



unitec®

FACULTAD DE INGENIERIA

GOBERNABILIDAD DE LA INFORMACIÓN

Sección:

164

Catedrático:

Ing. Lucas Cueva

Actividad:

Resumen de Charla

Presentado Por:

Mirian Georgina Pinto Welchez – 22111199

Cortes, San Pedro Sula

Jueves 08 de julio de 2023

Contenido

¿Qué es el gobierno de TI?	6
¿Cuáles son los alcances del gobierno de TI?	6
¿Cuáles son las 5 principales áreas que rigen el gobierno de TI?	6
¿Qué es la administración de TI?	6
¿Cuáles son los marcos de referencia para el gobierno de TI?	6
¿Qué es COBIT?	6
¿Qué es ITIL?	7
Que es ISO/IEC 27001:2005?	7
¿Cuáles son los 6 principios que ISO presenta para el gobierno de TI?	7
¿Cuáles son las 3 principales tareas que los directores deben usar para gobernar según ISO?	7
¿Cuáles son los 3 tipos de mecanismos que adopta un gobierno efectivo?	7
¿Qué debemos hacer para ayudar en un buen inicio en la implementación del gobierno de TI? ..	8
¿Cuáles son los esquemas para implementar esquemas de gobierno?	8
¿Que es ISO/IEC 38500?	8
¿Cuál es la función de ISO?	8
¿Cuál es el objetivo de ISO?	8
Cuál es el propósito de ISO	8
¿Cuáles son los 6 principios que ISO presenta para el gobierno de TI?	8
¿Cuáles son las 3 principales tareas que los directores deben usar para gobernar según ISO?	8
¿Para qué se utiliza la gobernanza de TI?	9
¿Cuáles son las áreas que cumple el gobierno de TI?	9
¿Porque debemos implementar un gobierno de TI?	9
¿Cuáles son las necesidades tienen las organizaciones?	9
¿Cales son los 3 aspectos claves que se consideran en ISO 27001?	10
¿Cuáles son los 3 principales ciberriesgos?	10
¿Cuál es el objetivo de ISO 27001?	10
¿Que permite garantizar una gestión eficaz de la ciberseguridad?	10
Que debemos considerar para orientar la Norma ISO/IEC 27001?	10
¿Cuáles son los beneficios de ISO 27001?	11
¿Cuáles son las soluciones integradas en la ciberseguridad?	11
¿Como se estructura ISO?	11

¿En qué se basa la norma ISO 27001?	11
¿Qué se hace en planificar según el ciclo?	11
¿Qué se hace en la D o Hacer del ciclo?	11
¿Qué se hace en la C o verificar del ciclo?	12
¿Qué se hace en la A o Actuar del ciclo?	12
¿Cuáles son los pasos para implementar ISO 27001?	12
¿Qué es COBIT 5?	12
¿Cuáles son los principios de COBIT 5?	12
¿Cuáles son las 7 categorías de catalizadores?	13
¿Qué es gobierno según COBIT 5?	13
¿Qué es la gestión según COBIT 5?	13
¿Cuáles son los factores críticos para una implementación con éxito de COBIT5?	13
¿Cuáles son las típicas áreas sensibles para los que el nuevo gobierno o gestión puede se una solución?	14
Cuales son otros eventos en el entorno interno y externo de la empresa que pueden señalar o poner el foco en el gobierno y gestión de TI.	14
¿Cuáles son los 3 componentes interrelacionados del ciclo de vida?	15
¿Cuáles son las fases de la gestión del programa?	15
¿Cuáles son las fases de la habilitación del cambio?	15
Cuale son las fases del ciclo de vida de mejora?	15
¿Qué es el caso de negocio?	15
¿Cuáles son las etapas del ciclo de vida de ITIL?	16
¿Qué es a la fase de estrategia del servicio?	16
¿Cuál es la misión de la estrategia del servicio?	16
¿Cuáles son los procesos de la fase de la estrategia de los servicios?	16
¿Qué es el Diseño e servicio de ITIL?	16
¿Cuáles son los procesos del diseño el servicio?	16
¿Qué es la transición del servicio ITIL?	17
¿Cuál es el objetivo de la transición de servicios ITIL?	17
¿Cuáles son los procesos de la transición de servicios ITIL?	17
¿Qué es la operación el servicio ITIL?	17
¿Cuál es el objetivo de la operación del servicio ITIL?	17

