UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

ASPECTOS DE SEGURIDAD INFORMÁTICA EN LOS SERVICIOS DE TELEMEDICINA.

TRABAJO MONOGRÁFICO

PARA OBTENER EL GRADO DE

INGENIERO EN REDES

PRESENTA

RICARDO JAVIER TORRES SALAZAR

SUPERVISORES

DR. JAVIER VÁZQUEZ CASTILLO
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA
M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
DR. JAIME SILVERIO ORTEGÓN AGUILAR
M.C.I. MELISSA BLANQUETO ESTRADA

CHETUMAL, QUINTANA ROO, MÉXICO, SEPTIEMBRE DE 2019

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO TITULADO

ASPECTOS DE SEGURIDAD INFORMÁTICA EN LOS SERVICIOS DE TELEMEDICINA

ELABORADO POR

RICARDO JAVIER TORRES SALAZAR

BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE

INGENIERO EN REDES

COMITÉ SUPERVISOR

SUPERVISOR: _____
DR. JAVIER VAZQUEZ CASTILLO

SUPERVISOR: _____
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA

SUPERVISOR: _____
M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

SUPERVISOR SUPLENTE: _____
DR. JAIME SILVERIO ORTEGÓN AGUILAR

SUPERVISORA SUPLENTE: _____
M.T.I. MELISSA BLANQUETO ESTRADA

CHETUMAL, QUINTANA ROO, MÉXICO, SEPTIEMBRE DE 2019

Resumen.

Los servicios de Telesalud representan ventajas significativas respecto a la atención tradicional de salud, especialmente en las poblaciones alejadas de las ciudades y que se encuentran marginadas de atención médica especializada. Algunas de las ventajas que destacan son el mejoramiento de diagnósticos oportunos en un paciente, la reducción de tiempo y dinero de los pacientes que podrían evitar algunos traslados desde sus comunidades a los centros hospitalarios de las ciudades y una mejor gestión en el sistema de citas médicas.

Las tecnologías de información y la comunicación son piedra angular en la implementación de proyectos de Telesalud, sin embargo, ésta se expone a riesgos que tienen que ver con aspectos fundamentales de la seguridad informática como la autenticación, la confidencialidad, la privacidad y el no repudio en procesos básicos como transmitir información de consultas médicas, videos, audios y textos en los expedientes de los pacientes.

El almacenamiento de datos sensibles de los pacientes y de operatividad del sistema de telesalud son un claro ejemplo del reto que enfrentamos para tratar y salvaguardar información valiosa tomando en cuenta los aspectos de seguridad informática que deben establecerse siguiendo protocolos estrictos con el fin de detectar actividades sospechosas por parte de los usuarios del sistema (o de agentes externos) que busquen manipular, destruir y/o acceder a información confidencial o de lograr algún ataque dirigido a la infraestructura de telecomunicaciones.

El presente trabajo de investigación recopila información relevante de los aspectos de seguridad que deben tomarse en cuenta para la implementación y puesta en marcha de servicios de telesalud, los cuales comprenden la consulta de entre hospitales consultantes y los interconsultantes (teleconsulta) y la capacitación médica especializada a distancia (Teleeducación).

Se describen las principales estrategias en la gestión de aspectos fundamentales de la seguridad informática en la red de telecomunicaciones, la seguridad perimetral, detección y eliminación de virus informáticos, gestión de accesos no autorizados y seguridad en la capa de aplicación.

Agradecimientos.

Primeramente, doy gracias a Dios por acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito una de mis metas propuestas.

Así mismo, le agradezco a la Universidad de Quintana Roo por haberme dado la oportunidad de continuar y concluir con mis estudios, dentro de ésta le doy gracias especialmente:

Al Dr. Javier Vázquez Castillo por ser mi director de monografía y guiarme en este último recorrido, por las clases impartidas a lo largo de este tiempo y por todo lo que me dejo como enseñanza.

Al M.S.I Rubén Enrique González Elixavide por las clases, las correcciones, sus prácticas de laboratorio y entrega de las mismas, los consejos que me dio a lo largo de este tiempo en clase y fuera de ellas. Siempre tuvo las palabras necesarias para inspirarme y hacer que piense que es lo que quiero de mi futuro y hasta donde quiero llegar.

Al M.T.I Vladimir Veniamin Cabañas Victoria por sus chistes, su buen humor y por tenerme en cuenta para integrarme en algunos proyectos, los cuales me ayudaron para el trabajo en equipo y experiencia laboral.

Al Dr. Jaime Silverio Ortegón Aguilar por ser mi tutor durante este tiempo, a pesar de que solo nos vimos en algunas clases, de no tener mucha comunicación durante el semestre más que para saludarnos y para cuando necesitaba autorización de mis materias, creo que nunca dudo de mi capacidad y sabía que este momento iba a llegar y se lo agradezco.

También a todos y cada uno de los profesores que fueron parte importante en mi formación.

Agradezco a mis padres María Angélica Salazar Gerónimo y Francisco Javier Torres Catzin por darme la vida, por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron. Sé que en algún momento ya no estarán en este mundo porque nada es eterno, eso lo tengo muy claro. Y tal vez no sea muy expresivo, sin embargo, les quiero decir que cada día junto a ustedes es un regalo para mí y les doy gracias por enseñarme a ser sencillo y humilde, a estar orgulloso de quien soy y de dónde vengo, a ser feliz con lo poco o mucho que tenga, a nunca envidiar lo que tengan los demás sino a luchar para conseguir las cosas de la manera correcta, con el sudor de mi frente. Nunca me he avergonzado

de ustedes, de su origen, del poco o nulo estudio que tienen, siempre me he sentido orgulloso de lo trabajadores que son y por ser ese gran ejemplo para mí y mis hermanas. Gracias por tener un minuto para escucharme porque de ese minuto aprendí y entendí muchas cosas para ser quien soy y estar donde estoy. Hoy les doy este pequeño premio a todo lo antes mencionado, sin embargo, nunca podré pagarles ni agradecerles todo lo que han hecho por mí.

También a mi tía Margarita De Jesús Torres Catzin, a la cual considero como mi segunda madre, gracias por haberme aconsejado y ayudado siempre, por enseñarme a ser sencillo y agradecido con lo que tengo. Durante mi niñez, gracias por llevarme mi desayuno a la primaria todos los días, por ayudarme con mi tarea, a estudiar para mis exámenes, por seguir dándome consejos incluso a esta edad. También por acompañarme a mis clases y viajes cuando practicaba Tae Kwon Do, en fin, gracias por todo.

A la Mtra. Dalia Bastarrachea Loeza por haber sido parte importante en mi formación y por siempre estar pendiente de mi desarrollo como persona y como estudiante durante mi paso por la primaria. Usted fue parte importante de mi crecimiento, me ayudó a vencer muchos miedos que tenía de pequeño, también a quererme tal y como soy sin importar la opinión de los demás. Gracias a todo el apoyo que le dio a mis papás y a mí principalmente hoy tienen su recompensa.

A Sugely Aguilar Jiménez, una persona muy especial e importante, mi compañera de vida. Gracias por permitirme conocerte cuando teníamos 15 años, a pesar de que solo tuvimos la oportunidad de estudiar juntos un año, siempre me has dado consejos y ánimos, y estas cuando más lo necesito. Cuando he estado a punto de tirar la toalla siempre tienes las palabras correctas para ayudarme a seguir en la búsqueda de cumplir con mis sueños y objetivos.

Dedicatoria.

Con mucho cariño para:

Mis padres María Angélica Salazar Gerónimo y Francisco Javier Torres Catzin, este logro también es suyo porque a pesar de que ninguno de los dos tuvo la oportunidad de estudiar o de seguir estudiando, ustedes me dieron el apoyo necesario y la oportunidad de estudiar, y eso junto con la educación que me dieron, es la mejor herencia que me han podido dar. Nunca podré pagarles y terminar de agradecerles todo lo que han hecho por mí, pero esto se los doy con mucho orgullo y cariño.

A mis hermanas Sheila Nayeli Torres Salazar y Keila Monserrat Torres Salazar para que vean y se den cuenta que en la vida nada es imposible. Nunca permitan que otra persona les arruine sus sueños y les diga que no podrán realizarlos, el único límite para lograrlo son ustedes mismas. Si tienen sueños y metas luchen por cada uno de ellos porque cada día que pasa es una nueva oportunidad para lograrlos, tal vez algunos no se lleven a cabo como esperaban pero siéntanse felices por haberlo intentado porque muchos ni siquiera lo intentan.

También a mi tía Margarita De Jesús Torres Catzin por ser una madre más para mí. Por esas palabras de aliento y esos sabios consejos en momentos difíciles, por ser parte fundamental en mi crecimiento como persona y estudiante, porque todos los momentos que atravieso en mi vida las tomo de la mejor manera gracias a ti, recordando todo lo que me has enseñado y lo que has hecho por mí.

A mis abuelos María Aniceta Catzin Matos y Erasmo Torres Che por darme el ejemplo de trabajar con humildad, por enseñarme a que la edad no es impedimento para ganarme el pan de cada día y ser felices. Sin importar los problemas que los aquejan, ustedes nunca se dan por vencidos sino todo lo contrario, día a día luchan para salir adelante y eso es algo que he aprendido de ustedes, a nunca rendirme.

