Mejora de la seguridad mediante un modelo de incidencias en tiempos de Pandemia

MPEDT Hilda, Díaz Rincón, Dr. José Antonio Navarrete Prieto, M. A. Iliana G. Laguna López de Nava, Fátima Paloma Carbajal Miranda, Dr. Eric Hernández Castillo

[a] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, c_computo_sie@hotmail.com, Tlalnepantla de Baz, Estado de México, México
[b] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, posgrado_ittla@yahoo.com.mx, Tlalnepantla de Baz, Estado de México, México
[c] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, ilianaxim@hotmail.com, Tlalnepantla de Baz, Estado de México, México.
[d] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, c_computo_sie@yahoo.com.mx, Tlalnepantla de Baz, Estado de México, México.
[e] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, eric.hc@tlalnepantla.tecnm.mx, Tlalnepantla de Baz, Estado de México, México.

Resumen

El incremento de los ciberataques en tiempos de Pandemia en las instituciones financieras requiere de integrar una seguridad proactiva en las comunicaciones a través del uso de diversas estrategias siendo una de ellas el uso de un modelo de incidencias para la detección de situaciones que ocurren en las mismas. Como parte de un programa de seguridad se aplicó un monitoreo de 24 hrs y los siete 7 días de la semana a partir del 15 de marzo de 2021 al 9 de julio de 2021 de un total de 110 equipos para verificar el nivel de seguridad actual, al término del periodo y la aplicación del modelo, se realizó un análisis de las diferentes incidencias ocurridas en los mismos siendo la de mayor incidencia el control de puertos en los equipos de acceso, por lo que se integraron medidas de mejora de seguridad con la utilización de la autenticación con la norma 802.1X y MAC (código de autenticación de mensaje) en el Servidor Radius con el apoyo de un software de monitoreo como es la plataforma Centro de gestión inteligente (IMC Intelligent Management Center) obteniendo con ellos una disminución en las incidencias. Se aplico una investigación descriptiva-propositiva. Los resultados obtenidos indican que los beneficios de implementar la estrategia con base en el análisis de puertos mejoro en un 30% los tiempos de respuesta de atención al incidente.

Palabras clave—autenticación, conectividad, incidencia, puerto, seguridad.

Abstract

The increase in cyber-attacks in times of Pandemic in financial institutions requires the integration of proactive security in communications through the use of various strategies, one of them being the use of an incident model for the detection of situations that occur in them. As part of a security program, a 24-hour monitoring was applied seven days a week from March 15, 2021 to July 9, 2021 of a total of 110 devices to verify the current security level. At the end of the period and the application of the model, an analysis was made of the different incidents that occurred in them, the most common being port control in the access devices. 1X and MAC (message authentication code) in the Radius Server with the support of monitoring software such as the Intelligent Management Center (IMC Intelligent Management Center) platform, thus obtaining a decrease in incidents. A descriptive-propositive research was applied. The results obtained indicate that the benefits of implementing the strategy based on port analysis improved incident response times by 30%

Keywords— *authentication, connectivity, incident, port, security.*

1. INTRODUCCIÓN

La evolución tecnológica ha permitido a los países maximizar su interconectividad y operaciones comerciales, pero a la vez trae consigo nuevos riesgos y amenazas y con ello grandes desafíos para las áreas de seguridad. En la actualidad existen amenazas latentes que buscan atacar las redes institucionales para afectar su continuidad, extraer información y mal utilizar los recursos de red, por lo cual las redes empresariales se encuentran ante nuevos retos, como es el aseguramiento del acceso de usuarios internos y externos a los recursos de esta, debido a que a través de la red, fluye información que debe llegar a los destinatarios adecuados, cuidando su confidencialidad y garantizando el acceso oportuno a la misma.

Según el informe Estado de la ciberseguridad en el sector El informe de la Organización de los Estados Americanos (OEA) del 2019 revela que el 43% de las grandes entidades financieras de México sufrieron incidentes cibernéticos el último año, la OEA presentó el 11 de julio del 2019 el informe "Estado de la Ciberseguridad en el Sistema Financiero de Mexicano", donde se analizó la seguridad digital de 240 entidades financieras mexicanas de diferentes sectores como parte de su tarea de fortalecer las capacidades y nivel de conciencia sobre las amenazas cibernéticas en América Latina y el Caribe, Entre los principales hallazgos, el estudio señala que: El 43% de las grandes entidades financieras sufrieron incidentes cibernéticos en el último año.

2 de cada 10 entidades financieras sufrieron incidentes cibernéticos relacionados con malware o código malicioso cada día. El costo total de respuesta y recuperación ante incidentes de seguridad digital oscila entre los 2,3 millones de dólares al año para las entidades grandes y los 317 mil dólares para las pequeñas. Este informe apoyo de la Comisión Nacional Bancaria y de Valores de México y el Gobierno del Reino Unido [1].

[2] José Cisneros, presidente del consejo de seguridad de seguridad informática de la Asociación Mexicana De Instituciones Bursátiles, menciono las nuevas tendencias digitales se hacen cada día más palpables, como un catalizador de estas se encuentra la pandemia, al limitar la interacción y obligando a las empresas a trabajar a través de medios digitalizados en mayor medida, lo cual ha desencadenado un aumento en ciberataques en un 56% a nivel mundial, explicó en el Foro Forbes Ciberseguridad.