¿Cuáles son los procesos de la operación del servicio ITIL?	18
¿Qué es la mejora continua del servicio IITL?	18
¿Cuál es el objetivo?	18
¿Cuál es el objetivo de las iniciativas de mejora continua?	18
¿Cuáles son los procesos de la mejora continua del servicio de ITIL?	18
Defina el concepto de Gobierno de TI	18
ISO/38500 es un estándar internacional para las buenas prácticas del gobierno de las tecnologías de la información?	19
Enumere los 5 principios propuestos por ISO/38500	19
Enumere las 3 actividades que deben realizar los directores para gobernar TI	19
AL implementar un gobierno de TI, no es necesario visualizar el área de tecnologías de información de la empresa como un apoyo transversal a todos los demás procesos que interactúan dentro de las diferentes unidades de negocio.	19
Se logra entender que la gobernanza de TI a menudo se utiliza para describir los procesos, para decidir cómo se debe gastar el dinero para los recursos de TI. Este proceso de gobierno e TI incluye la priorización y justificación de las inversiones en TI.	20
Indique por lo menos 4 razones por las cuales se debe implementar un gobierno de TI	20
Hay que tener siempre claro que es correcto pensar que el área de Tecnologías de Información (TI) es independiente del negocio o que deba percibirse como un gasto más allá de una inversión.	20
Enumere los tres (3) aspectos clave que considera el ISO 27001, para la prevención y defensa de Ciberseguridad:	20
Enumere los tres (3) principales ciber riesgos a los que está expuesta una organización:	21
La Gestión eficaz de la Ciberseguridad permite garantizar la confidencialidad, la integridad y la disponibilidad de la información.	21
Hay que considerar varios aspectos para orientar la Norma ISO/IEC 27001 a la ciberseguridad, enumérelas:	21
COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, sin considerar los intereses relacionados con TI de las partes interesadas internas y externas.	22
Enumero por lo menos tres [3] factores críticos de éxitos al momento de implementar COBIT. ...	22
Enumere, por lo menos cuatro (4) eventos en el entorno interno y externo de la empresa pueden señalar o poner el foco en el gobierno y gestión de TI.	22

El Gobierno de TI se encarga de monitorear que el desempeño, cumplimiento y progreso sean acorde a las directivas y objetivos acordados.....23

Guía de estudio

Presentación 1:

¿Qué es el gobierno de TI?

El gobierno de TI es un ciclo de vida continuo

Determina quien toma las decisiones.

Es el encargado de tomar las decisiones mas importantes, quien posee la información clave y provee un adecuado direccionamiento para la implementación de esas decisiones.

El Gobierno de TI se encarga de monitorear que el desempeño, cumplimiento y progreso sean acorde a las directivas y objetivos acordados

¿Cuáles son los alcances del gobierno de TI?

- La entrega de valor de TI al negocio: se logra a través del alineamiento estratégico de TI con el negocio.
- Mitigación de los riesgos de TI: se alcanza haciendo de la responsabilidad algo inherente a la organización.
- Ambos necesitan ser soportador por recursos adecuados.

¿Cuáles son las 5 principales áreas que rigen el gobierno de TI?

- Las primeras dos de ellas son resultados: la entrega del valor y la gestión de riesgos
- Tres de ellas son facilitadores: alineamiento estratégico, gestión de recursos y medición del desempeño

¿Qué es la administración de TI?

Es el proceso de toma de decisiones y su implementación.

¿Cuáles son los marcos de referencia para el gobierno de TI?

- COBIT
- ITIL
- ISO/IEC 28500

¿Qué es COBIT?