A Sugely Aguilar Jiménez por estar conmigo siempre en cada decisión que tomo y cada paso que doy, por ayudarme a conseguir mis sueños y objetivos pero también por ayudarme a salir adelante cuando tengo un problema u obstáculo frente a mí. Tú eres parte importante de este logro, así que también es tuyo.

Contenido

Índice de ilustraciones.

1 INTRODUCCIÓN

1.1 JUSTIFICACIÓN

El uso de redes para conectar sistemas de tecnología de la información (TI) heterogéneos puede generar un aumento de la productividad para las organizaciones y nuevas capacidades creadas por los sistemas conectados. Las redes desempeñan en la actualidad un papel clave para las infraestructuras fundamentales de muchos países, como pueden ser el comercio electrónico, las comunicaciones de voz y datos, las instalaciones, las finanzas, la salud, los transportes y la defensa.

La interconexión de las redes y el acceso omnipresente son elementos clave de los sistemas de TI actuales. No obstante, la amplitud del acceso y la fácil conexión de los sistemas de TI pueden ser una fuente primaria de vulnerabilidad generalizada. Las amenazas que planean sobre los sistemas en red, como los ataques de denegación de servicio, el robo de datos financieros y personales, los fallos de red y la interrupción de telecomunicaciones de voz y datos, son cada vez más numerosas.

Los protocolos de red que se utilizan hoy en día se crearon en un entorno de confianza. La mayoría de las nuevas inversiones e investigaciones se dedican a la creación de nuevas funcionalidades, pero no a su seguridad.

Las amenazas a la ciberseguridad crecen rápidamente. Los virus, gusanos, caballos de Troya, ataques de falsificación, robos de identidad, etc., están al alza. Es necesario entender lo que es la ciberseguridad para poder sentar los cimientos necesarios a fin de poder proteger las redes del futuro.

Se alienta a que las empresas y organismos gubernamentales consideren la seguridad como un proceso o una perspectiva de protección de los sistemas, redes, aplicaciones y recursos. El principio subyacente es que las redes conectadas conllevan riesgos inherentes.

Sin embargo, la seguridad no debe ser un obstáculo para el funcionamiento. El objetivo es saber cómo ofrecer los servicios necesarios de manera segura.

Las aplicaciones se ejecutan en las redes por capas. Se supone que hay seguridad entre cada una de estas capas. Abordar la seguridad por capas permite a las organizaciones crear múltiples niveles de defensa contra las amenazas.

En adición la protección de los datos en los expedientes clínicos electrónicos es claramente especificada por norma. En este sentido la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud **(Secretaria de Salud, 2012)** establece los criterios para la protección de datos en los expedientes clínicos electrónicos, como:

1. Establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud, entrando en vigor 60 días después de su publicación.
2. Corresponde a la Secretaría de Salud establecer, conforme a las disposiciones jurídicas aplicables, la normatividad a que deben sujetarse los Sistemas de Información de Registro Electrónico para la Salud (SIRES) que utilicen los prestadores de servicios de salud, a fin de garantizar el intercambio, procesamiento, interpretación y seguridad de la información contenida en dichos sistemas.
3. Los prestadores de servicios de salud a través de los SIRES deben garantizar la confidencialidad de la identidad de los pacientes, así como la integridad y confiabilidad de la información clínica y establecer las medidas de seguridad pertinentes y adecuadas a fin de evitar el uso ilícito o ilegítimo que pueda lesionar la esfera jurídica del titular de la información, de acuerdo con las disposiciones jurídicas aplicables.
4. Los prestadores de servicios de salud que utilicen SIRES deben implementar un Sistema de Gestión de Seguridad de la Información de acuerdo con las disposiciones jurídicas aplicables en materia de transparencia, protección de datos personales y

estándares en materia de seguridad de la información, que aseguren la confidencialidad, integridad, disponibilidad, trazabilidad y no repudio de la información en salud.

5. Los SIRES deben registrar y resguardar la información derivada de la prestación de servicios de salud en forma de documentos electrónicos estructurados e inalterables de acuerdo a las disposiciones jurídicas aplicables. Los SIRES deben permitir la firma electrónica avanzada del profesional de la salud para toda aquella información que determine el prestador de servicios de salud en su sistema de gestión de seguridad de la información, de conformidad con lo establecido en las disposiciones jurídicas aplicables.
6. Todos los usuarios, organizaciones y dispositivos deben ser autenticados en los SIRES como mínimo por un nombre de usuario y una contraseña cuya definición debe aprobarse por el grupo de trabajo estratégico de seguridad de la información de la organización. Se recomienda el uso de factores adicionales de autenticación.
7. Los SIRES deben implementar mecanismos de autorización basada en roles. Los perfiles de usuario deben ser definidos por cada prestador de servicios de salud de acuerdo con las disposiciones jurídicas aplicables a cada organización.
8. Con fines de intercambio de información entre prestadores de servicios de salud los SIRES deben implementar mecanismos de autenticación, de cifrado y de firma electrónica avanzada de acuerdo con las disposiciones jurídicas, Guías y Formatos aplicables.
9. Los SIRES deben permitir la exportación de la información del paciente de acuerdo con lo establecido en las disposiciones jurídicas aplicables en materia de transparencia y protección de datos personales, utilizando las guías y formatos que para este fin se definan. Así mismo deben implementar controles sobre los consentimientos del titular de la información o quien tenga facultad legal para decidir por él, de acuerdo a lo establecido por las disposiciones jurídicas aplicables en materia de transparencia y protección de datos personales.

El intercambio de información entre prestadores de servicios de salud en nuestro país es un requerimiento esencial para otorgarle continuidad a la atención médica entre los mismos. El

avance tecnológico que presenta la informática médica posibilita que los Sistemas de Información de Registro Electrónico para la Salud, entre los que se encuentran los Expedientes Clínicos Electrónicos, puedan intercambiar información útil con este objetivo, además de permitir explotar información de salud pública, lo que facilita la toma de decisiones en el sector. **(Secretaria de Salud, 2012)**

De los puntos anteriores:

En el punto 1 se menciona que los Sistemas de Expediente Clínico Electrónico deben garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos de salud.

En el punto 2 se menciona que la Secretaría de Salud debe garantizar el intercambio, procesamiento, interpretación y seguridad de la información contenida en los SIRES.

En el punto 3 se menciona que los prestadores de servicios de salud como toda ética profesional deben garantizar al paciente que toda la información que éste nos brinde será usada de manera adecuada. Se debe tener en cuenta el principio de confidencialidad y confiabilidad más en aquellos que ejercen en el ámbito de salud pública.

En el punto 4 se menciona que los prestadores de servicios de salud que utilicen los SIRES deben dar la certeza que los datos están protegidos y bajo confidencialidad, que estos no sean corrompidos para un mal uso o manipulación. Que este en disponibilidad para todo aquel que le sea necesario, pero siempre bajo los estándares establecidos.

En el punto 5 se menciona que los SIRES deben registrar y resguardar la información derivada de la prestación de servicios de salud en forma de documentos electrónicos estructurados e inalterables. Además, deben permitir la firma electrónica avanzada del profesional de la salud para toda aquella información que determine el prestador de servicios de salud.

En el punto 6 se menciona que todo aquel que requiere ingresar a los SIRES debe tener una cuenta ya autorizada y verificada que conste de un usuario y contraseña, esto para evitar que personas no autorizadas ingresen, ya que como se mencionó anteriormente, los datos deben ser manejados de manera confidencial.

En el punto 7 se menciona que los SIRES deben implementar mecanismos de autorización basada en roles. Además, los perfiles de usuario deben ser definidos por cada Prestador de Servicios de Salud.

En el punto 8 se menciona que para fines de intercambio de información entre Prestadores de servicios de salud se deben considerar más requerimientos con base a las disposiciones jurídicas, guías y formatos aplicables para tener la veracidad de que con quien se comparte la información es el titular.

En el punto 9 se menciona que los SIRES deben permitir la exportación de la información del paciente en caso de ser necesario, siempre tomando en cuenta los lineamientos que se deben cumplir para la obtención de la misma. También es importante conocer si el titular de la información ha otorgado y firmado un consentimiento informado, el cual quiere decir que autoriza que toda su información brindada sea usada de manera adecuada.

1.2 Objetivo General.

Proporcionar información detallada de los aspectos de seguridad informática para los servicios de Telemedicina.

1.3 Objetivos Particulares.

1. Revisar la Norma Oficial Mexicana NOM-024-SSA3-X establecida para la protección de los datos en registros electrónicos de salud.
2. Revisar las recomendaciones para la ciberseguridad en el espacio en redes de datos, comunicaciones de sistemas abiertos y seguridad (UIT-T X.1205).
3. Revisar las técnicas de seguridad informática en redes de datos.
4. Definir los aspectos a considerar de seguridad informática para la red de Telemedicina del Estado de Quintana Roo.

2 Desarrollo del trabajo.

2.1 La Telemedicina.

El concepto de Telemedicina surge en la de cada de los 70's con el desarrollo de la tecnología (internet, ordenadores, móviles, entre otros), aparece como una forma de luchar contra las barreras geográficas aumentando la accesibilidad a los cuidados de salud, especialmente en países en desarrollo.

