material (Anexo 2)

Ejemplos:

- Operaciones en regiones económicamente inestables, por ejemplo, los países con importante devaluación de la moneda o economías altamente inflacionarias.
- Operaciones expuestas a mercados volátiles, por ejemplo, la negociación de futuros.
- Operaciones sujetas a un alto grado de regulación compleja.
- Problemas de negocios en marcha y liquidez que incluyen pérdida de clientes importantes.
- Restricciones en la disponibilidad de capital y crédito.
- Cambios en la industria en que opera la entidad.
- Cambios en la cadena de suministro.

Condiciones y eventos que pueden indicar riesgos de error material (Anexo 2)

- Desarrollo u oferta de nuevos productos o servicios, o cambiar a nuevas líneas de negocio.
- Expansión a nuevas localidades.
- Cambios en la entidad como grandes adquisiciones o reorganizaciones u otros eventos inusuales.
- Entidades o segmentos del negocio que probablemente se vendan.
- La existencia de alianzas y negocios conjuntos complejos.
- Uso de finanzas fuera del balance, entidades de propósito especial, y otros arreglos de financiamiento complejos.
- Transacciones importantes con partes relacionadas.
- Falta de personal con habilidades apropiadas de contabilidad e información financiera.
- Cambios en personal clave incluyendo salida de ejecutivos clave.
- Debilidades en control interno, especialmente las no atendidas por la administración.

NOESIS CONSULTING

Condiciones y eventos que pueden indicar riesgos de error material (Anexo 2)

- Inconsistencias entre la estrategia de TI de la entidad y sus estrategias de negocios.
- Cambios en el entorno de TI.
- Instalación de importantes sistemas nuevos de TI relacionados con la información financiera.
- Investigaciones de las operaciones o resultados financieros de la entidad, por parte de órganos de regulación o gubernamentales.
- Representaciones erróneas pasadas, historia de errores o una importante cantidad de ajustes al final del ejercicio.
- Importante cantidad de transacciones no de rutina o no sistemáticas, incluyendo transacciones inter-compañía y con grandes ingresos al final del ejercicio.
- Transacciones que se registran con base en los propósitos de la administración, por ejemplo, el refinanciamiento de deuda, activos por vender y clasificación de valores negociables.

NOESIS CONSULTING

Condiciones y eventos que pueden indicar riesgos de error material (Anexo 2)

- Aplicación de nuevos pronunciamientos de contabilidad.
- Mediciones contables que implican procesos complejos.
- Eventos o transacciones que implican una importante falta de certeza en la medición, incluyendo estimaciones contables.
- Litigios pendientes y obligaciones contingentes, por ejemplo, las garantías de ventas, garantías financieras y reparación medioambiental.

NOESIS CONSULTING

Ejercicio

- Realizar una evaluación del ambiente de control
- Toolkit 2

Sistema de información, incluidos los procesos de negocio relacionados, relevante para la información financiera y la comunicación

El auditor deberá obtener un entendimiento del sistema de información, incluyendo los relacionados con los procesos de negocios, que son relevantes a la información financiera, considerando las áreas siguientes:

- Cómo el sistema de información captura los eventos y condiciones que no sean transacciones, que son importantes para los estados financieros;
- El proceso de información financiera utilizado para preparar los estados financieros de la entidad, incluyendo estimaciones contables importantes y revelaciones; y
- Controles sobre los asientos de diario, incluyendo asientos no estándares de diario que se utilizan para registrar transacciones o ajustes no recurrentes, o inusuales.

Sistema de información, incluidos los procesos de negocio relacionados, relevante para la información financiera y la comunicación (Anexo 1)

Engloba los métodos y registros que:

- Identifican y registran todas las transacciones válidas.
- Describen en forma oportuna las transacciones con suficiente detalle para permitir la clasificación apropiada de las transacciones para la información financiera.
- Miden el valor de las transacciones en una manera que permite registrar su valor monetario apropiado en los estados financieros.
- Determinan el periodo de tiempo en que las transacciones ocurrieron para permitir registro de las transacciones en el ejercicio contable apropiado

Actividades de control

El auditor deberá obtener un entendimiento de las actividades de control relevantes a la auditoría, considerando aquéllas que el auditor juzgue necesario entender, para evaluar los riesgos de error material a nivel aseveraciones, y así mismo diseñar procedimientos adicionales de auditoría que respondan a los riesgos evaluados. Una auditoría no requiere un entendimiento de todas las actividades de control relacionadas con cada clase importante de transacciones, saldo de cuenta, y revelación en los estados financieros o con cada aseveración relevante a ellas.