Es un marco de referencia para el gobierno de TI y es un conjunto de herramientas de apoyo que permiten a los gerentes de TI encadenar los conceptos asociados a los requerimientos de control, los aspectos técnicos y los riesgos de negocio.

Habilita el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones.

Hace énfasis en el cumplimiento regulatorio.

¿Qué es ITIL?

Es esencialmente una serie de documentos que son usados para ayudar en la implementación de un marco de referencia para la administración de los servicios de TI.

Estándar de facto para las mejores prácticas en la provisión de servicios de TI

Que es ISO/IEC 27001:2005?

Es un estándar que establece los requerimientos de un sistema de gestión de la seguridad de la información.

Este ayuda a identificar, gestionar y minimizar el rango de amenazas a las cuales está expuesta regularmente la información

SESION 2

¿Cuáles son los 6 principios que ISO presenta para el gobierno de TI?

- Responsabilidad
- Estrategia
- Adquisición
- Desempeño
- Conformidad
- Conducta Humana

¿Cuáles son las 3 principales tareas que los directores deben usar para gobernar según ISO?

1. Evaluación del uso actual y futuro de TI
2. Preparación directa e implementación de planes y política para asegurar que el uso de TI se ajusta a los objetivos del negocio
3. Monitoreo de la conformidad de las políticas y desempeño en relación con lo planeado

¿Cuáles son los 3 tipos de mecanismos que adopta un gobierno efectivo?

- Estructura de toma de decisiones: Roles, comités, equipos ejecutivos
- Procesos de alineamiento: procesos formales para asegurar que las conductas del día a día son consistentes con las políticas de TI.
- Enfoques de comunicación: comunicados, recomendaciones, canales.

¿Qué debemos hacer para ayudar en un buen inicio en la implementación del gobierno de TI?

- Hacer preguntas.
- Saber plantear preguntas buenas,

¿Cuáles son los esquemas para implementar esquemas de gobierno?

- Estructuras, procesos y comunicaciones.

¿Que es ISO/IEC 38500?

- Es un estándar internacional para las buenas practicas del gobierno de TI

¿Cuál es la función de ISO?

Es gobernar las TI dentro de la empresa, para conseguirlo se basa en 6 principios y 3 procesos.

¿Cuál es el objetivo de ISO?

Proporcionar un marco de 6 principios para que los directores de la empresa puedan tomar decisiones basadas en los resultados que obtengan al dirigir monitorizar y evaluar el uso de las TI en si organización.

Cuál es el propósito de ISO

Es el promover el uso efectivo, eficiente y aceptable de la TI en todas las organizaciones para asegurarles a los involucrados que pueden tener la confianza en el gobierno de TI, así como proporcionar guías a los directivos para el uso adecuado de las TI.

¿Cuáles son los 6 principios que ISO presenta para el gobierno de TI?

- Responsabilidad: responsabilidades para el área de TI
- Estrategia: Planear las TI para apoyar de mejor forma a la empresa.
- Adquisición: que la adquisición sea por análisis y validaciones
- Desempeño: Asegurar que al TI tengan un rendimiento satisfactorio.
- Conformidad: Asegurar que la informática cumpla con las reglas formales.
- Conducta Humana: Asegurar que el uso de la TI respeta los factores humanos.

¿Cuáles son las 3 principales tareas que los directores deben usar para gobernar según ISO?

1. Evaluación del uso actual y futuro de TI
2. Preparar e implementar planes y políticas del uso de TI
3. Monitoreo de la conformidad de las políticas y desempeño en relación con lo planeado

Sesión 3

¿Para qué se utiliza la gobernanza de TI?

Se logra entender que la gobernanza de TI a menudo se utiliza para describir los procesos, para decidir cómo se debe gastar el dinero para los recursos de TI. Este proceso de gobierno de TI incluye la priorización y justificación de las inversiones en TI.

Incluye controles de gastos tales como presupuestos y niveles de autorización, obedece al sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información.

¿Cuáles son las áreas que cumple el gobierno de TI?