2.1.1 ¿Qué es Telemedicina?

La Organización Mundial de la Salud (OMS) la define como "Aportar servicios de salud, donde la distancia es un factor crítico, por cualquier profesional de la salud, usando las nuevas tecnologías de la comunicación para el intercambio válido de información en el diagnóstico, el tratamiento y la prevención de enfermedades o lesiones, investigación y evaluación, y educación continuada de los proveedores de salud, todo con el interés de mejorar la salud de los individuos y sus comunidades". **(MemoPast, 2018)**

2.1.2 En que consiste y en que ayuda.

Hay dos modalidades en Telemedicina, que varían en la temporalidad:

- Asíncrona (tiempo diferido), en la cual se realiza una grabación, almacenamiento y transmisión por el médico de primer nivel y, posteriormente, la repetición de la información por el médico especialista, el cual, posteriormente, emite el diagnóstico y una recomendación.
- Síncrona (tiempo real), la cual se realiza una transmisión en tiempo real entre el paciente y el personal de salud, que llegara al diagnóstico y a la recomendación del tratamiento. **(Alejandro Dabaghi-Richerand, 2012)**

La Telemedicina facilita la equidad en el acceso a los servicios sanitarios, proporcionando una atención médica de alta calidad, independientemente de la localización geográfica, reduce la necesidad de realizar desplazamientos por parte de los pacientes y/o profesionales de salud. De igual manera reduce el tiempo de espera, en la realización del

diagnóstico y, consecuentemente, menor tiempo en el tratamiento. **(Joseba Rabanales Sotos, 2011)**

2.2 La Ciberseguridad.

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno.

La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- **Disponibilidad:** Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.
- **Integridad:** Salvaguarda la precisión y completitud de la información y sus métodos de proceso.
- **Confidencialidad:** Asegura que el acceso a la información está adecuadamente autorizado.

Pueden utilizarse técnicas de ciberseguridad para garantizar la disponibilidad, integridad, autenticidad, confidencialidad y no repudio del sistema. La ciberseguridad puede emplearse para garantizar el respeto de la privacidad de los usuarios. Pueden utilizarse técnicas de ciberseguridad para asentar la confianza de los usuarios.

Tecnologías tales como las redes inalámbricas y el Protocolo de Transmisión de Voz por Internet (VoIP) amplían el alcance y escala de Internet. Desde este punto de vista, el ciberentorno incluye a los usuarios, Internet, los dispositivos informáticos conectados al mismo y todas las aplicaciones, servicios y sistemas que pueden estar directa o

indirectamente conectados a Internet y al entorno de las redes de la próxima generación (NGN), sean éstas públicas o privadas. Por tanto, con la tecnología VoIP, un teléfono fijo forma parte del ciberentorno. No obstante, también los dispositivos aislados pueden formar parte del mismo si pueden compartir información con dispositivos informáticos conectados a través de medios extraíbles.

El ciberentorno incluye el software que se ejecuta en los dispositivos informáticos, la información almacenada (y transmitida) en estos dispositivos o la información que éstos generan. Las instalaciones y edificios donde residen los dispositivos también forman parte del ciberentorno. La ciberseguridad ha de tener en cuenta todos estos elementos.

El objetivo de la ciberseguridad es proteger el ciberentorno, un sistema que puede incluir múltiples entidades públicas y privadas, utilizando diversos componentes y distintos métodos de seguridad. Por tanto, conviene considerar la ciberseguridad en los siguientes términos:

- El conjunto de políticas y acciones que se utilizan para proteger las redes conectadas (incluidos los ordenadores, los dispositivos, el hardware, la información almacenada y la información en tránsito) del acceso y la modificación no autorizados, el robo, la interrupción u otras amenazas.
- Una evaluación y supervisión constantes de dichas políticas y acciones a fin de garantizar la continua calidad de la seguridad frente a la naturaleza voluble de las amenazas. **(Unión Internacional de Telecomunicaciones, 2008)**

2.2.1 Naturaleza del entorno de ciberseguridad de la empresa.

Las organizaciones han de establecer un plan global para satisfacer sus necesidades de seguridad. La seguridad no es la misma para todo el mundo. No puede alcanzarse la seguridad con un conjunto de módulos ensamblados. Conviene que las organizaciones consideren la seguridad como un proceso o perspectiva de protección de sistemas, redes, aplicaciones y servicios de red.

La seguridad ha de abarcar todas las capas de la red. Es necesario adoptar un método por capas para la seguridad que, combinado con una sólida gestión y aplicación de la política, brinde a los profesionales de la seguridad una serie de soluciones modulares, flexibles y adaptables.

La seguridad es difícil de probar, predecir y aplicar. La misma seguridad no es válida para todos. Las necesidades de seguridad y las estrategias recomendadas de cada organización son únicas y diferentes. Por ejemplo, cada empresa, proveedor de telecomunicaciones, operador de red o proveedor de servicios tiene una serie propia de necesidades comerciales y puede modificar su entorno de red para adaptarse a las mismas.

Por ejemplo, una empresa cerrada utiliza líneas privadas lógicas (por ejemplo, retransmisión de tramas) o físicas, dando acceso a distancia de manera selectiva a los empleados que necesitan acceder a Internet. Se llega a la web a través de un centro de datos Internet de un proveedor de servicios (responsable del establecimiento de un entorno seguro). La organización también proporciona acceso por marcación convencional a los empleados a distancia (por ejemplo, que trabajan desde un hotel). La empresa utiliza el correo privado entre los empleados sin acceso externo. También se utilizan las LAN inalámbricas.

Por otra parte, una empresa extendida, proveedor de telecomunicaciones, operador de red o proveedor de servicios, caracterizados por diversos modelos comerciales, pueden ofrecer soporte para el teletrabajo y el acceso distancia a la oficina a través de VPN IP por Internet o conexiones de menor costo y más veloces, incluido el acceso para fines generales a Internet como, por ejemplo, el interfuncionamiento entre el sistema de correo interno y el resto del mundo.

En cambio, en una empresa abierta el modelo comercial consiste en utilizar Internet para permitir a sus socios, proveedores y clientes acceder al centro de datos Internet gestionado por la empresa, e incluso les da acceso selectivo a las bases de datos y aplicaciones internas (por ejemplo, como parte de un sistema de gestión de la cadena de producción). Los usuarios internos y externos pueden acceder a la red de la empresa desde sus

hogares, oficinas distantes u otras redes utilizando dispositivos alámbricos o móviles. En este sentido, los requisitos de seguridad para este tipo de empresas son diferentes del resto.

En la *Figura 1* se pueden observar algunos tipos de empresa.

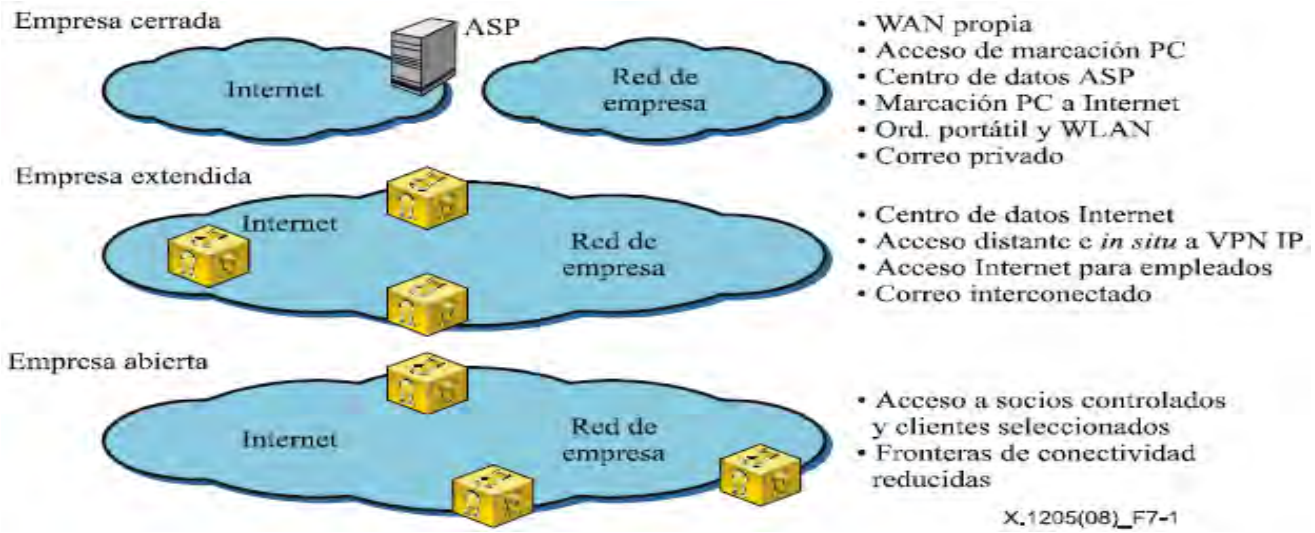

Figura 1. Tipos genéricos de empresa.