Es por ello por lo que el cibercrimen se perfila para ser uno de los principales desafíos de la próxima década. No actuar contra él puede significar la desaparición de cientos de organizaciones empresariales.[3]

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL sus siglas en inglés) es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general [4]. ITIL tiene como objetivo proporcionar a los administradores de sistemas de tecnologías de información (TI) las mejores herramientas y documentos que les permitan mejorar la calidad de sus servicios, es decir, mejorar la satisfacción del cliente al mismo tiempo que alcanzan los objetivos estratégicos de su organización. Para esto, el departamento de TI debe ser considerado como una serie de procesos estrechamente vinculados. Pragmáticamente, ITIL cumple con la lógica de hacer que la TI sea útil para los empleados y clientes en lugar de lo opuesto [5].

En lo que refiere a los servicios que presta la Tecnología Informática se pretende utilizar una herramienta conocida como ITIL que corresponde a un marco de referencia de mejores prácticas, que a través de un plan de implementación desea mejorar notablemente los servicios que presta una organización en cuanto a recepción de incidentes, identificación, manejo, asignación de un responsable de las acciones a tomar, hacer seguimientos a los casos presentados, documentarlos, darles una solución de manera ágil y oportuna, restablecer un servicio interrumpido y realizar análisis pertinentes para evitar futuras situaciones similares a las ya registradas, si reinciden tener un acción rápida a tomar entregando un producto que cumple con las exigencias del cliente. [3]

En este caso de estudio se propuso la utilización del marco para la implementación de ITIL en lo que respecta a la gestión de las incidencias y su impacto en los recursos de la red con la utilización del modelo de incidencia de ITIL v3.

ITIL v3 ayuda a las organizaciones a adoptar un punto de vista más estratégico que abarca todo el ciclo de vida del servicio. Este tipo de enfoque reporta ventajas: favorece la integración de la estrategia de negocio

Las empresas que buscan la perfección saben que los problemas, los contratiempos y los retrasos son parte del negocio, y deben aprender a gestionarlos [6] y [7] menciona que toda empresa de servicios necesita la Gestión de Incidencias para prevenir o restaurar tan pronto como sea posible cualquier interrupción o reducción no planificada en la calidad de su servicio. Sin embargo, se debe ser consciente de los desafíos y riesgos de la Gestión de Incidencias con el fin de garantizar la mejor operación de servicio.

Considerando lo anterior se enumeran las situaciones a resolver:

1. Controlar de manera correcta la configuración de los puertos en los switches.
2. Monitorear los puertos de cada switch con el uso de un software especializado.
3. Identificar modificaciones en los equipos y en los puertos con algún alertamiento o aviso.

El tipo de investigación que se llevó a cabo es descriptiva-propositiva ya que "parte de un diagnóstico, se establece metas y se diseñan estrategias para alcanzarlas" [6]

En [4] se define al modelo como la "representación de un sistema, proceso, servicio de Tecnología de Información, como un elemento de configuración etc. empleado para ayudar a entender o predecir comportamientos futuros.". La incidencia para el libro de Soporte del Servicio de ITIL es "cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad de este" [9] y finalmente servicio en ITIL se define como "Un servicio es un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados" [9].

Finalmente, debido al problema mundial de la pandemia las Instituciones Financieras establecen el trasladar a sus trabajadores al denominado "Trabajo en casa" (HOME OFFICE) y fortalecer la seguridad en sus áreas de servicio a clientes por lo que al analizar los riesgos se determinó que se debería de mejorar la seguridad aplicando lo que ITIL v3 indica en su prácticas para la Gestión de Incidencias considerando utilizar un modelo de incidencias el cual se integró a la estrategia de Monitorización de puertos y la plataforma de IMC.

2. DESARROLLO

Dentro de un mercado ultra competitivo, los clientes requieren respuestas rápidas a sus problemas, y las empresas, soluciones definitivas que minimicen el impacto negativo en su negocio.

La gestión de incidentes tiene como objetivo minimizar los impactos negativos en las empresas que reportan incidentes de soporte técnico y corregir los errores. Además, implementar la gestión de incidentes de forma correcta puede mejorar de forma considerable los procesos de mesa de ayuda, ya que en ocasiones la acumulación de información produce dificultad al identificar los eventos solucionados, esto ocasiona pérdida de tiempo en la solución de incidentes repetitivos; actualmente en el control de incidencias y requerimientos, se maneja en archivos propios de cada usuario, como consecuencia se descentraliza la información y provoca observaciones por parte de auditoría informática, tanto interna como externa. [10]

El modelo de incidencia de acuerdo [11] incluye los siguientes pasos a seguir como son: responsabilidades: quién debe hacer qué, plazos para la realización de las actividades, procedimientos de escalado: quién debería ser contactado y cuando. En [11] define al modelo como la "representación de un sistema, proceso, servicio de Tecnología de Información, como un elemento de configuración etc. empleado para ayudar a entender o predecir comportamientos futuros." y donde la incidencia para el libro de Soporte del Servicio de ITIL es "cualquier evento que no forma parte de la operación estándar de un

servicio y que causa, o puede causar, una interrupción o una reducción de calidad de este" [10] que además define al servicio como "un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados".
Un modelo de incidente es una forma de predefinir los pasos que deben ser tomados para manejar un proceso que está tratando con un tipo particular de incidente, en una forma acordada. Las herramientas de soporte pueden ser usadas para gestionar el proceso requerido, esto asegura que los incidentes comunes sean manejados de una manera predefinida y dentro de unas escalas de tiempos dadas. [11].
El modelo de incidentes de acuerdo con [11] debe incluir lo siguiente

- Los pasos que deben ser tomados para manejar los incidentes
- El orden cronológico en el que estos pasos deben ser tomados con cualquier dependencia o proceso predefinido.
- Responsabilidades. Quién debe de hacer qué.
- Escalas de tiempo y umbrales para la terminación de las acciones.
- Procedimiento de escalado. Quién debe ser contactado y cuándo.
- Y cualquiera de las actividades necesarias de evidencia y preservación.

