UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Proyecto de Investigación previo a la obtención del título de Ingeniero en Sistemas y Computación

TRABAJO DE TITULACIÓN

EVALUACIÓN DE RIESGOS EN EL AMBIENTE INFORMÁTICO DEL HOSPITAL GENERAL UNIVERSITARIO ANDINO DE CHIMBORAZO UTILIZANDO LA HERRAMIENTA MSAT

AUTOR:

Gabriela Sanndy Ortega Siguencia

TUTOR:

Mgs. Ana Elizabeth Congacha Aushay., Mgs.

RIOBAMBA - ECUADOR
2020

VEREDICTO DE LA INVESTIGACIÓN

Los miembros del tribunal de Graduación del proyecto de investigación de título: "**EVALUACIÓN DE RIESGOS EN EL AMBIENTE INFORMÁTICO DEL HOSPITAL GENERAL UNIVERSITARIO ANDINO DE CHIMBORAZO UTILIZANDO LA HERRAMIENTA MSAT",** presentado por la estudiante Srta. Gabriela Sanndy Ortega Siguencia, dirigido por la Mgs. Ana Elizabeth Congacha Aushay

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación escrito, con fines de graduación en el cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para la constancia de lo expuesto firman:

Mgs. Ana Congacha ……
Tutora del proyecto Firma

Mgs. Estela Narváez ……
Miembro del Tribunal Firma

Mgs. Diego Reina ……
Miembro del Tribuenal Firma

AUTORIA DE LA INVESTIGACIÓN

La responsabilidad del contenido de este Proyecto de Graduación corresponde exclusivamente a Gabriela Sanndy Ortega Siguencia, autor del proyecto de investigación, a la Mgs. Ana Congacha, Directora de Tesis; y el patrimonio intelectual de la Universidad Nacional de Chimborazo.

Autor

……..

Gabriela Sanndy Ortega Siguencia

171874953-2

Directora del Proyecto

……..

Mgs. Ana Elizabeth Congacha Aushay

060313796-9

DEDICATORIA

El presente proyecto de investigación está dedicado en primer lugar a Dios, quién me ha ido poniendo en el camino, a situaciones y personas adecuadas, que han contribuido como fuentes de inspiración a lo largo de todo mi trayecto universitario, para poder haber culminado una meta más en mi vida. A mis padres, Luis y Carmen, quienes, con mucho amor y esfuerzo, han ido forjando poco a poco, en mí, el interés de esfuerzo y valores que me servirán a lo largo de mi vida personal y profesional. A mis hermanos, quienes, con su constante apoyo, han sido mi guía y ejemplo a seguir. A mis amigos, por todos los momentos inolvidables vividos en mi vida universitaria y por impulsarme a seguir adelante. A los docentes de la carrera, que, gracias a su compromiso con una visión de enseñanza, crean día a día grandes profesionales.

Gabriela Sanndy Ortega Siguencia

AGRADECIMIENTO

Agradezco a Dios por permitirme continuar con mis objetivos planteados, a mis padres, hermanos, amigos y a todas las personas que me han acompañado en esta etapa.

A la Universidad Nacional de Chimborazo, en especial a la carrera de Ingeniería en Sistemas y Computación que me abrieron sus puertas para forjarme profesionalmente.

Un especial agradecimiento a la Mgs. Ana Congacha, tutora de tesis, por su constante apoyo, tiempo y conocimientos, de igual manera a mis tutores colaboradores Mgs. Estela Narváez y Mgs. Diego Reina.

A mis compañeros de clases, con los que he podido compartir buenos momentos y con los que he tenido la oportunidad de compartir conocimientos.

Gabriela Sanndy Ortega Siguencia

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la actualidad una organización para ser competitiva, debe contar con sistemas, recursos y plataformas de información y comunicación ágiles; con un alto nivel de disponibilidad, lo que exige una gestión efectiva y un amplio proceso de transformación digital. El proceso de transformación digital, propicia que puedan darse ataques contra la seguridad informática de las organizaciones desde cualquier parte del mundo utilizando como herramienta tan solo un ordenador.

El proyecto de investigación aplicado en el Hospital General Universitario Andino de Chimborazo, permitió evaluar los puntos débiles del entorno de seguridad de Tecnologías de la Información, utilizando la herramienta MSAT, que usa estándares internacionales ISO 17799, NIST 800.x, orientaciones normativas del Grupo Trutsworthy Computing de Microsoft y otras fuentes de seguridad externas.

