TECNOLOGICO NACIONAL DE MÉXICO
ITS ACAYUCAN

Asignatura: Estrategias de Gestión de Servicios de TI **Clave :** IFF – 1012 **Periodo:** Enero – Junio 2025

NOMBRE DE LA UNIDAD: Introducción a la Gestión de Servicios de TI **NUMERO:** Uno
Tema: 1.4 Importancia de la gestión de servicios de TI. **Valor:** 15% **Duración:** 50min.

Práctica **01**

NOMBRE DEL ALUMNO: Jose Arturo Dominguez Rodriguez **GRUPO:** 807-A

Recursos educativos	Hora de inicio	Software	Hardware	Fecha de elaboración
Video y/o Antología	11:10	Word, brave	PC o Laptop	07/02/2025
	Hora de Termino			**Lugar**
	1:40			Salón B-7

1. Introducción

La gestión de servicios de TI se refiere a la administración de todos los recursos tecnológicos que soportan las operaciones de una organización. Su importancia radica en que ayuda a garantizar que los servicios de TI sean eficientes, confiables y estén alineados con los objetivos de la organización.

2. Objetivo

El alumno analizará un caso práctico para comprender mejor la importancia de la gestión de servicios de TI.

3. Fundamento

Como estudiante de **Ingeniería Informática**, es esencial comprender la **gestión de servicios de TI** (Tecnologías de la Información) ya que es un aspecto clave para asegurar que las organizaciones funcionen de manera eficiente en la era digital. La gestión de servicios de TI implica la planificación, diseño, implementación, operación y control de servicios tecnológicos con el fin de asegurar su disponibilidad, rendimiento y alineación con las necesidades del negocio.

4. Procedimiento

Analiza el siguiente planteamiento:

Simula la **gestión de incidentes** en un entorno de TI. Los incidentes son eventos que interrumpen el funcionamiento normal de los servicios, como caídas de servidor o problemas de acceso.
Pasos a seguir:

- Simula el reporte de un incidente donde un empleado no puede acceder al sistema interno de la empresa.
- Clasifica el incidente según su severidad (por ejemplo, bajo, medio o alto) y asigna un tiempo estimado de resolución.
- Registra el incidente en una herramienta de gestión (puedes usar herramientas como **Jira**, **ServiceNow**, **Zendesk**, o cualquier otra plataforma de gestión de servicios).
- Desarrolla una solución temporal (workaround) para restaurar el servicio rápidamente.
- Resuelve el incidente, documenta la solución y verifica que el sistema vuelva a la normalidad.

Simulación de Gestión de Incidente en un Entorno de TI

Paso 1: Reporte del Incidente

Incidente Reportado: Un empleado A no puede acceder al sistema interno de la empresa. El sistema está solicitando credenciales, pero no las acepta, lo que impide acceder a los recursos internos.

Detalles del Incidente:

- **Usuario afectado:** Empleado A
- **Descripción del incidente:** El empleado intenta ingresar al sistema interno de la empresa y, a pesar de usar las credenciales correctas, recibe un mensaje de error de "Credenciales no válidas".
- **Fecha y hora del reporte:** 2025-02-06, 09:30 AM
- **Urgencia:** Alta (impacto en la productividad del empleado).

Paso 2: Clasificación del Incidente y Severidad

Clasificación según severidad:

- **Severidad:** Alta
- **Justificación:** El incidente impide el acceso al sistema interno de la empresa, lo que afecta la capacidad del empleado para realizar sus tareas diarias.

Tiempo estimado de resolución:

- **Tiempo estimado:** 2 horas
- **Motivo:** El acceso a los sistemas es crítico, pero no parece ser un fallo generalizado. Es probable que sea un error de autenticación o configuración en el sistema que se puede resolver rápidamente.

Paso 3: Registro del Incidente en Herramienta de Gestión

El incidente se registra en **Jira Service Management** como un ticket de soporte.

Detalles del ticket:

- **ID del Ticket:** INC-2025-02-06-001

- **Prioridad:** Alta
- **Categoría:** Problemas de acceso
- **Descripción:** El empleado A no puede acceder al sistema interno. Recibe un error de "Credenciales no válidas".
- **Asignado a:** Equipo de soporte técnico (Usuario de la herramienta asignado: Técnico IT-01)
- **Fecha de creación:** 2025-02-06 09:30 AM

Paso 4: Desarrollo de una Solución Temporal (Workaround)

Solución temporal para restaurar el servicio rápidamente:

- Se propone un **restablecimiento de contraseña temporal**. Para esto, el empleado A recibirá un enlace para crear una nueva contraseña y restaurar el acceso.