La ciberseguridad necesita de una gestión de riesgos. Este proceso conlleva la identificación del conjunto de componentes que han de protegerse. A fin de facilitar el análisis de riesgos, conviene considerar que los ataques se organizan en las siguientes categorías:

1. **Ataques de interrupción de servicios:** Este tipo de ataques inhabilita el acceso de los usuarios a los servicios deseados de manera temporal o permanente. Como ejemplos pueden citarse la falta de acceso a un sitio web o la incapacidad de llevar a cabo una transacción financiera o de iniciar una llamada de voz. Diversos tipos de ataques pueden conducir a una interrupción del servicio. Por ejemplo, la denegación de servicio (DoS, *Denial of Service*), los ataques de denegación de servicio

distribuidos (DDoS, *Distributed Denial of Service*), o los daños a edificios que albergan infraestructura crítica y pueden impedir a los usuarios acceder a un servicio.

2. **Activos en peligro:** Este tipo de ataques conlleva el robo o utilización fraudulenta de la infraestructura. Los ataques de este tipo pueden repercutir en la ciberseguridad si se llevan a cabo a gran escala.

3. **Piratería de componentes:** Este tipo de ataques supone tomar el control de algunos dispositivos y utilizarlos para lanzar nuevos ataques contra otros componentes del ciberentorno.

Cualquier elemento del ciberentorno puede considerarse un riesgo de seguridad, que en general se trata de una evaluación ponderada de las amenazas. El análisis de amenazas incluye la descripción del tipo de posibles ataques, los agresores potenciales y sus métodos y las consecuencias del éxito de un ataque. La evaluación de riesgos sumada al análisis de amenazas permite a la organización evaluar los posibles riesgos a que se enfrenta su red.

Los ataques pueden originarse en el ciberentorno, a través de gusanos u otro tipo de programas malignos; pueden ser ataques directos a la infraestructura básica, como los cables de telecomunicaciones, o pueden derivarse de las acciones de un usuario interno fiable. También es posible combinar distintos tipos de ataque. Por norma general, los riesgos se clasifican en altos, medios y bajos. El nivel de riesgo varía de un componente a otro del ciberentorno.

La seguridad depende fundamentalmente de la gestión de riesgos. Para gestionar los riesgos pueden utilizarse muchas técnicas distintas. Por ejemplo, puede desarrollarse una estrategia de defensa en la que se especifiquen las medidas que se adoptarán ante posibles ataques; puede recurrirse a la detección, que incluye la identificación de un ataque en curso o después de que se haya llevado a cabo; se puede formular una respuesta a un

ataque en la que se especifiquen las medidas que es necesario adoptar para frenar el ataque o reducir sus consecuencias; o se puede formular una estrategia de recuperación que permita a la red reanudar su funcionamiento a partir de un estado conocido. **(Unión Internacional de Telecomunicaciones, 2008)**

2.2.2 Amenazas a la ciberseguridad y metodología para contrarrestarlas.

Las amenazas a los sistemas de comunicaciones de datos incluyen las siguientes:

- Destrucción de información y/u otros recursos.
- Corrupción o modificación de información.
- Robo, eliminación o pérdida de información y/u otros recursos.
- Divulgación de información confidencial.
- Interrupción de servicios.

Las amenazas pueden clasificarse en accidentales o intencionales y pueden ser activas o pasivas. Las amenazas accidentales son las que existen sin que sean premeditadas. Ejemplos de ello pueden ser el disfuncionamiento del sistema, los errores operativos o del software. Las amenazas intencionales pueden ir del simple examen mediante herramientas de supervisión fáciles de conseguir a los ataques más perfeccionados que requieren conocimientos especiales del sistema. De llevarse a cabo, una amenaza intencional puede considerarse un "ataque".

Las amenazas pasivas son las que, de ponerse en práctica, no causarían ninguna modificación de la información contenida en el(los) sistema(s) y no se modificaría el funcionamiento ni el estado del sistema. La utilización de escuchas pasivas para observar la información que se transmite a través de una línea de comunicaciones es un tipo de realización de amenaza pasiva. Las amenazas activas a un sistema conllevan la alteración de la información del sistema o la modificación de su estado o funcionamiento. La modificación malintencionada de los cuadros de encaminamiento de un sistema por parte de un usuario no autorizado puede considerarse un ejemplo de amenaza activa.

Las características de seguridad suelen incrementar el coste de un sistema y pueden dificultar su utilización. Por consiguiente, antes de diseñar un sistema seguro, se aconseja identificar las amenazas específicas que hacen necesaria la protección. Esto se conoce como evaluación de amenazas. Un sistema tiene muchas vulnerabilidades, pero sólo algunas de ellas son explotables, porque el agresor carece de oportunidades o porque el resultado no justifica los esfuerzos necesarios ni el riesgo de ser detectado.

El siguiente paso consiste en analizar las amenazas, las vulnerabilidades (incluida la evaluación del impacto), las medidas para contrarrestarlas y los mecanismos de seguridad, con el fin de:

- Identificar las vulnerabilidades del sistema.
- Analizar la probabilidad de amenazas cuyo objetivo sea explotar estas vulnerabilidades.
- Evaluar las consecuencias de cada amenaza, en caso de que se llevase a cabo con éxito.
- Estimar el coste de cada ataque.
- Determinar el coste de las posibles medidas de respuesta.
- Seleccionar los mecanismos de seguridad que se justifican.

En algunos casos, las medidas no técnicas, como la cobertura de seguros, pueden ser alternativas rentables a las medidas de seguridad técnicas. En general, no es posible lograr una seguridad técnica perfecta. Por tanto, el objetivo debe ser elevar el coste de los ataques de manera que se reduzcan los riesgos a niveles aceptables. **(Unión Internacional de Telecomunicaciones, 2008)**

2.2.3 Seguridad de las comunicaciones de extremo a extremo.

La arquitectura de seguridad comprende todos los retos de seguridad de los proveedores de servicios, empresas y consumidores y es aplicable a las redes de voz, datos y convergentes inalámbricas, ópticas y alámbricas. La arquitectura observa los problemas

de seguridad de la gestión, control y utilización de la infraestructura de red, los servicios y las aplicaciones. La arquitectura de seguridad divide lógicamente un conjunto complejo de características de seguridad de la red de extremo a extremo en diversos componentes arquitecturales. Esta separación permite la adopción de un método sistemático para la seguridad de extremo a extremo que puede utilizarse para planificar nuevas soluciones de seguridad y para evaluar la seguridad de las redes existentes.

Una dimensión de seguridad es un conjunto de medidas de seguridad diseñadas para solventar un determinado aspecto de la seguridad de la red. Se definen ocho dimensiones que proporcionan protección contra las principales amenazas de seguridad. Estas dimensiones no se limitan a la red, sino que también se extienden a las aplicaciones y a la información de usuario extremo. Las dimensiones de seguridad se aplican a los proveedores de servicios o empresas que ofrecen servicios de seguridad a sus clientes. Las dimensiones de seguridad son:

- **Control de acceso:** Es el proceso de conceder permisos a usuarios o grupos de acceder a objetos tales como ficheros o impresoras en la red. El control de acceso está basado en tres conceptos fundamentales: identificación, autenticación y autorización.
- **Autenticación:** Capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.
- **No repudio:** Este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio:
    a) **No repudio en origen:** Garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío.
    b) **No repudio en destino:** El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo.
- **Confidencialidad de datos:** Asegura que el acceso a la información está adecuadamente autorizado.

- **Seguridad de las comunicaciones:** Disciplina que se encarga de prevenir que alguna entidad no autorizada que intercepte la comunicación pueda acceder de forma fácil a la información.
- **Integridad de los datos:** Salvaguarda la precisión y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.
- **Privacidad:** Control de la información que posee un determinado usuario que se conecta a la red.

A fin de proporcionar una solución de seguridad de extremo a extremo, las dimensiones de seguridad deben aplicarse a una jerarquía de equipos de red y agrupamientos funcionales que se denominan capas de seguridad. Se trata de las tres siguientes capas de seguridad:

1. Capa de seguridad de infraestructura.
2. Capa de seguridad de servicios.
3. Capa de seguridad de aplicaciones.

Las capas de seguridad identifican los puntos en que es necesario utilizar productos y soluciones de seguridad presentando una perspectiva secuencial de la seguridad de la red. Por ejemplo, en primer lugar, se tratan las vulnerabilidades de seguridad de la capa de infraestructura, luego las de la capa de servicios y las de la capa de aplicaciones. En la *Figura 2* se muestra cómo se aplican las dimensiones de seguridad a las capas de seguridad a fin de reducir las vulnerabilidades de cada capa.