- Rendición de cuenta
 - o Conocer el objetivo
 - o Que hacer para lograr la meta
 - o Seguimiento de las actividades
 - o Rendición de cuentas
- Clarificar la autoridad
 - o Establecer el modelo de gobierno
 - o Ejecución de proyectos según la dirección dada
 - o Gestión operativa
 - o Unidades de negocio integradas

¿Porque debemos implementar un gobierno de TI?

1. Inversiones sin retorno y fallas en los sistemas que impactan al negocio.
2. Alta complejidad por la convivencia de múltiples plataformas tecnológicas.
3. Tendencias digitales: movilidad, machine learning, social media, bots, entre otros
4. Big Data, según IDC Digital Universe Study el volumen de datos continuará creciendo, estimando un incremento por un factor de 8 en los próximos 5 años.
5. Cada año se pierden miles de millones de dólares en ciberataques.

¿Cuáles son las necesidades tienen las organizaciones?

- Aumentar el logro de los beneficios, a través del uso efectivo e innovador de las TI de la empresa.
- Generar valor para el negocio a partir de nuevas inversiones de la empresa que son soportadas con inversión en las TI.
- Mantener el riesgo vinculado a las TI a un nivel aceptable y a su vez lograr la excelencia operacional a través de la aplicación de la tecnología.
- Contener los costos de los servicios de TI, además de cumplir con las leyes, regulaciones y políticas pertinentes.

- Asegurar la colaboración entre el negocio y las TI, apuntando a la satisfacción del usuario del negocio con la participación de TI y sus servicios

Sesión 4

¿Cuales son los 3 aspectos claves que se consideran en ISO 27001?

1. El análisis, gestión y mitigación de los ciber riesgos en las Tecnologías de la Información y las comunicaciones (TIC) de las organizaciones.
2. Los principales controles/medidas para una protección adecuada de la información, los servicios y sistemas de la organización.
3. El ciclo de mejora continua (PDCA-Plan, Do, Check, Act).

¿Cuáles son los 3 principales ciberriesgos?

- Fuga de información, por descuido o por consecuencia de un ataque
- El ransomware
- Phishing

¿Cuál es el objetivo de ISO 27001?

Proteger la integridad, disponibilidad y confidencialidad de la información en la empresa

¿Que permite garantizar una gestión eficaz de la ciberseguridad?

- Confidencialidad
- Integridad: asegurando que la información y sus métodos de proceso son exactos y completos.
- disponibilidad

Que debemos considerar para orientar la Norma ISO/IEC 27001?

1. Análisis de riesgos orientado a procesos de negocio/servicios de TI.
2. Relación con centros de respuesta a incidentes de seguridad y centros que previenen, monitoriza y controlan la ciberseguridad (CERT y SOC).
3. Auditorías técnicas de Pentest.
4. Incidencias de seguridad (gestión y notificación desde la detección).
5. Gestión de los parches y deployment (para la resolución de las incidencias).
6. Plan de Contingencia de TIC/Ciber-resiliencia TIC.

¿Cuáles son los beneficios de ISO 27001?

- permite hablar un lenguaje de ciberseguridad orientado a los objetivos del negocio, involucrando a la alta dirección de las organizaciones.
- ahorro de costes de ciberseguridad superfluos
- Facilita el cumplimiento de las distintas normativas que afectan a las organizaciones en lo que respecta a datos almacenados y privacidad, protección de datos y seguridad de la información en general
- Mejora la imagen corporativa de la organización al obtener una certificación reconocida internacionalmente
- Proporciona a la organización mayor ciber resiliencia;

¿Cuáles son las soluciones integradas en la ciberseguridad?

- Incorporar a ISO 27001 el ISO 27032
- Incorporar a ISO 27001 el ISO 27017, ISO 27018.
- Incorporar a ISO 27001 el ISA 62443

Sesión 5

¿Cómo se estructura ISO?

1. Evaluación y tratamiento de riesgos
2. Aplicar las medidas de seguridad

¿En qué se basa la norma ISO 27001?

Se basa en un enfoque fundamentado en el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar o ciclo PDCA

¿Qué se hace en planificar según el ciclo?

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

¿Qué se hace en la D o Hacer del ciclo?