Tras el proceso de evaluación de riesgos, se obtuvieron resultados que visualizan las áreas de análisis, según el sector empresarial al que pertenece y la comparación con respecto a la defensa en profundidad implantado por la organización, obteniéndose como resultado un desequilibrio significativo en las áreas de operaciones y personal.

Con el análisis de los resultados obtenidos, se generó una guía fundamentada en una serie de parámetros de la norma ISO/IEC 27001.2005, donde se propone la utilización del modelo de W. Edward Deming. Esta guía de actividades prioritarias, tiene como finalidad el establecimiento de medidas preventivas y correctivas que proporcionen viabilidad y garanticen niveles superiores de seguridad de la información en el Hospital General Universitario Andino de Chimborazo.

Palabras claves: Evaluación de riesgos, Ataques informáticos, MSAT, Seguridad.

ABSTRACT

Abstract

Nowadays an organization for being competitive, must have agile information and communication systems, resources, and platforms; with a high level of availability, which requires effective management and an extensive digital transformation process. The digital transformation process encourages attacks against the IT security of organizations from anywhere in the world using only a computer as a tool. The research project applied at the Hospital General Universitario Andino Chimborazo, made it possible to evaluate the weak points of the Information Technology security environment, using the MSAT tool, which uses international standards ISO 17799, NIST 800.x, the Group's normative guidelines. Trustworthy Computing from Microsoft and other external security sources. After the risk assessment process, results were obtained that visualize the areas of analysis, according to the business sector to which it belongs and the comparison concerning the defense in depth implemented by the organization, resulting in a significant imbalance in the areas of operations and personnel. With the analysis of the results obtained, a guide based on a series of parameters of the ISO / IEC 27001.2005 standard was generated, where the use of the W. Edward Deming model is proposed. The purpose of this guide to priority activities is to establish preventive and corrective measures that provide viability and guarantee higher levels of information security at the Hospital General Universitario Andino Chimborazo.

Keywords: Risk assessment, Computer attacks, MSAT, Security.

Reviewed by:
Dra. Nelly Moreano Ojeda
ENGLISH PROFESSOR
c.c. 1801807288

INTRODUCCIÓN

El avance tecnológico, junto con el uso generalizado de internet y la implementación continua de nuevas tecnologías de la información y comunicación (TIC), experimentados en los últimos años, han generado en las organizaciones indiferentemente de su tamaño, inconvenientes de disponibilidad, integridad y/o confidencialidad de la información, siendo que la información es un activo que tiene un valor fundamental para la organización y debe ser protegida de un modo adecuado (INCIBE, 2015).

Por otra parte, los hospitales y centros de atención médica resultan un blanco atractivo para los cibercriminales, dado que cumplen un rol vital para el bienestar de una sociedad (Harán, 2020). Esto los convierte en un objetivo perfecto para la extorsión mediante una gran variedad de ataques. En Ecuador, a pesar de que no se han evidenciado ataques significativos a hospitales o centros de salud, tras el reporte de incidentes del 2018 de ESET Security, se evidencia que el índice de infecciones ransonware de Ecuador y Venezuela es superior al resto de países (ESET, 2018), por ello, es importante identificar los peligros que afectan a la seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardas.

Como propuesta para mejorar la seguridad en el Hospital General Universitario Andino de Chimborazo (HGUACH) se procede a la Evaluación de Riesgos utilizando la herramienta MSAT de Microsoft, con la finalidad de puntuar las medidas de seguridad adoptadas en el tiempo, obteniendo así, la situación actual de la organización, en cuestiones de seguridad. Adicionalmente, como resultado de la evaluación de riesgos, se procedió a la creación de una guía que incluyen diferentes actividades prioritarias, que actuarán a su vez, como controles o medidas preventivas, dichas actividades están clasificadas de acuerdo a las áreas propuestas por la herramienta. Las actividades resultantes hacen uso de estándares internacionales como las normas ISO 17799 y NIST-800.x, el Grupo Trustworthy Computing de Microsoft y otras fuentes externas de seguridad (Microsoft, 2017).