[12] indica que el objetivo primordial de este proceso es devolver a la normalidad las operaciones en el servicio lo más rápido como sean posibles. Un incidente se presenta cuando algo que estaba funcionando bien deja de hacerlo. También se consideran incidentes a todas aquellas fallas de elementos de configuración que todavía no hayan afectado a un servicio.

[13] señala que el proceso en la gestión de las incidencias cubre todos los tipos de incidencias que se vayan a presentar durante el normal desarrollo de las funciones de un proceso, ya estos sean fallas, consultas o preguntas que hacen los usuarios, generalmente se dan con una llamada al área de centro de servicios del usuario o bien al personal encargado, el cual sería el técnico especialista, también son detectadas de forma automática por las herramientas que se usan para monitorizar los eventos.
Por otro lado, para [11], el principal objetivo que se da en el proceso para la Gestión de Incidentes es el de regresar a la situación regular lo más pronto posible y disminuir el impacto que se da en el proceso de la organización.
En muchas circunstancias se llega a confundir un incidente crítico con un problema, pero un incidente siempre va a ser un incidente; es probable que vaya a incrementar su impacto, o bien su prioridad, eso sí, nunca va a llegar a ser considerado como un problema de TI. Un problema es la forma oculta a uno o muchos incidentes y siempre va a ser diferenciado.
Por lo que considerando lo que indica ITIL se diseñó y aplico el siguiente modelo de incidencias que se muestra en la figura 1.

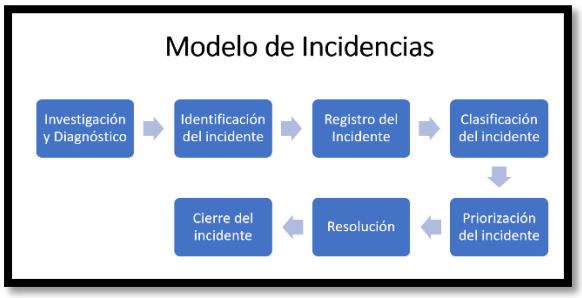

Figura 1. Modelo de Incidencias aplicado considerando lo que indica ITIL V3.
Fuente Elaboración propia

El modelo contiene las siguientes etapas como son:

Investigación y Diagnóstico.
Si la incidencia hace referencia a un fallo en el sistema, lo más probable es que se necesite investigar la causa del fallo. Las tareas más comunes dentro de esta actividad son las siguientes:

- Establecer exactamente qué es lo que no funciona correctamente y para qué secuencia de acciones del usuario.
- Establecer el impacto potencial de la incidencia.
- Determinar si la incidencia está producida después de la implementación de un cambio.
- Buscar en la base de datos de conocimiento (base de datos de errores conocidos, registro de incidencias) posibles soluciones y/o soluciones alternativas.

Identificación: Las incidencias pueden ser cualquier falla o interrupción del servicio de TI o en la configuración de ítems/activos. La entidad deberá de intentar rastrear los elementos importantes, de forma que los errores se puedan identificar lo antes posible y de esta manera poder comenzar el proceso en la gestión de incidencias. En el caso óptimo, todas las incidencias se logran resolver antes de que estos traigan consecuencias sobre los usuarios.
Registro: Las incidencias que se presenten deberán de quedar registradas con sus detalles, esto incluye las fechas y la hora
Clasificación: Los códigos de clasificación se deben utilizar apropiadamente para las incidencias
Priorización: El código de prioridad es la asignación correcta que se debe dar en una incidencia. Los gestores y las herramientas de apoyo emplean este código para establecer cómo se deberán de tratar las incidencias. Generalmente, las prioridades que se vayan a dar en una incidencia se podrán precisar a partir de:

- Impacto: esto precisará la importancia de la incidencia dependiendo cómo esto va a lograr afectar en los procesos del negocio o del número total de los usuarios.
- Urgencia: esto depende del máximo tiempo en la demora que va a aceptar el usuario para llegar a la solución de su incidencia reportada o por el nivel del servicio que se proporcione.

Al incluir la utilización de IMC se ahorró tiempo en el diagnóstico de equipo ya que es una plataforma que permite monitorear en tiempo real a los equipos y aplicaciones que están consumiendo recursos de red en un tiempo determinado, la cual posee su propio servidor que permite que cualquier usuario, una vez autenticado, pueda acceder a los equipos de forma remota con cualquier navegador.
Está desarrollado para plataformas Unix y Windows. Algunos de los protocolos soportados son: TCP/UDP/ICMP, RARP, ARP es capaz de detectar direcciones IP duplicadas. Ofrece características y funciones diseñadas para obtener una gestión completa de la infraestructura de red, ver figura 2.

Aplicando el Modelo de Incidencias.
Se integro información los meses de enero a junio del 2021, correspondiente a los incidentes reportados por el equipo de soporte técnico el cual reporto un total de 220 incidentes críticos. Por lo que se buscó de forma estratégica una alternativa para mejorar el tiempo de respuesta a estos incidentes siendo una de ellas la que se muestra en este caso de estudio

Figura 2. Ventana Principal de IMC.
Fuente: Software IMC

Posteriormente se inició con la identificación de la incidencia que tuvo mayor frecuencia, por lo que es importante indicar que para este caso de estudio se utilizó un software especializado denominado IMC como prueba para verificar su eficacia en el apoyo del monitoreo realizando un uso diario para validad los reportes de alertas que se obtienen de él, ver figura 3.