Pasos para implementar el workaround:

1. **Restablecimiento de la contraseña:** El equipo de soporte envía al empleado A un enlace seguro para restablecer la contraseña.
2. **Prueba de acceso:** Una vez restablecida la contraseña, se pide al empleado A que intente acceder nuevamente al sistema.
3. **Verificación temporal:** Asegurar que el empleado A haya podido acceder con la nueva contraseña antes de realizar un análisis profundo del incidente.

Resultado esperado: El empleado A debería poder acceder al sistema mientras se investiga la causa raíz del problema.

Paso 5: Resolución del Incidente y Documentación

Análisis del problema:

- El equipo técnico revisa los logs del sistema y descubre que un problema de sincronización en el servicio de autenticación provocó que las credenciales del empleado A no fueran reconocidas correctamente.
- La solución permanente es restaurar la sincronización de la base de datos del sistema de autenticación.

Solución definitiva:

1. Se realiza una **sincronización** de la base de datos del sistema de autenticación.
2. Se prueba el acceso de otros empleados al sistema para asegurarse de que la solución aplicada no cause efectos adversos en otros usuarios.

Verificación:

- Se confirma que el **empleado A** puede acceder al sistema con su nueva contraseña.
- Otros usuarios prueban el acceso y todo funciona correctamente.

- **Paso 6: Cierre del Incidente**

Cierre del ticket:

- **Estado:** Resuelto
- **Fecha de resolución:** 2025-02-06, 11:00 AM
- **Descripción de la solución:** Se restableció la sincronización de la base de datos del sistema de autenticación, lo que resolvió el problema de acceso.
- **Comentario final:** El incidente fue resuelto satisfactoriamente. No se han reportado más problemas relacionados.

Registro en Jira:

- **Estado del Ticket:** Cerrado
- **Resumen:** El empleado A reportó problemas de acceso al sistema interno. Se resolvió el problema de sincronización de la base de datos de autenticación.

Tomando en cuenta el planteamiento anterior, analice el siguiente caso: " Simule el reporte de un incidente donde es hackeada (ciberseguridad) la cuenta de un empleado que trabaja en una empresa dedicada a la venta de computadoras", aplique los pasos desarrollados y resuélvalo, tome en cuenta los siguientes formatos para una mejor organización de la información:

Simulación de Gestión de Incidente en un Entorno de TI

Paso 1: **Reporte del incidente**	
Incidente Reportado	
Un empleado C no puede acceder al sistema interno de la empresa. El sistema está solicitando credenciales, pero no las acepta, lo que impide acceder a los recursos internos. Además, se detectan actividades sospechosas en su cuenta, como envió de encuestas dudosas a los clientes.	
Detalles del incidente	
Descripción del incidente	**Usuario afectado**
El empleado intenta ingresar al sistema interno de la empresa y no puede acceder, además varios clientes reportan que se le han enviado encuestas pidiendo información comprometedora por parte de este empleado	Empleado C
Fecha y hora del reporte	**Urgencia (Alta, media o baja)**
2025-02-07, 11:30 AM	Alta (impacto en la seguridad del empleado y compromete la información de los clientes).

Paso 2: **Clasificación del Incidente y Severidad**	
Clasificación según severidad	
Severidad (Alta, media o baja)	**Justificación**
Alta	El incidente impide el acceso del empleado a su cuenta de usuario y se compromete la información personal de los clientes .
Tiempo estimado de resolución	
Tiempo estimado	**Motivo**
4 horas	Es necesario realizar una investigación profunda para determinar el alcance del ataque, asegurar la cuenta y prevenir futuros accesos no autorizados.