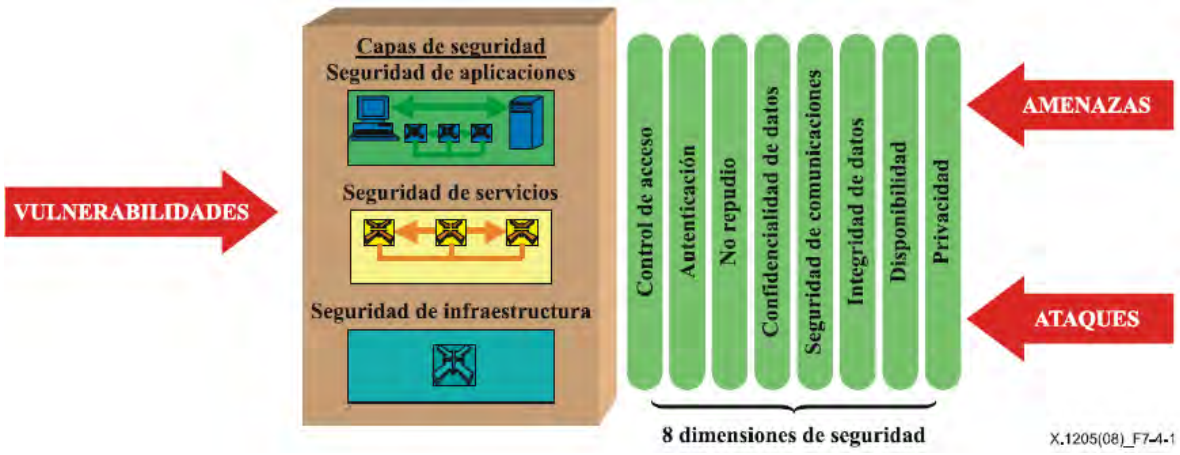

Figura 2. Aplicación de las dimensiones de seguridad a las capas de seguridad.

Un plano de seguridad es un determinado tipo de actividad de red protegida por las dimensiones de seguridad. Se definen tres planos de seguridad que representan tres tipos de actividades protegidas que se llevan a cabo en la red. Los planos de seguridad son:

1. Plano de gestión.
2. Plano de control.
3. Plano de usuario extremo.

Estos planos de seguridad observan las necesidades de seguridad específicas asociadas con las actividades de gestión de red, las actividades de control o señalización de red y las actividades de los usuarios extremos, respectivamente. Se sugiere que se diseñen las redes de manera que cualquier cosa que ocurra en uno de los planos de seguridad se mantenga aislado de los otros planos de seguridad.

En la *Figura 3* se muestra la arquitectura de seguridad con los planos de seguridad incluidos. El concepto de planos de seguridad permite diferenciar los problemas de seguridad específicos asociados con dichas actividades y da la capacidad de solucionarlos independientemente. Por ejemplo, en un servicio VoIP, que corresponde a la capa de seguridad de servicios, la tarea de asegurar la gestión del servicio debe ser independiente de la tarea de proteger el control del servicio. Estas tareas son independientes de la tarea

de proteger los datos de usuario extremo que transporta el servicio (por ejemplo, la voz del usuario). **(Unión Internacional de Telecomunicaciones, 2008)**

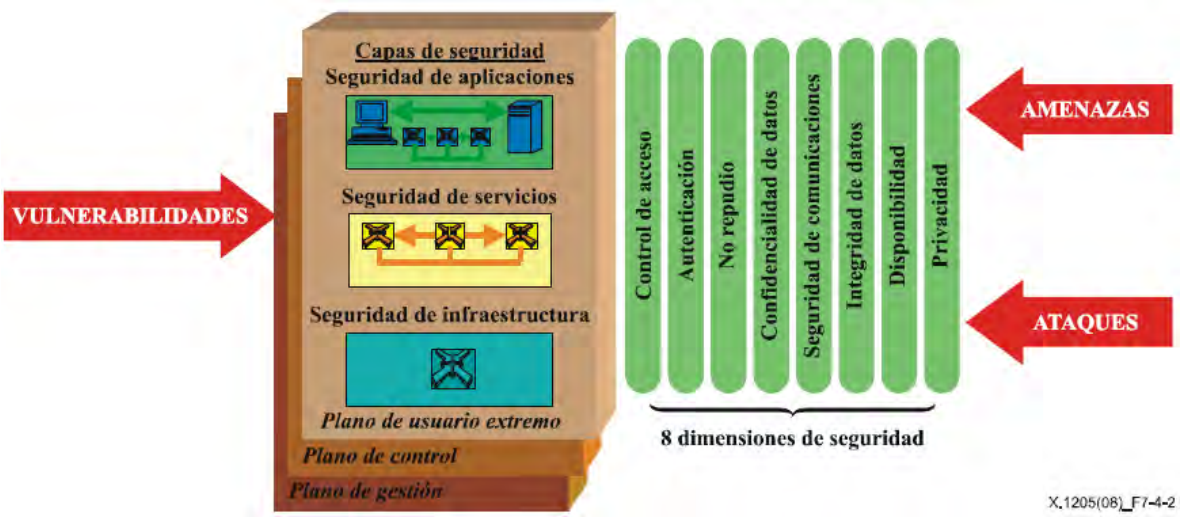

Figura 3. Los planos de seguridad reflejan los distintos tipos de actividades de la red.

2.3 Posibles estrategias de protección de la red.

La seguridad incluye todas las capas de la arquitectura de red. Este método es un buen punto de partida para el diseño de redes seguras. Esta descomposición permite a la capa superior definir sus propios requisitos de seguridad en esa capa específica y también le permite utilizar los servicios de seguridad de las capas inferiores. El método de seguridad por capas facilita el desarrollo de soluciones de seguridad, flexibles y adaptables en el nivel de red, el nivel de aplicación y el nivel de gestión de todas las organizaciones. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.1 Gestión de política de bucle cerrado.

Una política de seguridad adecuadamente diseñada y aplicada es un requisito básico para todos los tipos de empresas y organizaciones. La política de seguridad debe ser dinámica, en teoría y en práctica, y aplicarse, observarse y actualizarse de manera que refleje todos los cambios que experimenten la infraestructura de la empresa u organización y los requisitos de servicio.

La política de seguridad debe identificar claramente los recursos de la organización (y de la empresa) que corren riesgos y los correspondientes métodos para contrarrestar las amenazas. La política de seguridad debe prever la evaluación de vulnerabilidad y riesgos y definir las reglas de control de acceso adecuadas. La evaluación de vulnerabilidad y riesgos ha de llevarse a cabo en todos los niveles de la red. Con esta política deberá poderse identificar y descubrir las violaciones de seguridad y en ella estarán definidas las medidas de respuesta necesarias.

Se recomienda a los administradores de TI que utilicen herramientas de piratas para realizar la evaluación de vulnerabilidad de sus redes. Rige el principio de acceso con menos privilegios. Una de las tareas de los administradores de TI y de red es asegurarse de que se revisan los rastros de auditoría, cerrando así el bucle de la gestión de política. De encontrarse problemas en las auditorías, los administradores de TI velarán por que la política se actualice para reflejar las revisiones realizadas.

Una política de seguridad que no se observa es inútil. La observancia de la política de seguridad depende de las personas. Debe quedar claramente determinada la responsabilidad y dependencia de la observancia de la política. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.2 Gestión de acceso uniforme.

El término gestión de acceso se utiliza para definir sistemas que pueden utilizar tanto los servicios de autenticación como de autorización para controlar la utilización de un recurso. La autenticación es el proceso según el cual un usuario solicita a una red el establecimiento de una identidad. La autorización determina el nivel de privilegios de esa identidad de acuerdo con el control de acceso. El control del nivel de acceso depende de la definición y observancia de la política de control. En la *Figura 4* se muestra el modelo de referencia que ha de utilizarse como modelo de referencia para la autenticación y autorización seguras.

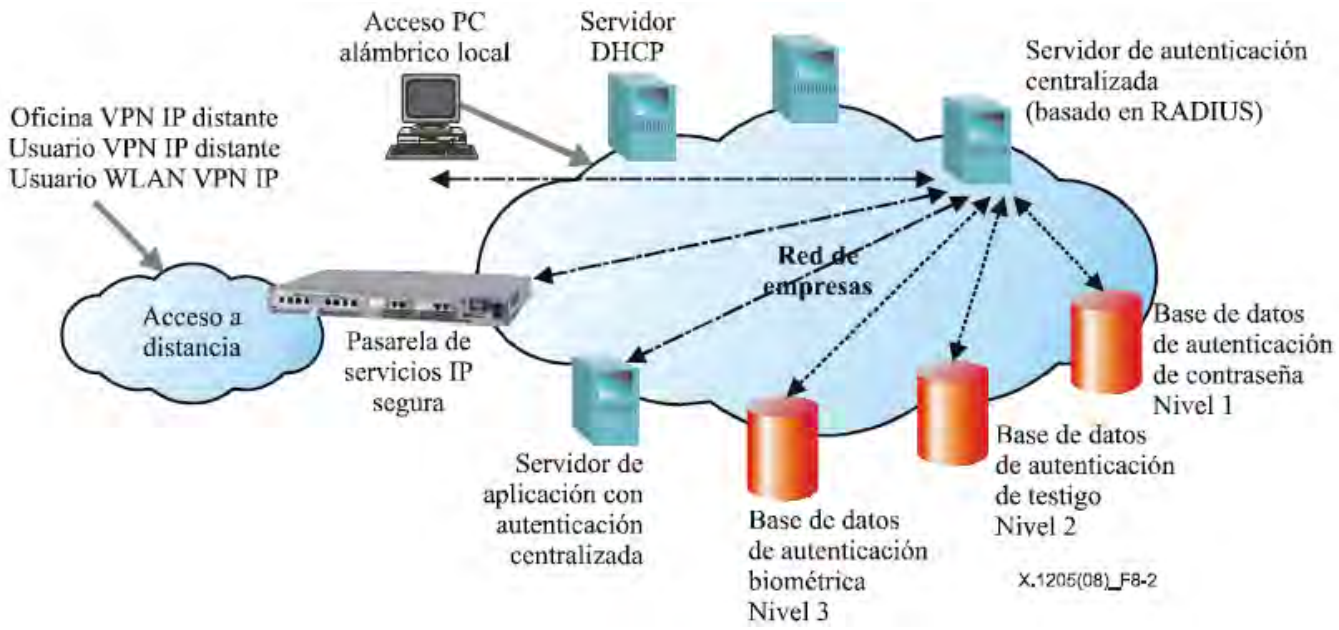

Figura 4. Modelo de referencia de autenticación y autorización seguras.