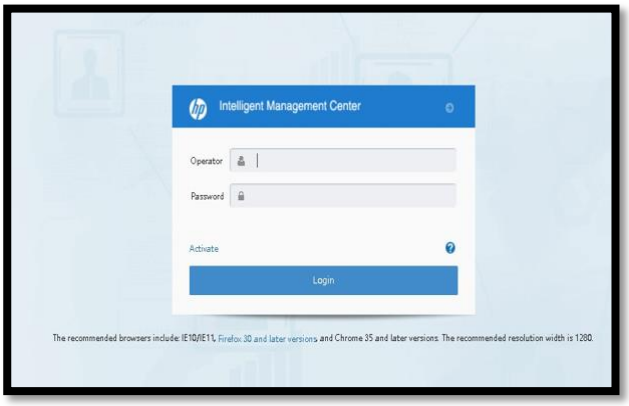

Figura 3. Inicio de Sesión IMC. Fuente: Elaboración propia con base en plataforma IMC

Los alertamientos obtenidos se validan realizando verificación de las alertas mediante el Software Putty, en el cual se ingresa Usuario y Contraseña personal (la conexión se realiza mediante el uso de SSH (Secure Shell Protocol) o protocolo de seguridad Shell, el cual es un protocolo de administración remota que puede ser utilizado mediante wi-fi o red LAN (Red de área local o Local Area Network por sus siglas en inglés) al ingresar al Switch se revisa el estatus de la interfaz si se encuentra arriba o abajo (up o down), que no tenga CRC (verificación de redundancia cíclica o sus siglas en inglés cyclic redundancy check), también se busca si hay algún tipo de afectación en el log el cual puede indicarnos la falla que pueda tener la interfaz si es que la hubiera.

Posterior a la identificación de la incidencia, se realiza el registro de la misma, considerando que además se revisa que el equipo se encuentre funcionando de forma correcta, validando los servicios como: las fuentes de poder, los ventiladores, la temperatura, en los equipos de acceso, los módulos que se encuentren bien, que no existe falla de POE en alguna interfaz, que no cuenten con loop (ciclo), que las fibras se encuentren UP y sin CRC y por último la conexión al Servidor Radius con un ping. Esto se realiza para verificar y validar que la incidencia está siendo correcta, ver figura 4.

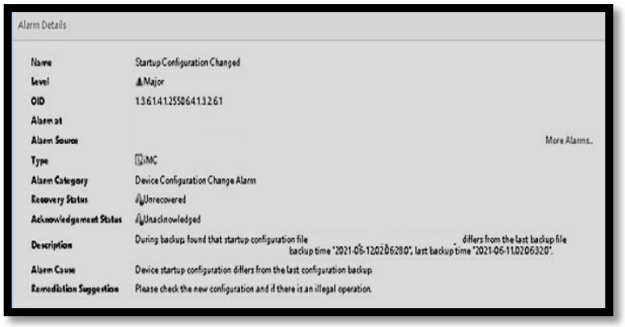

Figura 4. Detalle de la alerta.
Fuente: Elaboración Propia

Continuándose con la etapa de clasificación del incidente, para la cual se auxilia de una bitácora de trabajo especificando el motivo o causa por el cual se establece la alerta y se establece la categorización de acuerdo a la incidencia, revisando esta se observó que la de mayor ocurrencia fue la que se refiere a conectividad por lo que se establece realizar un diagnóstico integrando un análisis de puertos y de red, cuyo objetivo es es identificar la organización de las direcciones IP, los anfitriones y los puertos para determinar correctamente las ubicaciones del servidor vulnerables y diagnosticar los niveles de seguridad.
Al realizar este análisis de red en profundidad se integra una lista de anfitriones activos, obteniendo en este identificar los puertos abiertos de la red en donde el riesgo mayor es que permitirían accesos no autorizados, categorizando los estados como son: abiertos o cerrados.
Los puertos abiertos indican que el servidor o la red de destino acepta activamente conexiones o datagramas y ha respondido con un paquete que indica que está escuchando.

También indica que el servicio utilizado para el análisis (normalmente TCP o UDP) está en uso. Ver figura 5.

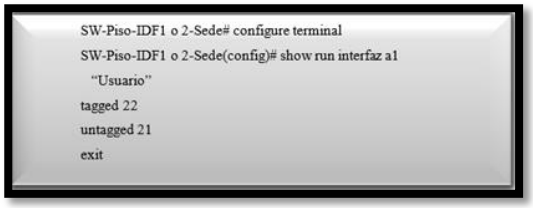

Figura 5. Puerto sin Seguridad
Fuente Elaboración propia

Puertos cerrados: Los puertos cerrados indican que el servidor o la red ha recibido la solicitud, pero no hay ningún servicio «escuchando» en ese puerto. Un puerto cerrado sigue siendo accesible y puede ser útil para mostrar que hay un anfitrión en una dirección IP, ver fig 6. La línea de comando que permite dar autenticación al puerto es aaa port-access authenticator y permite la salida a la red. La segunda línea aaa port-access authenticator clients-limit 3 nos permite, que al nodo se puedan conectar por LAN tres equipos diferentes y se les brinda el servicio de LAN, si se excede el límite permitido el puerto se bloquea automáticamente y dejará de dar servicio. Ver figura 6.

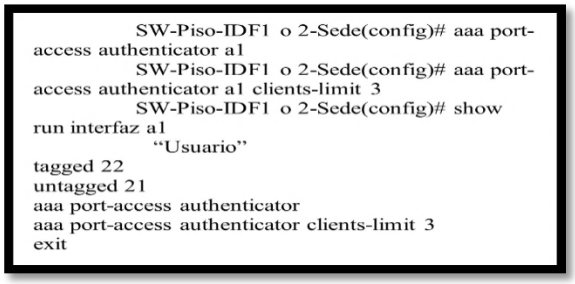

Figura 6. Puerto Cerrado.
Fuente: Elaboración propia

Para validar que el puerto está autenticando, se ingresa el siguiente comando que muestra la figura 7.

