****

**| Reto 8: Análisis de casos: seguridad y diseño de una red inalámbrica**

|  |  |
| --- | --- |
| Nombre completo | Benjamin Rivera |
| Matrícula | 19015478 |
| Fecha de elaboración | 4 de noviembre de 2020 |
| Nombre del Módulo | Redes de computadoras |
| Nombre del Asesor | Claudia Patricia Rojano |

|  |  |
| --- | --- |
| **1** | **Caso 1. Conexión de última milla** |
|  |  |

**Instrucción:** analiza el caso que se te presenta y realiza lo que se te indica en cada apartado.

|  |
| --- |
| **1. Funcionamiento del negocio o del lugar donde se instalará la red** |

Con el objetivo de proveer servicio de internet a las sucursales bancarias ubicadas en zonas rurales de difícil acceso, se ha valorado la posibilidad de conectar de forma inalámbrica a este tipo de poblaciones alejadas del área metropolitana. Para ello, se ha destinado un proyecto de red que permita conectarlas mediante tecnología inalámbrica de última milla.

|  |
| --- |
| **2. Determinar el equipo de red y los servicios a ofrecer** |

Escribe aquí una solución al caso considerando lo siguiente:

1. ¿Qué tecnología recomiendas para conectar zonas rurales y zonas urbanas con el objetivo de proveer de servicio de internet, wifi o WiMAX? ¿Por qué?

|  |
| --- |
| Dado que las zonas son de difícil acceso, considero que la mejor opción es usar la tecnología WiMAX. Esto porque permite la conexión inalámbrica en grandes distancias. |
|  |

1. ¿Qué especificaciones debe tener la red que se use en las sucursales bancarias?

|  |
| --- |
| En los interiores, para que los empleados puedan utilizar mas que solo los dispositivos alambrillas, debe haber dos redes.  Una red wifi que cumpla con los estándares 802.11n, los dispositivos que se usen para establecer esta debe contar con la posibilidad de implementar protocolo superior a WPA2.  La segunda parte de la red debe tener suficientes terminales como para poder abastecer a todos los dispositivos alambricos y estáticos de una conexión. |

1. De ser necesario proporcionar cobertura de internet en espacios cerrados dentro de la sucursal bancaria, ¿qué velocidad de transmisión puede obtenerse con el estándar 802.11n?

|  |
| --- |
| Una velocidad maxima de 600 Mbps. |

1. ¿Qué protocolos de seguridad sería recomendable implementar en la red inalámbrica de la sucursal bancaria?

|  |
| --- |
| Dado que solo el personal interno estaria accesando a lla red, considero que el filtrado de MAC’s es lo mas adecuado.  En caso de que se deseara tener una red publica esta bastaria con tener el protocolo actualizado WEP de seguridad. |

|  |
| --- |
| **3. Verificación: funcionamiento de la red** |

Menciona qué prueba(s) puedes realizar en una computadora de la sucursal bancaria para verificar el correcto funcionamiento de la red.

|  |
| --- |
| Al finalizar con las configuraciones hay que asegurarse de que cada una de las terminales bancarias pueda acceder a los recursos de la red. Ademas, en caso de que se quiera establecer una red publica, hay que verificar que exista una conexión estable. |

|  |  |
| --- | --- |
| **2** | **Caso 2. Conectividad de campus** |
|  |  |

**Instrucción:** analiza el caso que se te presenta y realiza lo que se te indica en cada apartado.

|  |
| --- |
| **1. Funcionamiento del negocio o del lugar donde se instalará la red** |

Un campus universitario requiere una red inalámbrica para dar cobertura de internet dentro de sus instalaciones.

Las distancias entre el edificio central y las redes secundarias son de menos de 1000 metros con vista directa entre edificios.

Dentro del edificio central se colocarán 100 computadoras con antenas inalámbricas, así como cuatro puntos de acceso inalámbrico para 50 computadoras portátiles.

Los *access point* se conectarán directamente a la red, sin realizar configuración adicional. Para el acceso de internet público se permite que los *access points* mantengan visibles su SSID. Los *access point* de última generación son configurados con el protocolo WEP, WPA y WPA2.

Se decide instalar una herramienta detectora de intrusos a la red, conocido como *firewall*, esta se coloca en la oficina del director para que su computadora esté segura.

Por otro lado, el estándar de seguridad elegido para las 100 computadoras con antenas portátiles es WEP; la razón por la que se quiere utilizar este estándar es que funciona con 64 bits para generar una clave de acceso fija.

