Instituto Tecnológico y de Estudios Superiores de Monterrey
TC2036
Implementación de Redes Seguras

Objetivo: Reestablecer la operación de una organización que ha sufrido un ataque cibernético a las configuraciones de los equipos de interconexión.
Subcompetencia de área: SICT0401 Aplica los estándares y normas en el ejercicio de su profesión, manifestándolos como referencia a seguir en la solución de problemas computacionales y tecnologías de información.
Subcompetencia de carrera: STE0302 Selecciona el protocolo de comunicación. Selecciona el protocolo de comunicación de acuerdo a su aplicación.
Subcompetencia transversal: **SEG0402 Argumentación ética**. Soluciona problemas de diversos ámbitos de la vida, con conciencia ética, argumentando desde principios y valores. **SEG0403 Integridad.** Resuelve situaciones de la vida académica, profesional y social, mediante el cumplimiento de leyes, normas y principios éticos.

La madrugada del día de hoy, el guardia de seguridad de la empresa **IT^2 Networking Consulting** reportó actividad sospechosa en el *site* donde se encuentran los servidores y equipos de ruteo de la compañía para la cual estamos realizando un proyecto de diseño y configuración de red. Este proyecto debe entregarse hoy mismo.

El reporte del guardia, del tercer turno, es el siguiente:

Reporte de seguridad		
Hora: 06:30	Lugar: Laboratorio de Infraestructura Computacional.	Reporta: Santiago N.
Descripción detallada del evento observado	Se reporta haber visto a un sujeto de camisa de cuadros de color café, rayas blancas y de gorra azul. Se observa que el sujeto está sentado en una mesa y realiza conexiones con un cable azul a unas cajas de color verde. Las cajas de color verde tienen unos foquitos de color verde encendidos. En ocasiones se ven parpadear. El sujeto se levanta de su silla y se retira a las 05:45. Se observa que deja la puerta abierta y no se lleva nada del lugar.	

El director de la empresa recibió el reporte a las 8:00 am y después de leerlo, decidió pasar el caso a sus consultores estrella para que revisen las configuraciones de los equipos de interconexión y corrijan lo que tengan que corregir para garantizar la funcionalidad de la red.

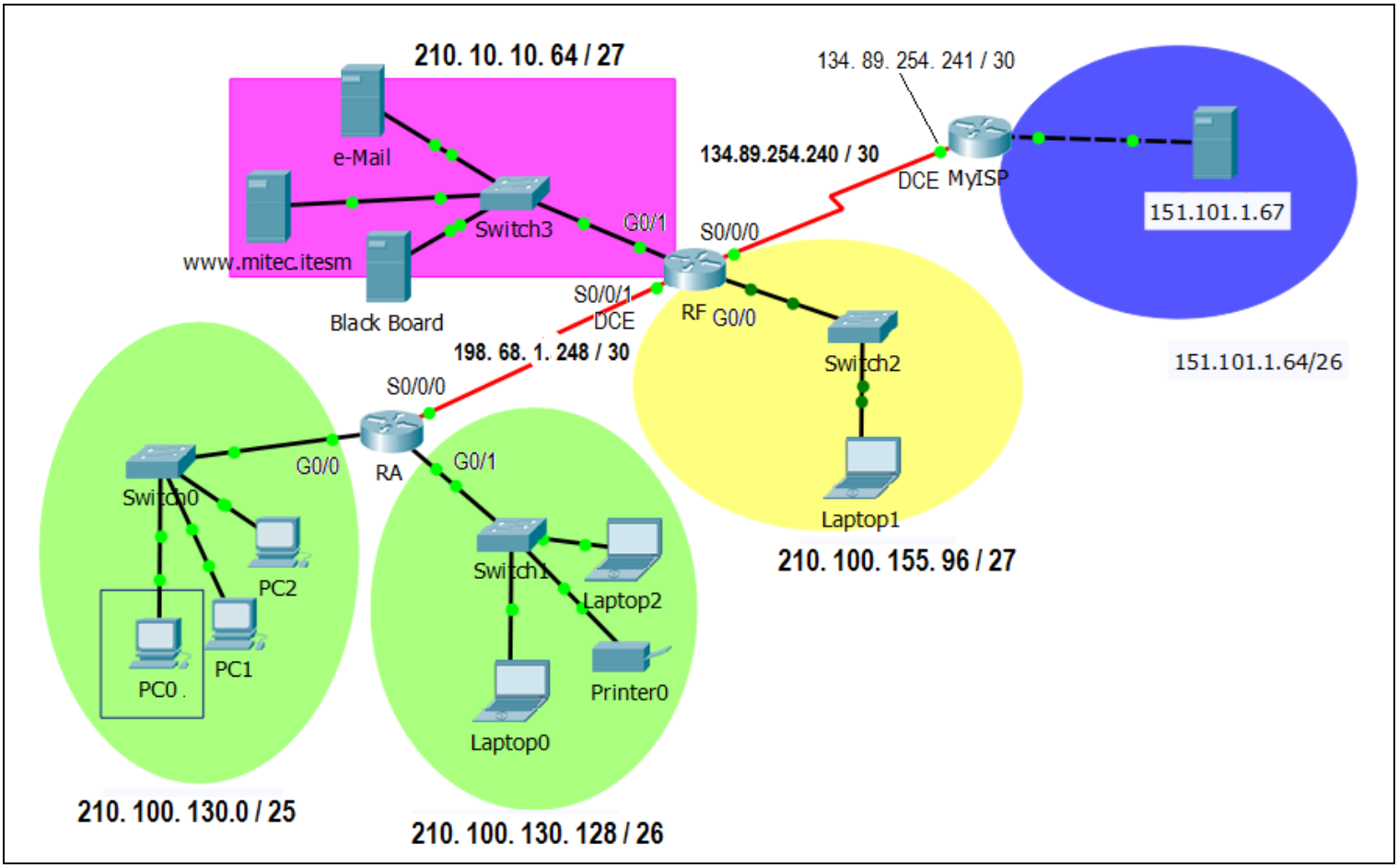
La hora de entrega final de tu solución se ha concretado para **hoy mismo**, por lo que el trabajo que debes realizar debe quedar resuelto en tiempo y forma.