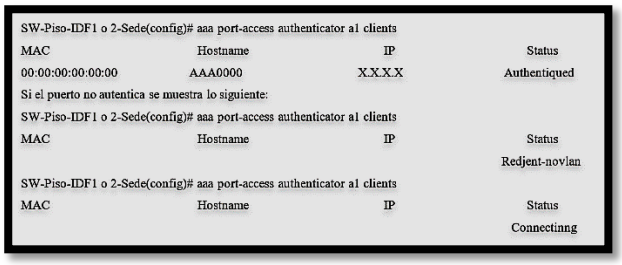

Figura 7. Validación de autenticación.
Fuente Elaboración propia

Posterior a este se hace uso nuevamente de la plataforma IMC en donde en la revisión se realiza en todas las alertas que salgan en el IMC y se recuperan, en caso de haber algún tipo de afectación se procede a documentarla y hacerla llegar al Cliente mediante correo explicando lo que sucede, ver fig. 8

Antes de recuperar las alertas se procede a sacar un recorte de los alertamientos y se documenta en un archivo el cual muestre las alertas y el cuadro comparativo si es que se realizó algún cambio en la configuración del switch. Ver figura 8.

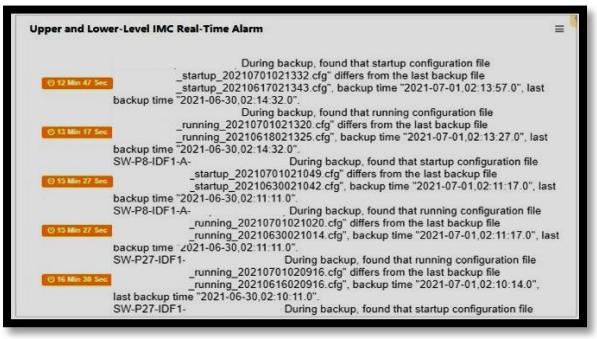

Figura 8. Ejemplo de Alertas obtenido de la plataforma IMC

La arquitectura IEEE 802.1X está compuesta por tres entidades funcionales:

El suplicante que se une a la red.
El autenticador que hace el control de acceso.
El servidor de autenticación que toma las decisiones de autorización.

Toda vez que se han analizado las incidencias en puertos se procede a mejorar la seguridad en la autenticación por 802.1X y MAC, como se muestra en la figura 9.

El protocolo de autenticación IEEE 802.1X (también conocido como Port-Based Network Access Control) es un entorno desarrollado originalmente para redes de cable, y posee mecanismos de autenticación, autorización y distribución de claves y además incorpora controles de acceso para los usuarios que se unan a la red.

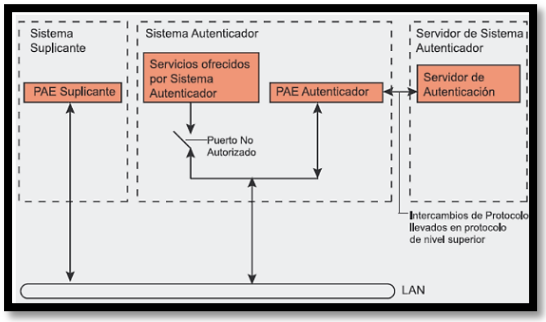

Figura 9. Modelo de IEEE 802.1X según la especificación IEEE 802.1X.

.

En los puertos de los equipos de acceso (Capa 2 del modelo OSI significa Open Systems Interconnection o, en español, Interconexión de Sistemas Abiertos.) se aplicó una configuración mediante la cual los puertos deberán autenticarse por 802.1X o MAC.

La configuración se realiza en base a las necesidades de los dispositivos, ya que pueden ser estaciones de trabajo con Windows y Extensión de teléfono, los cuales se autentican por 802.1X, otros dispositivos pueden tener Windows y Ubuntu (Máquina virtual) la configuración que requieren son por doble autenticación 802.X, MAC la Máquina virtual dará servicio por medio de la MAC Virtual y 802.1X proporcionará servicio a la Extensión de teléfono, las

impresoras darán el servicio algunas por 802.1X o Mac dependiendo del área en que se encuentre. Los Access Point, Cajeros automáticos, Sensores y equipos de videoconferencia darán servicio por MAC. Las cámaras se encontrarán Excluidas sin ningún tipo de autenticación, para proporcionas la seguridad correcta se crearán ACLs (Lista de Control de Accesos) para proporcionar la seguridad que solicita la Institución Financiera.

La seguridad es diferente en cada puerto, ya que cada necesidad es distinta y requieren diferentes formas de autenticación, para lo cual se crea un archivo llamado Control de acceso a la red (NAC). Ver tabla 1.

Tabla 1. Control de Puertos

Piso	IDF 1 A	IDF1B	IDF2A	IDF2B
802.1x	0	0	0	0
OPEN	0	0	0	0
EXCLUIDO	0	0	0	0
DOBLE	0	0	0	0
MAC-BASED	0	0	0	0
TOTAL DE PUERTOS	0	0	0	0

Fuente: Elaboración Propia

En esta tabla se muestra la cantidad de puertos que hay por 802.1X, Open, Excluido, Doble, Mac-Based, donde 802.1X: representa que los puertos estén cerrados o por 802.1X que significa lo mismo, esta seguridad indica que los puertos ya no sean tan vulnerables porque se tienen que autenticar al servidor Radius para tener servicio de Red. Donde **OPEN**: es utilizado para dar salida a una Vlan o forzar el servicio de una Vlan, OPEN es cuando se solicita que se quite la seguridad que tenga un puerto para carga de certificados o pruebas que tengan que realizar las demás áreas. **EXCLUIDO**: este término es para indicar que los puertos no cuentan con ningún tipo de seguridad, esto es lo que se intenta evitar porque el puerto, al estar sin seguridad, se puede conectar cualquier computadora ajena a la institución financiera y obtendría navegación sin restricciones. **DOBLE**: es utilizado cuando los puertos requieren de una doble autenticación por 802.1X y **MAC-BASED.** Esto quiere decir que 802.1X autentica la estación de trabajo que es una computadora con teléfono y MAC-BASED, autentica la máquina virtual que está instalada en la computadora con una dirección física virtual. Así es como se consigue la doble autenticación. MAC-BASED: autentica los puertos con la dirección física de los equipos (MAC), solo se consigue la autenticación si la dirección física se encuentra dada de alta en el Servidor ISE, el cual se comunicará al servidor Radius para dar la autenticación y proporcionar el servicio de Red. Ver tabla 2.