- Implantar el plan de gestión de riesgos
- Aplicar el SGSI
- Implantar los controles

¿Qué se hace en la C o verificar del ciclo?

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

¿Qué se hace en la A o Actuar del ciclo?

- Adoptar acciones correctivas
- Aplicar acciones de mejora

¿Cuáles son los pasos para implementar ISO 27001?

1. Identificar los objetivos de tu negocio
2. Consigue el soporte de administración
3. Define el alcance
4. Redacta una política de seguridad e la información
5. Define la metodología y estrategia de evaluación de riesgos
6. Elabora un plan de tratamientos de riesgos y administra esos riesgos
7. Establece políticas y procedimientos para controlar los riesgos
8. Asigna los recursos necesarios de implementa la capacitación y los programas de concienciación
9. Supervisa cuidadosamente el SSGI
10. Prepárate para una auditoría interna
11. Revisa periódicamente la gestión

Sesión 6

¿Qué es COBIT 5?

Provee de un marco integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de la TI corporativas.

Ayuda a las empresas a crear un valor optimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles y el uso de los recursos.

Es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o el sector público.

¿Cuáles son los principios de COBIT 5?

1. Satisfacer las necesidades de las partes interesadas
2. Cubrir la empresa extrema a extremo
3. Aplicar un marco de referencia único integrado

4. Hacer posible un enfoque holístico
5. Separar el gobierno de la gestión

¿Cuáles son las 7 categorías de catalizadores?

1. Principios, políticas y marcos de trabajo
2. Procesos
3. Estructuras organizativas
4. Cultura, tica y comportamiento
5. Información
6. Servicio, infraestructuras y aplicaciones
7. Personas, habilidades y competencias

¿Qué es gobierno según COBIT 5?

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

¿Qué es la gestión según COBIT 5?

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Sesión 7

¿Cuáles son los factores críticos para una implementación con éxito de COBIT5?

- Que la alta dirección proporcione la orientación y directrices para la iniciativa, así como un decidido compromiso y apoyo.
- Todas las partes deben apoyar los procesos de gobierno y gestión, para entender el negocio y las metas de TI.
- Asegurar la comunicación efectiva y la habilitación de los cambios necesarios
- Asegurar la comunicación efectiva y la habilitación de los cambios necesarios.
- Personalizar COBIT y otras buenas prácticas y estándares empleados para ajustarlos al entorno único de la empresa.
- Enfocarse en resultados inmediatos (quick wins) y priorizar las mejoras más beneficiosas que sean más sencillas de implementar

¿Cuáles son las típicas áreas sensibles para los que el nuevo gobierno o gestión puede ser una solución?

- Frustración a nivel de negocio con iniciativas fallidas, incrementando los costos de TI y la percepción de bajo valor de negocio
- Incidentes significativos relativos al riesgo de TI, como pérdida de datos y fallos en proyectos
- Problemas en la externalización de la entrega del servicio, como por ejemplo el fallo sistemático al mantener los niveles de servicio acordados.
- Incapacidad de cumplir con requerimientos regulatorios o contractuales
- Limitación por TI de las capacidades de innovación de la compañía y la agilidad de negocio
- Hallazgos periódicos de auditoría en relación con el bajo rendimiento de TI o notificación de problemas de calidad de servicio de TI.
- Gastos de TI ocultos o malintencionados
- Duplicación o superposición entre iniciativas, o despilfarro de recursos, como la cancelación prematura de un proyecto
- Insuficientes recursos de TI, personal con habilidades inadecuadas, agotado o insatisfecho
- Fallos en los cambios de TI a la hora de alcanzar las necesidades de negocio y entregados tarde o con sobre costo
- Miembros del consejo, altos directivos y ejecutivos de alto nivel que son reticentes de implicarse con las TI o una ausencia de patrocinadores de las TI comprometidos y satisfechos
- Modelos operativos e TI complejos.

Cuales son otros eventos en el entorno interno y externo de la empresa que pueden señalar o poner el foco en el gobierno y gestión de TI.