De la *Figura 4* se desprenden las siguientes recomendaciones:

- Utilizar un mecanismo de autenticación centralizada para facilitar la administración y eliminar la necesidad de almacenar localmente las contraseñas.
- Utilizar un sistema de autorización centralizada, estrechamente vinculado al sistema de autenticación, con la granularidad adecuada para cada empresa.
- Utilizar reglas de contraseñas fuertes (complejas) para todas las contraseñas.
- Almacenamiento seguro de todas las contraseñas en formato de cifrado en un solo sentido.
- Aplicación del principio de sencillez, que implica la facilidad de utilización y de administración. Un sistema sencillo es un sistema seguro, ya que es más fácil seguir las consignas de seguridad.
- Registro cronológico seguro de todos los eventos de seguridad relacionados con la autenticación y la autorización.

Los métodos para la gestión de acceso incluyen el filtrado de origen IP, los intermediarios y las técnicas basadas en credenciales. Cada método tiene sus ventajas y limitaciones.

Dependiendo del tipo de empresa, e incluso para un mismo tipo, pueden utilizarse uno o más métodos, o una combinación de ellos. Por ejemplo, una empresa puede optar por gestionar el acceso a las estaciones de trabajo utilizando el filtrado de origen IP y puede elegir utilizar un plan de credenciales para los demás usuarios.

Pueden utilizarse varios métodos para autenticar un usuario, entre los que se cuentan, las contraseñas, los pases de validez limitada, las técnicas biométricas, las tarjetas inteligentes y los certificados. La autenticación por contraseñas debe utilizar contraseñas fuertes (por ejemplo, de al menos, ocho caracteres con, como mínimo, uno alfabético, uno numérico y un carácter especial). La autenticación por contraseñas por sí sola puede no ser suficiente. De acuerdo con la evaluación de vulnerabilidad, puede ser necesario combinar la autenticación por contraseñas con otros procesos de autenticación y autorización como los certificados, el protocolo ligero de acceso al directorio (LDAP), el servicio de usuario de marcación de autenticación a distancia (RADIUS), Kerberos y la infraestructura de clave pública (PKI).

Todos los mecanismos de autenticación tienen ventajas e inconvenientes. Las combinaciones de ID de usuario/contraseña son sencillas, baratas y fáciles de gestionar, aunque los usuarios suelen tener dificultades para recordar muchas contraseñas complejas. Los sistemas de autenticación de doble y de triple factor añaden solidez a la autenticación, pero son onerosos, más complejos y son difíciles de mantener.

Un sistema de "contraseña única" con contraseñas fuertes puede ser una buena solución para la autenticación y autorización de empresa. Un sistema de este tipo proporciona una alta seguridad de autenticación, autorización granular y es fácil de administrar. Con este sistema, se sincroniza la contraseña fuerte única de usuario con muchas aplicaciones y sistemas de toda la empresa con fines de autorización y autenticación. Todos los sistemas y aplicaciones de la empresa remiten las funciones de autenticación y autorización al sistema de contraseña única. Al haber sólo una contraseña fuerte que recordar, el sistema es más sencillo de utilizar y no es probable que los usuarios lo eviten. Éstas son las ventajas del sistema de contraseña única:

- Un único método coherente para la creación de contraseñas.

- Un único método coherente para la autenticación y la autorización.
- Un único método para el registro y terminación de cuentas de usuario.
- Observancia de las directrices firmes de la empresa sobre contraseñas.
- Coherencia: Los usuarios saben qué deben hacer.
- Normalización: Facilidad de soporte y adopción.
- Rapidez: Interfaces y API normalizadas.
- Coste reducido y menos peticiones de ayuda.

La empresa abierta y extendida encuentra más problemas para diseñar su política de gestión de acceso. Resulta conveniente considerar la gestión de acceso como parte integrante de la política de seguridad. Estas organizaciones deben diseñar un sistema de gestión de acceso uniforme con reglas de granularidad más fina que han de aplicarse adecuadamente a:

- Directorios y bases de datos de identidades.
- Múltiples sistemas de autenticación como contraseñas, Kerberos, TACACS y RADIUS.
- Anfitriones, aplicaciones y servidores de aplicación.

El sistema de gestión de acceso uniforme debe gestionar las sesiones por usuario después de que éste haya sido autenticado. Se recomienda la utilización de una configuración flexible y una aplicación de política con reglas de granularidad fina capaces de tratar objetos específicos. También conviene realizar la adecuada supervisión, contabilidad y auditorías de seguridad. Es recomendable utilizar cuentas exclusivas para cada administrador donde se puedan rastrear las acciones realizadas por cada usuario, responsabilizándolos de las mismas. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.3 Comunicaciones seguras.

Las redes unificadas pueden transportar paquetes de voz, datos y vídeo. La finalidad de proteger el tráfico de red es garantizar la confidencialidad, la integridad y la exactitud de las comunicaciones de red. También ha de preverse la seguridad de las llamadas y el

tráfico de señalización en las redes telefónicas. Ha de utilizarse una tecnología de cifrado para las redes de datos y voz y las redes móviles. El cifrado puede obtenerse a través de:

- Técnicas VPN con IPSec, con encabezado de autenticación (AH) y encapsulación de cabida útil de seguridad (ESP) o tunelización gracias al protocolo de tunelización de capa 2 (L2TP).
- La gestión de claves puede basarse en el intercambio de claves de Internet (IKE).
- La gestión de certificados se basa en la infraestructura de clave pública (PKIX).
- El protocolo de gestión de certificados (CMP) y el protocolo de estado de certificado en línea (OCSP).
- En la capa de aplicación, mediante el uso de TLS con claves fuertes.

Es importante utilizar algoritmos de cifrado normalizados y funciones de aleatorización como DES, 3DES, AES, RSA y DSA. MD5 y SHA-1 podrían utilizarse para la integridad del mensaje, y Diffie-Hellman y RSA para el intercambio de claves.

NOTA – El NIST (National Institute of Standards and Technology) alienta la utilización del SHA-256 (Algoritmo de Hash Seguro (*Secure Hash Algorithm*) con claves codificadas de 256 bits) en lugar del SHA-1.

La privacidad equivalente a la de las redes alámbricas (WEP, *Wired Equivalent Privacy*), define una técnica para proteger la transmisión aérea entre los puntos de acceso de LAN inalámbrica (WLAN, *Wireless LAN*) y las tarjetas de interfaz de red (NIC, *Network Interface Cards*). Se ha visto que este protocolo no es seguro. Para dar seguridad a las WLAN con WEP se han de añadir medidas de protección como IPSec. Alternativamente, para lograr una mayor protección se puede utilizar el acceso protegido a Wi-Fi (WPA, *Wi-Fi Protected Access*). **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.4 Seguridad de profundidad variable.

Una VLAN (LAN Virtual) es un grupo de dispositivos de red, tales servidores y otros recursos, configurado para funcionar como si estuvieran conectados a un mismo segmento de red. En una VLAN, los recursos y servidores de otros usuarios en la red serán invisibles para los miembros de las demás VLAN. Las VLAN ayudan a cumplir los requisitos de

calidad de funcionamiento por cuanto dividen la red de manera más eficaz. Además, restringen la distribución de información en modo difusión y el tráfico entre nodos, de modo que se reduce el volumen de tráfico ajeno que pasa por la red. Todos los paquetes circulan entre varias VLAN pueden atravesar también un encaminador, por lo que pueden aplicarse medidas de seguridad en este dispositivo para limitar el acceso al segmento.

La seguridad por capas permite ofrecer grados de seguridad variables. Cada nivel de seguridad adicional se basa en las capacidades de la capa inferior y ofrece mayor seguridad con una granularidad más fina.

Por ejemplo, pueden recurrirse a las VLAN para efectuar una segmentación y una compartimentación básicas de la red, lo que permite contener y segmentar las diversas funciones de la empresa en sus propias redes de área local privadas controlando estrictamente o prohibiendo el intercambio de tráfico con otros segmentos de la VLAN. De la implantación de VLAN para zonas pequeñas o medianas dentro de la empresa se desprenden varios beneficios. Así pues, el uso de "etiquetas" VLAN permite dividir el tráfico en grupos específicos, como finanzas, recursos humanos y diseño. La separación de los datos sin que haya "fugas" entre las VLAN es un elemento importante para la seguridad.