Paso 3: **Registro del Incidente en Herramienta de Gestión _____**	
Clasificación según severidad	
Severidad (Alta, media o baja)	**Justificación**
Alta	El empleado C no puede acceder a su cuenta y se detectaron actividades sospechosas, como cambios no autorizados y envío de encuestas no autorizadas a nuestros usuarios.
Detalles del ticket	
ID del Ticket	**Prioridad (Alta, media o baja)**
INC-2025-02-07-003	Alta
Categoría	**Descripción**
Seguridad informática / hackeo	El empleado C no puede acceder a su cuenta y se detectan envío de encuestas no autorizadas a los clientes desde su cuenta.
Asignado a	**Fecha de creación**
Equipo de ciberseguridad (Usuario de la herramienta asignado: Analista de Seguridad IT-03)	2025-02-06 09:30 AM

Paso 4: **Desarrollo de una Solución Temporal (Workaround)**
Solución temporal para restaurar el servicio rápidamente (propuesta)
Bloqueo de la cuenta: Se desactiva temporalmente la cuenta del empleado C para evitar más actividades no autorizadas. Notificación al empleado: Se informa al empleado C sobre la situación y se le solicita que no intente acceder al sistema hasta que se resuelva el incidente.
Pasos para implementar el workaround
1. Desactivar la cuenta del empleado C en el sistema interno. 2. Notificar al empleado C sobre el bloqueo temporal de su cuenta. 3. Revisar los registros de actividad para identificar acciones realizadas por el atacante.
Resultado esperado
La cuenta del empleado C queda bloqueada, evitando más actividades no autorizadas mientras se investiga el incidente.

Paso 5: **Resolución del Incidente y Documentación**
Análisis del problema
El equipo de ciberseguridad revisa los logs del sistema y descubre que la cuenta del empleado C fue comprometida mediante un ataque de phishing. El atacante obtuvo las credenciales del empleado C y realizó cambios no autorizados en la configuración de la cuenta.
Solución definitiva
Restablecimiento de credenciales: Se genera una nueva contraseña segura para la cuenta del empleado C. Se habilita la autenticación de dos factores (2FA) para mayor seguridad**.** **Revisión de actividades:** Se revierten los cambios no autorizados realizados por el atacante. Se notifica a los clientes afectados por las encuestas no solicitadas. **Capacitación:** Se programa una sesión de capacitación en ciberseguridad para todos los empleados, enfocada en la identificación de ataques de phishing.
Verificación
Se confirma que el empleado C puede acceder al sistema con las nuevas credenciales y la autenticación de dos factores. Se verifica que no hay más actividades sospechosas en la cuenta. Se asegura que los cambios no autorizados han sido revertidos.

Paso 6: **Cierre del Incidente**	
Cierre del ticket	
Estado	**Fecha de resolución**
Resuelto	2025-02-07, 16:30 PM
Descripción de la solución	**Comentario final**
Se restablecieron las credenciales de la cuenta del empleado C y se implementó la autenticación de dos factores. Se revirtieron los cambios no autorizados y se notificó a los clientes afectados. Se programó una capacitación en ciberseguridad para prevenir futuros incidentes.	El incidente fue resuelto satisfactoriamente. Se recomienda monitorear las cuentas de los empleados y fortalecer las políticas de seguridad.
Registro en _____	
Estado del Ticket	**Resumen**
Cerrado	La cuenta del empleado C fue comprometida mediante un ataque de phishing. Se soluciono restableciendo las credenciales, implementando 2FA y se revirtieron los cambios no autorizados.

5. Conclusión (Mínimo 10 líneas)

La práctica realizada sobre el reporte y resolución de incidentes relacionados con la ciberseguridad, específicamente el hackeo de una cuenta de empleado en una empresa dedicada a la venta de computadoras, permitió comprender la importancia de contar con un protocolo estructurado y eficiente para gestionar este tipo de situaciones. A través de los pasos seguidos (reporte, clasificación, registro, solución temporal, resolución y cierre), se evidenció cómo un enfoque organizado y sistemático es fundamental para minimizar el impacto de los incidentes, garantizar la continuidad del negocio y proteger la información sensible de la empresa y sus clientes. En conclusión, esta práctica permitió consolidar conocimientos y habilidades esenciales para la gestión de incidentes de ciberseguridad, destacando la necesidad de contar con protocolos claros, equipos capacitados y una cultura organizacional orientada a la seguridad y la mejora continua.

6. Referencia Bibliográfica o Electrónica

1. Calvo, J. & et all. (2007).Análisis y diseño de Aplicaciones Informáticas de Gestión.
2. Laudon, K. (2009). Sistemas de Información Gerencial. Administración de la Empresa Digital; 10ª Edición; Edit.

Pearson Prentice Hall.

3. Lutchen, M. (2005). Dirigir las TI como un negocio, Ed. Mc Graw Hill.

Docente Evaluador	Calificación	Firma	Observaciones
MITE. JOSÉ ALBERTO DOMÍNGUEZ SANDOVAL			