Actividades de control

Las actividades de control que pueden ser relevantes a una auditoría pueden categorizarse como políticas y procedimientos pertinentes a lo siguiente (Anexo 1):

a) Revisiones de resultados (presupuestos).
b) Procesamiento de información (controles de aplicaciones y controles generales de TI).
c) Controles físicos (seguridad física de activos, salvaguardas, autorización para acceso a programas y archivos de computadoras, recuento periódico y cotejo vs registros).
d) Segregación de funciones (Autorización de transacciones, registro y custodia de activos).

Monitoreo de controles

El auditor deberá obtener un entendimiento de las principales actividades que la entidad tiene implementadas para monitorear el control interno sobre la información financiera, incluyendo las relacionadas con las actividades de control relevantes a la auditoría, y cómo inicia la entidad acciones correctivas para las debilidades en sus controles

Monitoreo de controles (Anexo 1)

- El monitoreo de controles puede incluir actividades como revisión de la administración de si las conciliaciones bancarias se preparan oportunamente; si la oportunidad y exactitud de las conciliaciones bancarias no se monitorean, es probable que el personal deje de prepararlas.
- Los auditores internos o personal que desempeñan funciones similares pueden contribuir al monitoreo de los controles de una entidad mediante evaluaciones separadas.
- Las actividades de monitoreo pueden incluir utilizar información de las comunicaciones de partes externas que puedan indicar problemas o resalten áreas en necesidad de mejora. Los clientes, de manera implícita, corroboran datos de facturación al pagar sus facturas o quejarse contra los cargos.

NOESIS CONSULTING

El control interno de la entidad

El auditor deberá entender los aspectos del control interno en vigor en la entidad que sean relevantes para la auditoría. No todos los controles que se relacionan con dicha información son relevantes para una auditoría. Es una cuestión de juicio profesional del auditor el considerar si un control, de manera individual, o en combinación con otros, es relevante para la auditoría. Una vez que el auditor ha comprendido y entendido los controles que son relevantes para la auditoría, éste deberá evaluar el diseño de esos controles y determinar y probar si han sido puestos en funcionamiento, para lo cual deberá aplicar los procedimientos de auditoría que considere adecuados en las circunstancias, y deben complementarse con preguntas hechas al personal de la entidad.

NOESIS CONSULTING

Diseño vs. Implementación

La evaluación del diseño de un control considera tomar en cuenta si el control, individualmente o en combinación con otros controles, es capaz de prevenir, detectar y corregir, de manera efectiva, errores importantes. La implementación de un control significa que el control existe y que la entidad lo está utilizando. No tiene sentido evaluar la aplicación de un control que no es efectivo, por lo que, en primer lugar, se deberá evaluar el diseño del control. Un control diseñado inadecuadamente puede representar una debilidad material del control interno de la entidad.

NOESIS CONSULTING

Documentación:

a) Las reuniones de trabajo tenidas con el equipo de auditoría en las que se trataron los puntos requeridos, así como las decisiones importantes tomadas.
b) Los elementos clave de la comprensión obtenida con respecto a cada uno de los aspectos de la entidad y de su entorno y de cada uno de los componentes de control interno; las fuentes de información de donde obtuvo su comprensión y los procedimientos de evaluación de riesgo realizados.
c) Los riesgos identificados y evaluados de error material a nivel de estados financieros y a nivel de aseveraciones (validez, integridad, registro, corte, valuación y presentación).
d) Los riesgos identificados y los controles relacionados sobre los que el auditor ha obtenido un entendimiento.

NOESIS CONSULTING

Ejercicio

- Evaluacion de las actividades de control
- Toolkit 3

NOESIS CONSULTING

RESUMEN

NOESIS CONSULTING

Resumen

- La ASFI hace una referencia a las NAGAs y NIAs
- La NAGA y NIA tiene una aplicación limitada para Auditoría de TI/SI
- La NIA-315 nos da algunas pautas de lo que se debe conocer y entender antes de realizar una auditoría de Sistemas.
  - Su enfoque es altamente orientado a los resultados financieros.
  - Su enfoque de la identificación de riesgos en relativamente simple sin embargo hace énfasis en el análisis Top Down.
  - Su enfoque a la verificación de los controles es más completa.

NOESIS CONSULTING