Tabla 2. Identificación de switches

SWITCH-PISO-IDF-A o B-SEDE – IP X.X.X.X			
Puerto	Etiqueta	VID	Modo NAC
A1			
A2			
A3			
A4			

Fuente: Elaboración Propia

Esta tabla está dividida en 4 columnas, las cuales empiezan en la fila 2, ya que en la fila 1 se encuentra SWITCH-PISO-IDF-A o B-SEDE – IP X.X.X.X, esto ayuda a identificar más rápido en que IDF se encuentra y también por la propia IP.

PUERTO: es la primera columna y está representada con la letra del módulo en el que se encuentra. Los puertos en el módulo A y B solo llegan hasta el 20, los dos puertos restantes son utilizados para las fibras, pero esos no se anotan en el archivo, del módulo C hasta la letra N todos son de 24 puertos.

ETIQUETA: es la columna 2 y es el nombre que tienen asignados los puertos para identificar de qué son cada uno, algunos tienen el nombre de USUARIOS, ACCESS-POINT, IMPRESORAS, TELEFONO y CÁMARAS.

VID: es la columna 3 y es la Vlan o Vlans que tenga el puerto, por lo regular tienen asignadas dos, en casos especiales puede tener 3 o 4 y los que tienen una sola Vlan es porque solo requieren ese servicio y por lo regular son los ACCESS-POINT, IMPRESORAS y CÁMARAS.

MODO NAC: es la columna 4 y es como se describe la seguridad que tiene cada puerto, como se muestra en la Tabla 1.

Para apoyo de la gestión se creó también una bitácora la cual se muestra en la tabla 3. Esta se utilizará para llevar el registro de las actividades que requieran alguna configuración de un puerto. Los apartados más importantes son: petición por, con el que se sabrá quién es la persona que solicita alguna configuración, actividad requerida, se explicara qué es lo que se solicita y para que, si alcanza LAN se comentará con un sí, cuando se pueda realizar la configuración por Putty, nombre del ingeniero que realiza la configuración o la actividad que se le solicite y las observaciones, si fue posible realizar la configuración porque se dio la autorización o que no procedió la solicitud y por qué no procedió

Tabla 3. Bitácora de control de incidencias

Fecha	Hora	Ubicación (SEDE)	Piso	Petición Por	Actividad Requerida	LAN	Nombre de Ingeniero	Observaciones

Fuente: Elaboración Propia

Para realizar pruebas se tiene acceso a switches y servidor de IMC, el cual es controlado, ya que para poder ingresar a ellos se tendrá que contar con los permisos de un usuario y contraseña específicamente creado para cada usuario.
La autenticación por 802.1X y autenticación por MAC actúan sobre redes de computadora, concretamente en redes de área local (LAN) y redes de área metropolitana (MAN).
Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso al puerto si la autenticación falla.
En un sistema de control de dispositivos de red, este se basa en los puertos, para cada empleado se tiene dispuesto un puerto, si no cuenta con la seguridad adecuada el puerto se valida como no autenticado y permanecerá cerrado.
Estas autenticaciones utilizan el servidor RADIUS, 802.1 X realiza la petición por autenticación, autorización y anotación (AAA), consultando con el servidor de bases de datos que la información del empleado sea válida y otorgando el acceso a LAN con la habilitación del puerto y los privilegios establecidos. De igual forma MAC realiza una petición al servidor RADIUS el cual se comunica con el servidor ISE para verificar que la petición solicitada sea autorizada siempre y cuando la MAC se encuentre agregada de forma correcta al grupo que le corresponde y manda la respuesta al servidor RADIUS para otorgar o denegar el acceso a la red LAN. Ver figura 10.

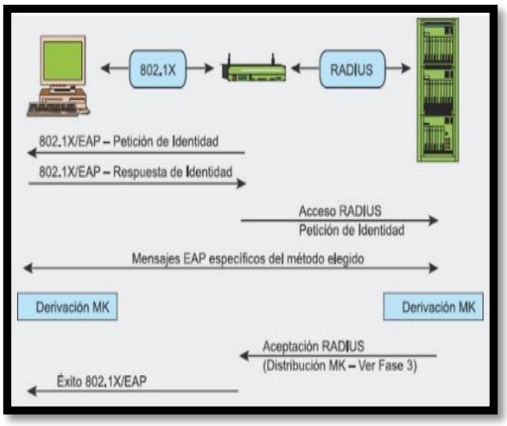

Figura 10. Detalle de la alerta
Fuente: Elaboración Propia con base en funcionamiento general del RADIUS.

El funcionamiento del control de acceso basado en puertos tiene el efecto de crear dos formas lógicas distintas de acceso, en el punto de conexión física del dispositivo, a la LAN.

Puerto incontrolado: Permite el intercambio de paquetes del dispositivo (authenticator) a otros dispositivos en la LAN, a pesar del estado de autorización. Es utilizado durante el proceso de autenticación. Este puerto en ocasiones también es referido como puerto no autorizado.