CAPÍTULO I

1. Planteamiento del problema

Problema y Justificación

Dado el incremento de ataques informáticos en los últimos años registrados a hospitales, organizaciones y empresas del sector sanitario en diferentes países, como son los casos siguientes: en el Reino Unido el brote de WannaCry (2017), donde fueron afectados 700.000 equipos de 16 hospitales y centros de salud con ransomware; en Francia con el mismo ataque, se generó un apagón informático en 120 hospitales; lo mismo sucedió en hospitales de Australia y Estados Unidos en 2019 (Harán, 2020). Esto ha motivado a las entidades dedicadas al sector de la salud a identificar e implementar medidas de seguridad dando como resultado organizaciones bajo parámetros de seguridad en sus entornos informáticos.

Un estudio en el que se analiza los países que tienen una baja seguridad cibernética, realizado por Comparitech, Ecuador ocupa el puesto diecinueve de 76 países (Bischoff, 2020), de manera que se evidencia la necesidad de implementar medidas de seguridad a diferentes niveles organizacionales.

En el Hospital General Universitario Andino de Chimborazo (HGUACH), no se ha llevado a cabo con anterioridad una evaluación de riesgos en su entorno informático. Por otra parte, otro elemento a tener en consideración es la gran brecha digital existente entre algunos grupos de la organización. La utilización de la herramienta de Microsoft Security Assessment Tool (MSAT) en el HGUACH permite el análisis de los riesgos en el entorno informático proporcionando información y actividades de buenas prácticas de seguridad en una infraestructura de tecnología de la información (Microsoft, 2017)

Llevar a cabo una evaluación de riesgos informáticos dentro de una organización es una actividad importante, que aporta beneficios como: garantizar la continuidad de la organización, optimización de tiempo y recursos, evitar gastos innecesarios, salvaguardar

la privacidad, adquisición justificada de equipos de seguridad, entre otros. Por lo que, en esta investigación, se procede a la realización de una evaluación de riesgos mediante el uso de la herramienta MSAT que utiliza estándares internacionales como son las normas ISO 17799 y NIST-800.

Objetivos

General

- Evaluar los riesgos en el ambiente informático del Hospital General Universitario Andino de Chimborazo utilizando la herramienta MSAT.

Específicos

- Analizar la herramienta Microsoft Security Assessment Tool (MSAT) para la evaluación de riesgos.
- Aplicar la herramienta MSAT en el ambiente informático del Hospital General Universitario Andino de Chimborazo.
- Elaborar una guía de actividades prioritarias para soluciones de seguridad en el Hospital General Universitario Andino de Chimborazo.

CAPÍTULO II

2. Marco teórico

2.1 Seguridad de la información a nivel organizacional

La información es un activo que tiene un valor fundamental para la organización y debe ser protegida de un modo adecuado (INCIBE, 2015). Un riesgo se entiende como una posible pérdida, producido por eventos peligrosos e inciertos ligados a vulnerabilidades existentes (Soler et al., 2018). Es por esto que, resulta importante una correcta gestión de la seguridad en una corporación para mitigar riesgos. La seguridad informática se entiende como la disciplina que se responsabiliza de la protección de aspectos como la integridad y la privacidad de la información contenida en un entorno informático, contra cualquier tipo de amenazas, reduciendo en gran parte los riesgos físicos y lógicos a los que se expone (Urbina, 2016). En el marco de la seguridad, se distingue dos conceptos importantes, la seguridad informática y la seguridad de la información. La primera se enfoca en la tecnología propiamente dicha, es decir, en las infraestructuras tecnológicas que sirven para la gestión de la información en las organizaciones, y la segunda hace referencia a la información en sí misma, como activo estratégico de la organización (Valencia-Duque y Orozco-Alzate, 2017).

2.2 Análisis de riesgos

El objetivo principal de un análisis de riesgos, consiste en detectar los principales factores de riesgo que provocarían un impacto en una entidad. De esta manera detectan los riesgos, los califica y los evalúa para la obtención de información de los mismos, consiguiendo así establecer niveles de riesgo e implementar los controles y/o acciones adecuadas para dicho riesgo.

Por lo tanto, la evaluación de Riesgos cumple un papel muy importante a la hora de seleccionar los controles de seguridad adecuados para mitigar el riesgo, así como, estimar el valor de los activos de riesgos, ver para cada activo la probabilidad de ocurrencia del

riesgo y la valoración del riesgo (De Freitas, 2009). La valoración de un activo se puede realizar de forma cuantitativa, asignando una cantidad numérica, también es posible valorar el activo de forma cualitativa, asignando niveles (Imbaquingo et al., 2019). La valoración de riesgos es un proceso que consiste en detectar un problema antes de que este se presente (Areitio, 2008).