Tú objetivo el día de hoy es revisar las configuraciones recuperadas y corregir la configuración de un conjunto de equipos de interconexión (routers y switch) y recuperar la conexión con Internet desde cualquier equipo de la LAN.

Revisa todas las configuraciones recuperadas de cada equipo de interconexión (routers y switch) y utiliza la gráfica que se proporciona, como parte de la documentación de la red, para realizar las adecuaciones necesarias y tener a tiempo el proyecto funcional.

Para reconstruir las configuraciones de las interfaces de los equipos de interconexión, puedes auxiliarte de la información de los equipos terminales ya que éstos no fueron alterados.

Confiamos en tus competencias desarrolladas hasta este momento y tu tenacidad para resolver problemas, por lo que estamos seguros que recuperar las configuraciones de los equipos de interconexión será un reto que resolverás satisfactoriamente en el tiempo asignado.



Los archivos a los que tienes acceso, contienen el diseño de red de la gráfica mostrada y el archivo de configuraciones que se pudo extraer de cada router. En este momento, y por seguridad, los equipos de interconexión (routers y switch) de la red local están vacíos.

a) Escribe en cada renglón de la Tabla 1 (exclusivamente notación punto decimal) las direcciones **IP** de cada una de las interfaces de los routers y la **Máscara** correspondiente que darán servicio a este esquema de direccionamiento.

Router	S0/0/0	S0/0/1	G0/0	G0/1
MyISP	134. 89. 254. 241 ---------- 255. 255. 255. 252	**No se usa** ---------- **No se usa**	**Ya Configurado** ----------	**No se usa** ---------- **No se usa**
RFrontera	134. 89. 254. 242 ---------- 255. 255. 255. 252	----------	----------	**210.10.10.94** ---------- **255.255.255.224**
RA	----------	**No se usa** ---------- **No se usa**	----------	----------

Tabla 1

b) Se te pide utilizar el formato **RCA** para realizar un análisis post-mortem, documentar todo lo identificado como incorrecto y documentar las acciones emprendidas para reconstruir las configuraciones. Utiliza toda la información disponible con la que cuentas para documentar el análisis post-mortem.

Puedes encontrar más detalle de cómo conducir un análisis causa-raíz en el siguiente enlace https://www.thecompassforsbc.org/how-to-guides/how-conduct-root-cause-analysis.

Formato RCA (Root-Cause-Analysis)

1. Información General del Incidente

En esta sección documenta el "cuándo sucedió", "a qué hora se atendió y a qué hora terminó". Notifica cuál fue el impacto para la organización y la urgencia de atenderlo.

Impacto	Alto/Bajo/ sin impacto	Prioridad	Alto/medio/bajo
Urgencia	Muy alta/ crítica		
Reportado por	Persona1	Fecha Incidente	24-09-20
Atendido por	Persona2	Fecha Reporte Inicial	25-09-20
Responsable del incidente	Persona3	Fecha Cierre Reporte	28-09-20

2. Historial de Revisiones

Este documento tiene un control de revisiones.