- Fusiones, adquisiciones o desinversiones
- Un movimiento en el mercado, la economía o en el modelo de dotación de recursos.
- Un cambio en el modelo operativo de negocio o en el modelo de dotación de recursos.
- Nuevos requerimientos regulatorios y legales
- Un cambio tecnológico significativo o un nuevo paradigma
- Un proyecto de ámbito corporativo
- Un nuevo CEO, CFO, CIO, etc
- Auditorías externas revisiones de consultores
- Una nueva estrategia o prioridad de negocio

¿Cuáles son los 3 componentes interrelacionados del ciclo de vida?

- Ciclo de vida de mejora continua - este no es un proyecto único
- Habilidad el cambio – abordar los aspectos culturales y de comportamiento
- Gestión del programa

¿Cuáles son las fases de la gestión del programa?

- Iniciar el programa
- Definir problemas y oportunidades
- Definir hoja de ruta
- Planificar el problema
- Ejecutar el plan
- Obtener beneficios
- Revisar la efectividad

¿Cuáles son las fases de la habilitación del cambio?

- Establecer el deseo de cambio
- Constituir equipo de implementación
- Comunicar el resultado
- Identificar rol de los intervinientes
- Operar y usar
- Incorporar nuevos enfoques
- Sostener

¿Cuáles son las fases del ciclo de vida de mejora?

- Reconocer la necesidad de actuar
- Revisar el estado actual
- Definir el estado objetivo
- Construir mejoras
- Implantar mejoras
- Operar y medir
- Supervisar y evaluar

¿Qué es el caso de negocio?

Es una herramienta dinámica y operativa que debe ser continuamente actualizada para reflejar las previsiones actuales de manera que se pueda mantener una perspectiva de la viabilidad del programa.

¿Cuáles son las etapas del ciclo de vida de ITIL?

- Estrategia del servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

¿Qué es a la fase de estrategia del servicio?

Es el núcleo del enfoque de ciclo de vida, definido en el enfoque ITIL

¿Cuál es la misión de la estrategia del servicio?

Es definir los servicios informáticos que van a proporcionar valor a la organización.

¿Cuáles son los procesos de la fase de la estrategia de los servicios?

1. gestión de la estrategia: evalúa ofertas, capacidades del proveedor de servicios,
2. gestión del portafolio de los servicios: Garantiza que el proveedor disponga de los servicios adecuados
3. gestión financiera: Gestiona los requisitos de presupuesto, contabilidad
4. gestión de la demanda: Garantizar que el proveedor tenga capacidad suficiente para satisfacer la demanda
5. gestión de la relación de las relaciones del negocio: Identifica las necesidades de los clientes actuales y potenciales.

¿Qué es el Diseño e servicio de ITIL?

Consiste en el diseño de los servicios y de todos los elementos de apoyo para su introducción en el entorno real

Desde el diseño de nuevos servicios hasta cambios y mejoras a los servicios existente.

¿Cuáles son los procesos del diseño el servicio?

- Coordinación del diseño: Garantiza el diseño coherente y eficaz de los servicios de TI nuevos o modificados,
- gestión del catálogo de servicios: Garantiza la elaboración y el mantenimiento de un catálogo de servicios que contenga información precisa sobre todos los servicios operativos
- gestión del nivel de servicio: Deben negociarse los Acuerdos de Nivel de Servicio con los clientes, diseñando los servicios de acuerdo con los objetivos acordados
- gestión e riesgos: Identifica, evalúa y controla los riesgos.
- gestión de la capacidad: Garantiza que la capacidad de los servicios de TI y la infraestructura de TI puedan ofrecer los objetivos de SLA de manera rentable y eficaz

- gestión de la disponibilidad: Garantiza que toda la infraestructura de TI, los procesos, las herramientas y las funciones sean adecuados para los objetivos de disponibilidad acordados
- gestión de la continuidad del servicio de TI: Garantiza que el proveedor de servicios de TI pueda proporcionar siempre los niveles de servicio mínimos acordados
- Gestión de la seguridad de la información: Garantiza la confidencialidad, integridad y disponibilidad de la información
- gestión del cumplimiento: Garantiza que los servicios, procesos y sistemas de TI cumplen con las políticas empresariales y los requisitos legales
- gestión de la arquitectura: Define un plan para el desarrollo del panorama tecnológico en el futuro
- gestión de proveedores: Garantiza que todos los contratos con los proveedores den apoyo a las necesidades de la empresa

¿Qué es la transición del servicio ITIL?