Es importante mencionar que un análisis de riesgos tiene validez dentro del tiempo en el que se realiza, dado que puede haber a lo largo del tiempo nuevos tipos de amenazas, así mismo, puede darse el caso que las vulnerabilidades encontradas anteriormente fueron solventadas o en su caso pueden haberse añadido nuevos dispositivos o nuevas políticas de seguridad. La evaluación de riesgos cumple un papel muy importante a la hora de seleccionar los controles de seguridad adecuados para mitigarlos, tiene como finalidad en cuestión de los riesgos, su estimación del valor de los activos del mismo, su probabilidad de ocurrencia y su valoración en relación a los activos (De Freitas, 2009).

Dentro del marco del análisis de riesgos en un entorno de sistemas de información en la Tabla 1 se muestra un resumen de diferentes investigaciones.

Tabla 1. *Casos reales de Gestión y/o Análisis de Riesgos y los resultados obtenidos*

Autor	Tema	Características
Ramos (2016) Ecuador (Loja)	Análisis de riesgos informáticos y desarrollo de un plan de seguridad de la información para el gobierno autónomo descentralizado municipal de Catamayo.	• Identificación de activos. • Identificación de amenazas para crear perfiles de riesgos para cada activo. • Plan de seguridad para el tratamiento del riesgo.
Quiroz (2016) Perú (Chiclayo)	Implementación de gestión de riesgos de TI para obtener el certificado ISO 27001 en el Hospital Regional de Lambayeque.	• Certificación ISO 27001.
Agrawal (2018)	Prácticas de gestión de riesgos en la seguridad de la información (Con el método DSRM).	• Intercambio de conocimientos basados en la comunidad ISP (Tesis).

De Freitas et al. (2018)	Análisis del proceso de gestión de riesgo en el desarrollo del plan maestro de tecnología de la información del sector público.	• Identificar y comprender la gestión de riesgos. • Enmarcar los mecanismos de gestión de riesgos. • Planificación estratégica.
Diwan et al. (2018)	Marco de gestión de riesgos de seguridad de la información para un dominio del hospital.	• Identificación de los posibles hallazgos. • Análisis de riesgos. • Planes de contingencia generando recomendaciones para mitigar los riesgos de manera global.
Force (2018)	Marco de gestión de riesgos (RMF). Un enfoque de ciclo de vida del sistema para la seguridad y la privacidad.	• Implementación de procesos de monitoreo continuo. • Proporcionó información necesaria para tomar decisiones eficientes, rentables y de gestión de riesgos sobre los sistemas a los líderes principales y ejecutivos.
Ramírez (2018) Colombia (Dos Quebradas)	Análisis de riesgos y diagnóstico de la seguridad de la información de la E.S.E. (Empresa Social del Estado) Hospital Santa Mónica.	• Entrevista inicial al personal del departamento. • Inspección a cada dependencia. • Propuesta de mitigación de riesgos y plan de mejora.

Fuente*:* Elaboración propia

La Tabla 1 visibiliza mejoras de seguridad, detección y mitigación de riesgos, siendo esto beneficioso para el cumplimiento de metas expuestas en cada proyecto, o en el caso de estudio de "Gestión de riesgos de TIC en el Hospital Regional Lambayeque", la obtención de la certificación ISO 27001.

2.3 Definiciones utilizadas en la evaluación de riesgos

La norma ISO/IEC 27000 recoge los términos y definiciones empleados en el resto de normas de la serie. A continuación, se detallan las siguientes definiciones:

- **Activo**: Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (Liñan, 2017).
- **Ataque**: Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.
- **Autenticación**: Propiedad de que una entidad es lo que afirma ser.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados (Docplayer, 2016).
- **Control**: Medida por la que se modifica el riesgo.
- **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias.
- **Impacto**: El coste para la empresa de un incidente, que puede o no ser medido en términos estrictamente financieros.
- **Integridad**: Propiedad de la información relativa a su exactitud y completitud.
- **Política**: Intenciones y dirección de una organización, expresada formalmente por su alta dirección.
- **Probabilidad**: Posibilidad de que ocurra algo.
- **Riesgo**: Efecto de la incertidumbre sobre los objetivos.
- **Salvaguarda:** Controles de protección ante un riesgo.
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas (Liñan, 2017).