Puede lograrse una segunda capa de seguridad utilizando un perímetro y firewall-filtros distribuidos en puntos estratégicos de la red. La capa de firewalls permite segmentar aún más la red en zonas pequeñas y ofrece conexiones seguras con la red pública. Los firewalls limitan el acceso al tráfico interno y externo a los protocolos explícitamente configurados en ese firewall. Además, puede introducirse la autenticación de usuarios entrantes o salientes. Los firewalls que soportan la traducción de dirección de red (NAT) permiten optimizar el direccionamiento IP dentro de la red.

Los firewalls aportan otra capa de protección útil para el control de acceso. La aplicación de un acceso conforme a la política permite la personalización del acceso de acuerdo con las necesidades de la empresa. El uso de un método de firewalls distribuidos tiene además la ventaja de que puede adaptarse a la evolución de las necesidades de la empresa. Pueden instalarse firewalls personales en los sistemas extremos para garantizar la integridad de las aplicaciones.

Como tercera capa de seguridad pueden añadirse VPN de capa 3. Las VPN afinan la granularidad del control de acceso y la personalización. Las VPN aportan seguridad de granularidad muy fina hasta el nivel de usuario y permiten el acceso a distancia seguro para los emplazamientos distantes y los socios comerciales. Con las VPN no se necesita utilizar líneas dedicadas. El encaminamiento dinámico por túneles seguros en Internet es una solución muy segura, fiable y adaptable. El uso de VPNs sumadas a las VLAN y los firewalls facilitan al administrador de red la limitación del acceso por usuarios o grupos de usuarios de acuerdo con los criterios de la política y las necesidades de la empresa. Las VPN garantizan más sólidamente la integridad y la confidencialidad de los datos. En esta capa puede aplicarse un fuerte cifrado de datos para lograr la confidencialidad y la integridad de los datos.

Las soluciones de seguridad basadas en el método por capas son flexibles y adaptables a las necesidades de seguridad de la empresa. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.5 Gestión de la seguridad.

La gestión de la seguridad es más un método global que un conjunto de características de seguridad de un elemento de red determinado. Cada una de las zonas que se exponen a continuación representa un componente crítico que necesita atención para lograr formar un tejido protector alrededor de la red.

Hay nueve dominios de gestión de red clave cuya seguridad ha de tenerse en cuenta antes de que el plano de gestión de red pueda considerarse seguro. Éstos son:

1. Registros cronológicos de actividad seguros.
2. Autenticación del operador de red.
3. Control de acceso para los operadores de red.
4. Cifrado del tráfico de gestión de red.
5. Acceso a distancia seguro para los operadores.
6. Firewall.
7. Detección de intrusos.
8. Endurecimiento de SO.

9. Software sin virus **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.6 Gestión de política.

Los registros cronológicos seguros pueden utilizarse para mantener una auditoría de las actividades de los usuarios o el administrador y de los eventos generados por el dispositivo mismo, y son un elemento fundamental para cerrar el bucle de la gestión de política. Los datos brutos recopilados se denominan "registro cronológico de auditoría", y el trayecto verificable de eventos gracias a los registros cronológicos de auditoría se denomina "rastro de auditoría". Para ser eficaces, los registros cronológicos de auditoría de seguridad tienen que contener suficiente información para permitir una investigación o análisis después de los incidentes de seguridad.

Estos registros cronológicos de auditoría sirven para lograr varios objetivos de seguridad, incluidos la responsabilidad individual, la reconstrucción de eventos pasados, la detección de intrusos y el análisis de los problemas. Los registros cronológicos también pueden utilizarse para el análisis de tendencias a largo plazo.

La información de los registros cronológicos de auditoría ayuda a identificar la causa primera de un problema de seguridad y a evitar futuros incidentes. Esta información debe almacenarse de manera segura. Por ejemplo, los registros cronológicos de auditoría pueden emplearse para reconstruir la secuencia de eventos que ha conducido a un problema, como que un intruso logre acceso no autorizado a los recursos del sistema, o el disfuncionamiento del sistema causado por una configuración incorrecta o una aplicación fallida. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.7 Gestión de acceso seguro.

La autenticación del operador de red debe basarse en una fuerte autenticación centralizada de los operadores y administradores de red. La administración centralizada de contraseñas contribuye a la solidez de las contraseñas y elimina la necesidad de almacenar localmente las contraseñas en los elementos de red y los sistemas EMS. RADIUS es el mecanismo básico para automatizar la autenticación centralizada.

Para controlar el acceso de los operadores de red han de seguirse las prácticas adecuadas. Por ejemplo, a fin de determinar el nivel de autorización, puede emplearse una técnica basada en servidores RADIUS para lograr un nivel básico de control de acceso, y añadirse un servidor LDAP para que la granularidad del control de acceso sea más fina, de ser necesario. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.8 Cifrado del tráfico de gestión de red.

Se recomienda el cifrado de todo el tráfico de datos utilizado para la gestión de red a fin de garantizar la confidencialidad e integridad de los datos. Con cada vez más frecuencia, las empresas emplean una gestión de red en banda, por lo que es necesario separar el tráfico de gestión mediante cifrado.

El cifrado del tráfico de gestión da una fuerte protección contra los usuarios internos, a excepción de un pequeño grupo que tiene acceso legítimo a las claves de cifrado. Es necesario el cifrado entre los clientes del centro de operaciones de red (NOC) y los servidores y/o elementos de red del sistema de gestión de elementos (EMS), lo que incluye el tráfico SNMP, pues se sabe que SNMP v1 y v2 tienen vulnerabilidades resueltas en SNMP v3.

Dependiendo del tipo de tráfico, los protocolos de seguridad que hay que utilizar en estos enlaces son TLS, IPSec y el intérprete de comandos seguro (SSH). SSH es un protocolo de seguridad de nivel de aplicación que sustituye directamente a Telnet y FTP, pero que normalmente no puede utilizarse para proteger otro tipo de tráfico. Por otra parte, el protocolo IPSec sólo se ejecuta entre la capa de red (capa 3) y la capa de transporte (capa 4) y puede emplearse para proteger cualquier tipo de tráfico de datos, independientemente de las aplicaciones y protocolos utilizados.

IPSec es el método más recomendable, aunque SSH puede utilizarse si el tráfico sólo está formado por Telnet y FTP. La tecnología TLS puede proteger el tráfico HTTP cuando se utiliza en una capacidad de la gestión de red entre los clientes NOC y el EMS y/o los elementos de red. Para proteger el tráfico de gestión puede recurrirse a un dispositivo VPN IPSec externo en diversas partes de la red. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.9 Acceso a distancia seguro para los operadores.

Debe darse seguridad a los operadores y administradores que gestionan la red a distancia a través de una red pública. La mejor solución es crear una VPN con IPSec, ya que así se garantizará el fuerte cifrado y autenticación de todos los operadores distantes. Debe situarse una VPN en la interfaz del sistema de gestión y todos los operadores deberán estar equipados con clientes de acceso extranet en sus ordenadores portátiles o de escritorio. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.10 Firewall.

Para aplicar los principios de seguridad de profundidad variable conviene dividir el entorno de gestión de red con VLAN y firewalls. El firewall controla el tipo (protocolo, número de puerto, dirección de origen y destino) de tráfico utilizado para cruzar la frontera entre distintos dominios de seguridad. Dependiendo del tipo de firewall (aplicación por oposición a filtrado de paquetes), también puede ampliarse hasta comprender el filtrado del contenido de aplicación del flujo de datos. La ubicación del firewall, su tipo y las reglas de filtrado dependen específicamente de la implementación de cada red. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.11 Detección de intrusos.

Los sistemas de detección de intrusos basados en el anfitrión pueden incorporarse a los servidores de gestión para defenderse de las intrusiones en la red. Los sistemas de detección de intrusos pueden emplearse para advertir a los administradores de red de la posibilidad de que ocurra un incidente de seguridad, como la puesta en peligro de un servidor o un ataque de denegación de servicio. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.12 Capa de seguridad de aplicación.

Se recomienda el endurecimiento de todos los sistemas operativos utilizados en la gestión de red. Es necesario endurecer todos los sistemas operativos utilizados para la gestión de red, ya sean sistemas operativos generales o sistemas operativos en tiempo real incorporados. En el caso de los sistemas operativos que no disponen de directrices de

endurecimiento específicas, es necesario remitirse al fabricante del sistema para obtener los parches y procedimientos más recientes. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.13 Software sin virus.

Todo el software, ya se haya creado dentro de la empresa o se haya comprado a terceros, ha de examinarse para garantizar, en la medida de lo posible, que no tiene virus. Ha de diseñarse un proceso para la detección de virus, que comprenda el análisis de todo el software con una herramienta de detección de virus específica antes de poder instalarlo. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.14 Seguridad por capas en la aplicación, la red y la gestión de red.

Cada organización o empresa tiene un umbral de seguridad y una infraestructura tecnológica distinta. Las aplicaciones Internet representan mayores riesgos y amenazas para las empresas. Estas aplicaciones deben tener algún tipo de seguridad incorporada en el nivel de aplicación, aunque con las funcionalidades de seguridad de capas de red inferiores se puede mejorar la seguridad de las aplicaciones.