En esta fase se construye, prueba y traslada el Diseño a la producción para permitir que el cliente empresarial logre el valor deseado.

¿Cuál es el objetivo de la transición de servicios ITIL?

Es crear y desplegar servicios de TI y garantizar que ellos cambios en los servicios y los procesos de gestión del servicio se lleven a cabo de forma segura y coordinada.

¿Cuáles son los procesos de la transición de servicios ITIL?

- gestión de cambios
- Evaluación e cambios
- gestión de proyectos
- Desarrollo de aplicaciones
- gestión de lanzamientos de implementación
- Validación y pruebas del servicio
- gestión de activos e servicio y configuración
- gestión del conocimiento

¿Qué es la operación el servicio ITIL?

Supervisan el estado general de los servicios que se prestan a los usuarios y a las funciones empresariales.

¿Cuál es el objetivo de la operación del servicio ITIL?

Es asegurarse de que los servicios de TI se prestan de forma eficaz y eficiente, satisfaciendo las peticiones de los usuarios, etc.

¿Cuáles son los procesos de la operación del servicio ITIL?

- gestión de eventos
- gestión de incidencias
- Cumplimiento de solicitudes
- gestión de accesos
- gestión de problemas
- Control de operaciones de TI
- gestión de las instalaciones
- gestión de aplicaciones
- gestión técnica
- Cierre

¿Qué es la mejora continua del servicio ITIL?

Utiliza métodos de gestión de la calidad para aprender de los éxitos y fracasos del pasado y mejorar la claridad general.

¿Cuál es el objetivo?

Mejorar continuamente la eficacia y eficiencia de los procesos y servicios de TI.

¿Cuál es el objetivo de las iniciativas de mejora continua?

Definir e implementar esfuerzos específicos destinados a mejorar los servicios y procesos con base en los resultados de las revisiones de los servicios y las evaluaciones de los procesos.

¿Cuáles son los procesos de la mejora continua del servicio de ITIL?

- Revisión del servicio
- Evaluación de procesos
- Definición de iniciativas de mejora continua
- Seguimiento de las iniciativas de CSI

Examen Bernie

Defina el concepto de Gobierno de TI

ISO/38500 es un estándar internacional para las buenas prácticas del gobierno de las tecnologías de la información?

R/ Falso

Enumere los 5 principios propuestos por ISO/38500

R/ Estrategia

Responsabilidad

Adquisición

Conducta Humana

Conformidad

Rendimiento

Enumere las 3 actividades que deben realizar los directores para gobernar TI

R/ Evaluar el uso de los TI

Preparar e implementar planes y políticas de uso de TI

Monitorear la conformidad con las políticas y el desempeño en relación con los planes

AL implementar un gobierno de TI, no es necesario visualizar el área de tecnologías de información de la empresa como un apoyo transversal a todos los demás procesos que interactúan dentro de las diferentes unidades de negocio.

R/ Falso

Se logra entender que la gobernanza de TI a menudo se utiliza para describir los procesos, para decidir cómo se debe gastar el dinero para los recursos de TI. Este proceso de gobierno e TI incluye la priorización y justificación de las inversiones en TI.

R/ Verdadero

Indique por lo menos 4 razones por las cuales se debe implementar un gobierno de TI

R/

1. A través de la implementación de un gobierno de TI se logra aportar valor a las áreas de la empresa implicadas en el proyecto.
2. Se puede mitigar las pérdidas por ciberataque, cada año se pierden miles de millones de dólares en ciberataques.
3. Inversiones sin retorno y fallas en los sistemas que impactan al negocio.
4. Tendencias digitales: movilidad, machine learning, social media, bots, entre otros.
5. Big Data, debido a que el volumen de datos sigue en crecimiento y lo seguirá durante los próximos años según expertos.
6. Alta complejidad por la convivencia de múltiples plataformas tecnológicas.
7. Las juntas empresariales, los ejecutivos y la gerencia tienen que adoptar a TI como cualquier otra parte importante del negocio.