El personal del área de sistemas informáticos aún no decide el estándar de seguridad para la red inalámbrica del edificio central, pero se tienen 4 opciones diferentes a elegir: WEP, WPA, WPA2 o WPA3. Finalmente, la conexión principal con el proveedor de internet deberá contar con la mayor velocidad posible.

|  |
| --- |
| **2. Determinar el equipo de red y los servicios a ofrecer.** |

Escribe aquí una solución al caso considerando lo siguiente:

1. De acuerdo a la descripción del caso y a la necesidad del edificio central, ¿qué estándar inalámbrico podrá emplearse? ¿Por qué?

|  |
| --- |
| Para la conexión entre los edificios recomendaría que fuera conexión cableada, esto aumentaría la seguridad y velocidad de conexión fuera del edificio central; en caso de que se necesitara aque fuera inalámbrico, recomendaría un protocolo WiMAX.  Para las conexiones en interiores recomiendo la implementación del protocolo WIFI, por la cantidad de usuarios y la distancia que debe cubrirse. Además de que este protocolo y el hardware disponible nos permitiría implementar el resto de las características solicitadas y sugeridas. |
|  |

1. ¿Qué protocolo de seguridad se recomienda utilizar para cumplir con las normas estandarizadas?

|  |
| --- |
| Se recomienda que los protocolos de seguridad inalámbrica se al menos la versión estandarizada WPA2, ya que de otra forma serían constantes amenazas de seguridad. |

1. ¿Por qué razón es recomendable utilizar un protocolo de seguridad en una red inalámbrica, a diferencia de una red Ethernet cableada?

|  |
| --- |
| A diferencia de la red cableada, la red inalámbrica transmite la información al aire, lo que podría ser una amenaza de seguridad si no estuviera protegido. Además de que cualquiera con las credenciales correctas puede conectarse a estas, a diferencia de la red cableada, de los cuales no debería haber puertos o cables no asignados a un punto específico. |

1. ¿Qué función tiene el dispositivo de red *firewall* en el caso planteado?

|  |
| --- |
| En esta caso el Firewall tiene el objetivo de proteger la rede interna de posibles ataque externos. Principalmente los archivos que se encuentren en los dispositivos del edificio central. |

1. ¿Qué mecanismo adicional implementarías en la red inalámbrica para contar con mayor seguridad?

|  |
| --- |
| En la red inalámbrica del edificio central, y principalmente de las oficinas administrativas y académicas, propondría la implementación de un filtrado por  direcciones MAC. Esto porque las personas de estos departamentos no suelen rotar mucho y se puede establecer limite de dispositivos. |

1. ¿ Qué recomendaciones harías en cuanto a la decisión de dejar visible el SSID?

|  |
| --- |
| En las redes publicas y de áreas que no manejen datos confidenciales me parece una buena decisión. Esto porque las áreas antes mencionadas estarían parcialmente protegidas por el firewall de accesos no directos, y en estas áreas si debería de mantenerse ocultan como mencione en el punto 5. |

1. ¿Cuáles serían las consecuencias en caso de que la escuela mantenga el estándar de seguridad WEP en sus antenas?

|  |
| --- |
| Entonces todas sus comunicaciones que pasen por estos puntos pueden estar comprometidas. Ademas de que estos puntos de acceso serían posibles amenazas de seguridad para el resto de la red si el firewall no esta correctamente configurado. |

|  |
| --- |
| **3. Verificación: funcionamiento de la red** |

Menciona qué prueba(s) puedes realizar para verificar el correcto funcionamiento de la red.

|  |
| --- |
| En este escenario se deberá corroborar que en cada una de las zonas abarcadas se posible acceder a los archivos de red y también que se pueda conectar a recursos externos de la red interna. |

|  |  |
| --- | --- |
| **3** | **Caso 3. Estándares y protocolos de seguridad** |
|  |  |

**Instrucción:** realiza lo que se te indica en el siguiente apartado.

|  |
| --- |
| **1. Velocidad de los estándares de la IEEE** |

Considerando los estándares de la IEEE indicados, escribe la velocidad del estándar que le corresponde a cada uno.

|  |  |
| --- | --- |
| **Estándares de la IEEE** | **Velocidad de transmisión de datos** |
|  | Escribe en esta columna la velocidad de transmisión de datos del estándar correspondiente. |
| **802.11** | 2 Mbps |
| **802.11b** | 11 Mbps |
| **802.11a** | 20 Mbps |
| **802.11g** | 22 Mbps |
| **802.11n** | 600 Mbps |
| **802.16e** | 15 Mbps |

|  |
| --- |
| **2. Protocolos de seguridad inalámbrica** |

**Instrucción:** con base en los contenidos de la Lección, determina en el siguiente cuadro comparativo, las características, tamaño de la clave de seguridad y tipo de cifrado de los protocolos de seguridad inalámbrica que se indican.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **WEP** | **WPA** | **WPA2** | **WPA3** |
| Características | Publicado en 1997 usando un sistema abierto de clave precompartida | Publicado en 2003 usando un sistema con variante EAP de clave precompartida | Publicado en 2004 usando un sistema abierto de clave precompartida (PSK) | Publicado en 2018 de sistema de autenticación simultanea. |
| Tamaño de la clave de seguridad | 64 | 128 | 128 | 256 |
| Tipo de cifrado | RC4 estático | TKIP y RC4 dinámico | AES-CCMP dinámica | AES-CCMP y AES-GCMP dinámico |

**CRÉDITOS:**

*Autor:* Miguel Alfonso López Alonso

*© UVEG. Derechos reservados. El contenido de este formato está sujeto a las disposiciones aplicables en materia de Propiedad Intelectual, por lo que no puede ser distribuido, ni transmitido, parcial o totalmente, mediante cualquier medio, método o sistema impreso, electrónico, magnético, incluyendo el fotocopiado, la fotografía, la grabación o un sistema de recuperación de la información, sin la autorización por escrito de la Universidad Virtual del Estado de Guanajuato.*