Revisión	Descripción	Autor	Fecha
1	Reporte inicial del incidente	Persona que inicia la escritura del documento.	25-09-20
2	Modificaciones en análisis de la causa raíz.	Persona que realiza la modificación.	25-09-20
3	Modificaciones en resumen ejecutivo.	Persona que realiza la modificación.	26-09-20
4	Reporte final del incidente.	Persona que termina la escritura del documento.	28-09-20

3. Detalle del Incidente

Dimensiona el incidente para que se pueda cuantificar su impacto.

Equipos Afectados:	Core cisco (equipos/servicios con falla)
Inicio del Incidente (Fecha y Hora)	24/09/2020 09:00:00 p. m.
Fin del Incidente (Fecha y Hora)	25/09/2020 11:10:00 a. m.

Duración del impacto en servicios (Días/Horas/Minutos)	14:10:00
Descripción del Incidente	Ejemplo: Se recibe reporte de falla en el core cisco
Usuarios Afectados	Planta:1900 Cliente: 1900 Colaboradores: 200
Equipos involucrados	Operaciones/infraestructura/monitoreo/seguridad, (departamentos que estuvieron en el incidente)

4. Resumen Ejecutivo

Resume en un pequeño párrafo el incidente.

Falla en una línea de producción que afectó al cliente X y que fue restablecida a las 13:45 hrs.

5. Narrativa del Incidente

Historia cronológica de sucesos. Trata de narrar, personas, eventos, sucesos e hilar el impacto de lo que ocurrió, así como las medidas que fueron sucediendo para reactivar la línea de producción, la red, el proceso, monitoreo, etc.

No.	Fecha/Hora	Descripción
1		
2	25 sep 2020 11:00	Se detecta la falla.
3	11:00	Se reporta incidente
4	11:10	Cambió y se modificó equipo1
5	11:30	La persona 1 reportó otra falla
6	11:50	La línea de producción se restablece.
7	12:10	Cierre del incidente.
8		
9		
10		
n		

6. Análisis Causa Raíz

En esta sección de los ¿Por qué? Generalmente son cinco (o más) ¿Por qué? Esto debido a que una pregunta lleva a otra sucesión de hechos que deben de ser analizados o trabajados en acción de corregir la causa de raíz.

No.	Pregunta	Descripción
0	¿Qué?	Falla en …
1	¿Por qué?	Cambio no programado ..
2	¿Por qué?	Falta de presupuesto
3	¿Por qué?	Falla en un punto único de distribución
4	¿Por qué?	Equipo de alimentación falló
5	¿Por qué?	No existe monitoreo
n	¿Por qué?	

7. Acciones de seguimiento

En este punto debes de registrar Acciones que planteas y que van a apoyar a resolver o mitigar la afectación raíz. Se compone de acciones, responsables, fecha compromiso de cumplimiento, el estatus es el proceso en el que se encuentra con base en la fecha actual con respecto a la prometida.

No.	Tarea	Responsable	Fecha Compromiso	Estatus
1	Restablecer línea de producción…	REDES	25 feb	TERMINADO
2	Generación de controles de cambios….	REDES	25 feb	NO INICIADO
3	Generar orden de comprar, adquirir ….	DEPARTAMENTO DE COMPRAS	2 marzo	EN PROCESO
4	Entregar políticas de cambios…..	MONITOREO	5 marzo	EN PROCESO
3				
4				
N				

Después de revisar los videos de las cámaras de seguridad, se pudo determinar que la última persona en salir del *site* es un empleado que sostiene haber borrado accidentalmente las configuraciones pues estaba muy agotado y quizá sin darse cuenta guardó una configuración previa.

El Director General de la empresa está por tomar una decisión sobre la continuidad laboral del empleado en la organización, sin embargo requiere de toda la información disponible para proceder con una decisión.

El empleado es tu conocido desde hace algunos años, sabe que estás trabajando en la recuperación de las configuraciones y el análisis post-morten, y te ha compartido que además de necesitar del trabajo, requiere de las horas extras para poder hacer frente a un compromiso económico que acaba de contraer, por lo que pide tu ayuda para que modifiques a su favor, el reporte que entregarás como análisis post-morten y así evitar que sea despedido de la organización.

Esta petición te pone en un dilema, pues sabes que el empleado necesita del empleo y tú debes entregar el reporte tan pronto como sea posible (ASAP).

c) Argumenta, desde el punto de la Ética, la decisión que tomarás sobre su petición y qué harás con el reporte final que se te solicita. ¿Qué argumentos utilizarás para dar una respuesta a tu conocido? ¿Cuáles son las consecuencias de acceder a la petición de tu compañero?