Hay que tener siempre claro que es correcto pensar que el área de Tecnologías de Información (TI) es independiente del negocio o que deba percibirse como un gasto más allá de una inversión.

R/ falso

Enumere los tres (3) aspectos clave que considera el ISO 27001, para la prevención y defensa de Ciberseguridad:

Su respuesta:

1. El análisis, gestión y mitigación de los ciberriesgos en las Tecnologías de la Información y las comunicaciones (TIC) de las organizaciones.
2. Los principales controles/medidas para una protección adecuada de la información, los servicios y sistemas de la organización.
3. El ciclo de mejora continua (PDCA-Plan, Do, Check, Act).

Enumere los tres (3) principales ciber riesgos a los que está expuesta una organización:

Su respuesta:

- . La fuga de información: causada por un descuido o resultado de un ataque.
- . El Ransomware: Secuestro de información clave de la empresa, pidiendo un rescate por dicha informacion.
- . El Phishing: Descuido de los usuarios, debido a que es una suplantación de una web originar, enfocada en su mayoría a la banca online.

La Gestión eficaz de la Ciberseguridad permite garantizar la confidencialidad, la integridad y la disponibilidad de la información.

R/ Verdadero

Hay que considerar varios aspectos para orientar la Norma ISO/IEC 27001 a la ciberseguridad, enumérelas:

Su respuesta:

1. Analisis de riesgos orientado a procesos de negocio/servicios de TI.
2. Relación con centros de respuesta a incidentes de seguridad y centros que previenen, monitoriza y controlan la ciberseguridad (CERT y SOC).
3. Auditorías técnicas de Pentest.

4. Incidencias de seguridad (gestión y notificación desde la detección).
5. Gestión de los parches y deployment (para la resolución de las incidencias).
6. Plan de Contingencia de TIC/Ciber-resiliencia TIC.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, sin considerar los intereses relacionados con TI de las partes interesadas internas y externas.

R/ falso

Enumero por lo menos tres [3] factores críticos de éxitos al momento de implementar COBIT.

Su respuesta:

1. Que la alta dirección proporcione la orientación y directrices para la iniciativa, así como un decidido compromiso y apoyo.
2. Todas las partes deben apoyar los procesos de gobierno y gestión, para entender el negocio y las metas de TI.
3. Asegurar la comunicación efectiva y la habilitación de los cambios necesarios.
4. Personalizar COBIT y otras buenas prácticas y estándares empleados para ajustarlos al entorno único de la empresa.
5. Enfocarse en resultados inmediatos (quick wins) y priorizar las mejoras más beneficiosas que sean más sencillas de implementar.

Enumere, por lo menos cuatro (4) eventos en el entorno interno y externo de la empresa pueden señalar o poner el foco en el gobierno y gestión de TI.

Su respuesta:

- . Es importante para las iniciativas de implementacion que se apoyen en COBIT que sean correctamente gobernadas y adecuadamente gestionadas.
- . El apoyo y orientacion de las partes interesadas clave es critico para que las mejoras sean adoptadas y mantenidas.
- . Los requerimientos basados en aspectos sensibles y factores actuales deberian ser identificados por la direccion como áreas que tienen que ser consideradas.
- . Los roles y responsabilidades esenciales del programa deberian ser definidos y asignados.
- . Una vez que el compromiso ha sido obtenido, es necesario contar con los recursos adecuados para apoyar el programa.
- . Hay que tener cuidado de cara al exterior en mantener el compromiso de todas las partes interesadas afectadas

El Gobierno de TI se encarga de monitorear que el desempeño, cumplimiento y progreso sean acorde a las directivas y objetivos acordados.

R/ verdadero