Puerto controlado: Permite el intercambio de paquetes sólo si el estado actual del puerto es autorizado. Antes de la autenticación, el enlace permanece truncado y no son enviadas tramas entre el cliente y los dispositivos a los que se pueden acceder mediante el authenticator. Cuando el cliente es autenticado con éxito mediante IEEE 802.1X, el enlace es establecido y las tramas pueden ser enviadas entre el cliente y los nodos alcanzables vía el authenticator.

Este puerto en ocasiones también es referido como puerto autorizado. Los puertos controlado e incontrolado son considerados como parte del mismo punto de conexión física a la LAN.

Al realizar la revisión de la seguridad de puertos se muestra en la figura 11 como se verifica si un puerto no tiene seguridad para lo cual se tiene que aplicar una lista de control de acceso (ACL).

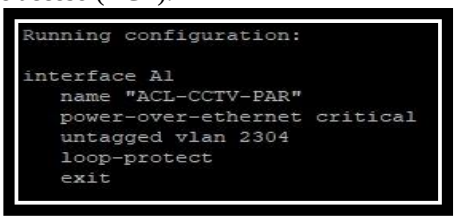

Figura 11. Puerto sin seguridad
Fuente: Elaboración Propia

La siguiente configuración es la asignada a una estación de trabajo y con seguridad 802.1X, también tiene un comando adicional y su función es que el puerto se autentique cada cierto tiempo ya sea en horas o segundos. Ver figura 12.

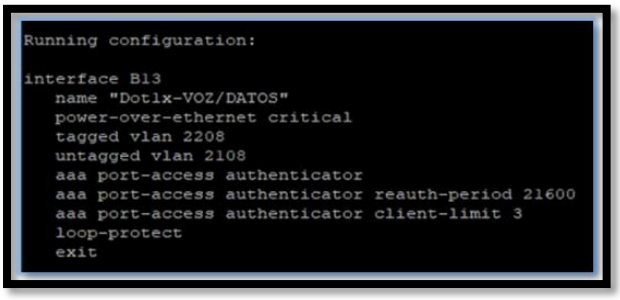

Figura 12. Puerto con autenticación
Fuente: Elaboración Propia

La siguiente configuración es la asignada a una estación de trabajo con máquina virtual, con seguridad 802.1X y MAC. Esto permitirá la autenticación por la doble seguridad. Ver figura 13.

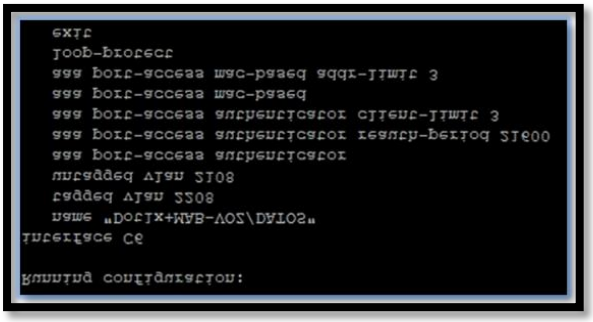

Figura 13. Revisión de la seguridad
Fuente: Elaboración Propia

Por el ultimo, este es el comando que se utiliza para validar que los puertos se encuentren con la seguridad que le corresponda a cada uno. Ver figura 14.

Figura 14. Verificación de seguridad
Fuente: Elaboración Propia

La etapa final antes de que se conceda al usuario acceso al switch es la autenticación de sus credenciales. Para ello, la mayoría de los usuarios de SSH (Secure Shell Protocol) o (protocolo de seguridad Shell, el cual es un protocolo de administración remota que les permite a los usuarios controlar y modificar sus servidores remotos a través de Internet por medio de un mecanismo de autenticación.) utilizan una contraseña, donde se le solicita al usuario que introduzca el nombre, seguido de la contraseña. Estas credenciales pasan con seguridad a través del túnel cifrado simétricamente, así que no hay ninguna posibilidad de que sean capturadas por un tercero. Con la resolución se procede a el cierre de la incidencia, donde en este caso los equipos que mostraron incidencia en la seguridad fueron solo los equipos de acceso. Esto se valida entrando a los switches e ingresando el comando de la imagen anterior o revisando el alertamiento del IMC que muestra el puerto, que no tenga la seguridad asignada.

Las fallas en equipos se redujeron al configurar la seguridad y los alertamientos ya que, de 110, solo 2 de ellos no se lograron actualizar debido a fallas de estos, por lo que se obtuvo una eficiencia del 98% al aplicar el modelo, ya que, si se detecta un puerto sin seguridad, se procede a realizar un recorte o captura de pantalla, mostrando el puerto y agregándolo a la bitácora de alertas y se procede a realizar el procedimiento ya establecido para este tipo de incidencia. Este permite además realizar la actividad de configuración de una manera eficaz y reduciendo los tiempos integrar información de estas en la plataforma para la continuidad y monitoreo de la red.

3. CONCLUSIONES Y RECOMENDACIONES

La plataforma de Monitoreo IMC es una gran herramienta de apoyo para el área de soporte técnico ya que permite realizar configuraciones masivas a los equipos sin tener que ingresar directamente a ellos, muestra los alertamientos de cambios de configuración en los puertos, cuando un puerto sufre desconexión por que se retiró el equipo del nodo en que se encuentra, indica si un switch pierde conexión o es desconectado, de igual forma alerta si una fibra pierde conexión y también permite mandar los alertamientos a algún correo en específico.

Desventajas de la plataforma: para poder monitorear se necesita estar conectado por Red LAN, no permite el acceso por WI-FI, la licencia tiene un costo bastante alto y solamente es por periodos de un año, no permite más tiempo, el servidor no cuenta con conexión a internet, solo se puede acceder físicamente con cable de consola o por escritorio remoto y el soporte de la empresa HPE solo es de 9 de la mañana a 4 de la tarde, no es de 24 horas.