Al nivel de aplicación, se recomienda utilizar una política de seguridad con granularidad fina. En la medida de lo posible, se deben direccionar los objetos en el nivel de identificadores uniformes de recursos (URI, *Uniform Resource Identifiers*). Han de inhabilitarse las funcionalidades innecesarias y, siempre que se pueda, conviene utilizar TLS. Se recomienda el uso de pasarelas a nivel de aplicación, así como un sólido mecanismo de autenticación y autorización. Si la infraestructura de seguridad lo permite, los servicios de correo electrónico deben protegerse con S/MIME y técnicas como PGP.

En la capa de red se habrán de utilizar las técnicas expuestas en la cláusula 2.3.15 para garantizar una seguridad aceptable en la empresa. Esta seguridad se logra empleando la arquitectura de capas, que puede adaptarse a las necesidades de seguridad de cada empresa.

La protección del tráfico de gestión de red es uno de los requisitos fundamentales de la protección de la red. Para ello, en primer lugar, es necesario verificar que el sistema operativo está endurecido contra las amenazas conocidas. Será necesario obtener del fabricante del sistema operativo los últimos parches y procedimientos de endurecimiento del mismo. Habrán de tomarse las medidas necesarias para garantizar que todo el software instalado está libre de virus conocidos. Es preferible cifrar siempre todo el tráfico de gestión con IPSec o TLS para proteger el tráfico HTTP. El cifrado es una práctica adecuada y recomendable si el tráfico transita fuera de la LAN local. Se recomienda utilizar SNMPv3 y RADIUS para controlar el acceso a distancia de los operadores de red, además de múltiples mecanismos de control en varios niveles, que incluyan el uso de contraseñas y la capacidad de administrar de manera centralizada el sistema de control de acceso. Es fundamental la protección de los registros cronológicos del tráfico de gestión de red. **(Unión Internacional de Telecomunicaciones, 2008)**

2.3.15 Supervivencia de la red incluso en caso de ataque.

En el entorno actual, las redes de empresa soportan operaciones fundamentales y son vitales para su funcionamiento. La red debe ser segura, fiable y estar disponible para todos los socios comerciales en cualquier momento.

Hay muchas técnicas que pueden emplearse para garantizar la fiabilidad de la red, de la que depende el adecuado funcionamiento de una red en caso de fallo de los componentes de software y/o hardware. No obstante, en presencia de amenazas de seguridad, ha de emplearse el concepto de redes supervivientes. Una red superviviente es una red que sigue llevando a cabo una serie de funcionalidades básicas mínimas convenientemente en caso de sufrir un ataque. La funcionalidad básica consiste en la prestación básica y oportuna de servicios, incluso si parte de la red es inalcanzable o está en estado de fallo a causa de un ataque.

Para diseñar redes supervivientes es necesario empezar organizando los servicios de red en dos categorías: servicios básicos y servicios no básicos. Por supervivencia se entiende que la red pueda resistir un ataque. Es indispensable contar con una estrategia clara sobre cómo tratar y recuperarse de los ataques.

Dependiendo del tipo de ataque, el administrador de red puede considerar diversas estrategias de resistencia, identificación y recuperación. Una de las características de las redes supervivientes es su adaptabilidad. Por ejemplo, la red puede reencaminar el tráfico de un servidor a otro, si se detecta en el primer servidor una intrusión o un ataque.

Es necesario determinar en la fase de diseño de la política de seguridad cuáles son los servicios básicos que la red debe poder prestar incluso en caso de ataque. En esta fase se debe identificar cómo la red resistirá al ataque, cómo la red superará tales ataques y cuál será el mejor método para recuperarse de ellos. En este análisis se tendrán en cuenta los sistemas de gestión, los anfitriones, las aplicaciones, los Routers y los Switches.

Puede aumentarse la resistencia de las redes supervivientes a los ataques utilizando mecanismos de control de acceso con autenticación y cifrado fuertes. El filtrado de mensajes y paquetes y la segmentación de red y servidor también mejoran la resistencia de la red en caso de ataque. Con las adecuadas técnicas de detección de intrusos se puede identificar un ataque. Pueden emplearse las técnicas de copia de seguridad adecuadas para la recuperación del sistema y la red. **(Unión Internacional de Telecomunicaciones, 2008)**

3 Discusión

Actualmente el SACMED realiza parte de los procesos de control y seguridad acorde a las. normas que han sido revisadas en este documento, sin embargo, no se cuenta con políticas estrictas que permitan garantizar la ejecución de las normas. El análisis será realizado tomando en cuenta las recomendaciones de los estándares analizados en este trabajo y con ello tener una medición del nivel de seguridad de la infraestructura de red de Telemedicina.

El proyecto de Telemedicina cuenta con unidades Consultantes y de Interconsulta las cuales son interconectadas con equipo de telecomunicaciones para realizar cada una de las consultas. Además, el proyecto incluye contar con servicios de Teleeducación para su uso en campañas de prevención, educación médica, entre otros.

Como primer punto, los usuarios usan contraseñas fuertes, esto gracias al directorio activo el cual no permite el uso de contraseñas fáciles. Además, los usuarios cambian de contraseña con regularidad, aproximadamente cada 3 meses.

Por otra parte, las computadoras que se usan para este proyecto no cuentan con un antivirus como tal y eso es algo que considero incorrecto ya que, un atacante con ayuda de un USB podría infectar o irrumpir en dicha computadora, además de que un antivirus brinda más beneficios en el momento que el médico por algún descuido descargue un archivo infectado desde Internet y éste no se dé cuenta.

Sin embargo, para evitar esto ellos tienen bloqueado el acceso a diversas páginas web, así como también a las redes sociales. Únicamente tienen acceso a los expedientes y a ciertas páginas web lo cual es algo bueno porque en muchas ocasiones el usuario se distrae por tener todo libremente y no se da cuenta de lo que descarga y de los beneficios o desventajas que traen para la computadora.

Otro punto importante es que las computadoras usan direcciones IP privadas algo que sirve para identificar a los equipos o dispositivos dentro de una red privada y mantenerlas aisladas de las direcciones IP públicas. Cada dispositivo debe tener una IP distinta de los demás, de lo contrario ocasionaría problemas. Además, para poder conectar una red privada con Internet, el cual se

considera una red pública, se necesita el NAT que sirve como puente o intermediario y permite cosas como poder entrar desde una computadora que tiene una IP privada a un servidor donde está un sitio web que tiene una IP pública.

Por último, en la red de Telemedicina se tiene implementado una VPN para el acceso a distancia la cual ayuda en la integridad, confidencialidad y seguridad de los datos. Además, las VPN reducen los costos, son sencillas de usar, facilita la comunicación entre dos usuarios en lugares distintos y con las VPN no se necesita utilizar líneas dedicadas. El uso de las VPN sumadas a las VLAN y los firewalls facilitan al administrador de red la limitación del acceso por usuarios o grupos de usuarios de acuerdo con los criterios de la política y las necesidades de la empresa.

4 Conclusiones

La ciberseguridad es una práctica en continua evolución, si bien día a día aparecen nuevos y complejos tipos de incidentes, aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las personas. En consecuencia, se requieren efectivas acciones de concientización, capacitación y difusión de mejores prácticas.

Es necesario mantener un estado de alerta y actualización permanente: la seguridad es un proceso continuo que exige aprender sobre las propias experiencias.

No es posible establecer un entorno 100% seguro, se tiene que asumir. Es necesario realizar con frecuencia auditorías que indiquen los niveles de seguridad para ser conscientes de los riesgos que está asumiendo la organización.

Las organizaciones no pueden permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de las organizaciones.

Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

Los ataques están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso las personas, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios.

5 Bibliografía

Alejandro Dabaghi-Richerand, A. C.-G. (2012). Telemedicina en México. En A. C.-G. Alejandro Dabaghi-Richerand, *Historia y Filosofía de la medicina* (Vol. Vol.57, págs. 353-357). México: Anales Médicos (Asociacion Medica ABC) . Obtenido de http://www.medigraphic.com/pdfs/abc/bc-2012/bc124n.pdf

Cisco. (22 de Septiembre de 2019). *Cisco*. Obtenido de https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

It Governance. (14 de Mayo de 2019). Obtenido de https://www.itgovernance.co.uk/what-is-cybersecurity

Joseba Rabanales Sotos, I. P.-T. (Febrero de 2011). Tecnologías de la Información y las Comunicaciones: Telemedicina. *Clínica de Medicina de Familia, 4*, 42-48. Obtenido de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1699-695X2011000100007

Landi, H. (20 de Noviembre de 2018). *hea!thcare innovation*. Obtenido de https://www.hcinnovationgroup.com/cybersecurity/news/13030900/cybersecurity-telehealth-and-interoperability-top-of-mind-for-it-execs-in-2019

Secretaria de Salud. (30 de Noviembre de 2012). Obtenido de http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2012.pdf

MemoPast. (04 de Julio de 2018). Obtenido de https://www.memopast.com/blog-memopast/item/6-telemedicina-un-avance-en-la-relacion-medico-paciente

Unión Internacional de Telecomunicaciones. UIT-T X.1205. (Abril de 2008). *Aspectos generales de la ciberseguridad.*