La seguridad en la autenticación por 802.1X y MAC es complementada al incluir la seguridad con el control de acceso a la red (NAC) y el Servidor Radius, ambos se complementan para alcanzar la seguridad deseada, ya sea por 802.1X o por MAC, ya que permiten la autenticación cliente/servidor y dar el servicio de Red LAN a los equipos que solo sean de la institución financiera, por lo que ya no se tendrá el problema con los dispositivos ajenos, debido a que no tendrán servicio de Red LAN.

El modelo de incidencias aplicado derivo de un alertamiento al utilizar la plataforma originado por el diagnóstico inicial del reporte de incidencia generado por las áreas correspondientes, ya que con la pandemia se tenía de dar a los usuarios de la institución la posibilidad de que pudieran compartir sus archivos, colaborar en proyectos, enviar mensajes instantáneos o de correo electrónico de forma simultánea. Por lo que se tuvo como prioridad el de controlar los recursos desde una ubicación central la administración y servicios de red. Es importante indicar que para realizar las pruebas del cierre de puertos y escaneo constantes no se realizaba de forma inmediata ya que se requieren de tiempo y fechas específicas asignadas por la institución financiera.

Con el uso de la plataforma de software HPE Intelligent Management Center Enterprise que es una herramienta de gestión integral de redes cableadas e inalámbricas compatible con el modelo de FCAPS que proporciona una gestión empresarial integral de TI, escalabilidad de la arquitectura de sistema y alojamiento para la nueva infraestructura y tecnología, esta es compatible con la gestión de dispositivos Hewlett Packard Enterprise y de otros fabricantes, se mejoraron los tiempos de respuesta ya que con uso de este software.

Se concluye que, dentro del análisis expuesto, es posible vislumbrar que los objetivos se cumplieron satisfactoriamente en los equipos de pruebas, para la correcta implementación en los equipos de producción de todas las sedes de la institución financiera, permitiendo un mejor crecimiento, control y eficiencia de la seguridad de la institución.

El análisis de la eficacia de las soluciones de seguridad se está realizando con herramientas especializada las cuales fueron seleccionadas por la empresa, pero debido a la confidencialidad y protección de la información que corresponde a esta, no se mencionan en el presente artículo

Trabajo a futuro

Los alertamientos saldrán de forma diaria a las 2 de la mañana los cuales mostrarán las modificaciones que sufran los switches de acceso, indicándonos si algún puerto no cuenta con la seguridad requerida.

El control que se llevará para identificar las modificaciones que sufran los equipos ya sea por parte de la institución financiera o los usuarios, es en una bitácora con fecha, sede, piso, nombre del solicitante, actividad requerida y nombre del ingeniero. A principios de cada mes esta bitácora nos

ayudará a identificar que equipos son los que sufren más cambios en su configuración durante todo el transcurso del mes pasado.

4. REFERENCIAS

[1] Organización de los Estados Americanos "Estado de la Ciberseguridad en el Sistema Financiero Mexicano2, 2019, [En línea]. Disponible: https://www.cnbv.gob.mx/Documents/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf?ID=65 [Último acceso: 16 julio 2021].

[2] Cisneros, J.," El papel del CEO, parte del éxito en la estrategia de ciberseguridad", 2020, [En línea] Disponible: https://forbescentroamerica.com/2020/07/14/el-papel-del-ceo-parte-del-exito-en-la-estrategia-de-ciberseguridad/, [Último acceso:16 julio 2020].

[3] Forbes," Protección de datos, el desafío de la era post covid - 19", 2020, [En línea] Disponible: https://foroforbes.com/2020/latam/forbes-ciberseguridad-latam-2020/, [Último acceso:16 julio 2020].

[4] J.-F. Pillou, «CCM,» 16 octubre 2008. [En línea]. Disponible en: https://es.ccm.net/contents/602-itil-biblioteca-de-infraestructuras-de-tecnologias-de-informaci [Último acceso: 09 junio 2021].

[5] ITIL, "ITIL Service Operation". Disponible: www.best-management.practice.com. ISBN 9780113313075.

[6] DATADEC, "Consejos para una correcta gestión de incidencias", 2017, [En línea] Disponible: https://www.datadec.es/blog/consejos-para-correcta-gestion-de-incidencias [Último acceso: 17 marzo 2022].

[7] Plataforma Group Soluciones Tecnológicas, "Qué es la Gestión de incidencias y sus principales actividades según ITIL v3". [En línea] Disponible: https://www.servicetonic.cl/itil/itil-v3-gestion-de-incidencias/ [Último acceso: 17 marzo 2022].

[8] Del Rincón, D.; Arnal, J.; Latorre, A.; y Sans, A., "Técnicas de investigación en ciencias sociales. Concepto y características de la observación participante", (1995).

[9] OSIATIS, "Gestión de Servicios TI", Disponible: http://itilv3.osiatis.es/gestion_servicios_ti.php, (2010-2) [Último acceso: 20 julio 2020].

[10] OSIATIS, "Curso puente ITIL v.3", Disponible: http://www.osiatis.es/formacion/Formacion_ITIL_web_V3Bridge.pdf.

[11] Peña, S., "Guía para la Gestión de Servicios de Ti Basada en ITIL V3", 2012.

[12] Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A., & Verheijen, T." Mejora continua del servicio basada en ITIL® V3 - Guía de Gestión". (2008), Van Haren Publishing.

[13] Bon, J. v., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van Der Veen, A., y Verheijen, T. "Fundamentos de ITIL® V3", (2010). Wilco NL: Van Haren Publishing.