2.4 Metodologías y herramientas utilizadas

Para el análisis y/o gestión de riesgos, existen diferentes metodologías, tales como, MAGERIT, OCTAVE, CORAS, MEHARI, NIST, IRAM Y CRAMM (Serrano et al., 2019). Existen herramientas informáticas basadas en una o varias de las metodologías mencionadas anteriormente, tales como, PILAR, RISICARE, SE Risk y MSAT.

En la Tabla 2, se presenta ejemplos de metodologías y sus características principales. En la Tabla 3, se observa herramientas que sirven de apoyo para la realización de la evaluación de riesgos.

Tabla 2 . *Metodologías para la evaluación de riesgos*

Metodología	Objetivo	Características
Magerit	Análisis y Gestión de riesgos de los Sistemas de Información del Gobierno de España para organizaciones públicas gubernamentales	Elaborada por el Consejo Superior de Administración Electrónica. Alineamiento con los estándares ISO. Libre y realiza un análisis cuantitativo y cualitativo. Utiliza herramientas como PILAR. Fallas en el inventario de las políticas. (Novoa y Rodríguez, 2015)
Octave	Evaluación de Amenazas Operacionales Críticas, Activos y Vulnerabilidades para la optimización de la evaluación de riesgos	Creada por la Universidad Carnegie Mellon. Existen tres versiones de OCTAVE (OCTAVE, OCTAVE-S, OCTAVE Allegro). Tiene 3 fases: evaluación de la organización (construcción de perfiles activo-amenaza), identificación de vulnerabilidades en la infraestructura de TI y elaboración de un plan y estrategia de seguridad. No tiene herramienta y realiza un análisis cualitativo. (Serrano et al., 2019)

Coras	Evaluación de riesgos de sistemas de Tecnologías de la información y comunicación críticos, de una manera precisa y efectiva	Elaborado por Sintef y un equipo de investigadores de Noruega. Se desarrolla en 7 etapas: presentación, análisis de alto nivel, aprobación, identificación de riesgos, estimación de riesgos, tratamiento de riesgos. Realiza un análisis cualitativo y no posee herramientas para la aplicación de su metodología. (Novoa y Rodríguez, 2015)
Mehari	Evaluación y Gestión de Riesgos	Desarrollada por la comisión métodos de Clusif. Análisis cuantitativo y cualitativo y utiliza la herramienta RISCARE. Conforme a la ISO/IEC 27005. (Rea-Guaman et al., 2018)
NIST	Guía destinada para la gestión de riesgos, apoyando a los procesos de valoración y mitigación de estos	Desarrollada por el Instituto Nacional de Estándares y Tecnología. No tiene en cuenta los procesos, activos y dependencias, y no tiene herramienta. Análisis cualitativo. (Serrano et al., 2019)
CRAMM	Análisis y gestión de riesgos	Para grandes empresas. Se desarrolla en 3 etapas: distinción de los objetivos para la seguridad, evaluación de riesgos, y elección de salvaguardas. Licencia comercial. (Novoa y Rodríguez, 2015)
EBIOS	Análisis y gestión de riesgos	Se trata de un conjunto de herramientas y guías. Se basa en el estudio de 5 fases: contexto, eventos peligrosos, escenarios de amenazas, riesgos y de las medidas de seguridad. Libre. (Reinoso, 2018)

Fuente: Elaboración propia

Tabla 3. *Herramientas para la evaluación de riesgos.*

Herramienta	Objetivo	Características
Pilar	Análisis de Riesgos	Creado por el Centro Nacional de Inteligencia. Realiza el procedimiento de Magerit, con la caracterización de los activos y amenazas y la evaluación de las salvaguardas. El resultado de su implementación se muestra mediante la generación de informes RTF, gráficas y tablas. (Molina-Miranda, 2017)
Risicare	Gestión de un Sistema de Gestión de Seguridad de la Información (SGSI)	Desarrollado por BUC S.A. Utiliza la metodología de MEHARI. Utiliza un conjunto de puntos de control que incluye la ISO 27002. Está destinado a pequeñas empresas. (Rea-Guaman et al., 2018)
MSAT	Evaluación de Seguridad	Desarrollada por Microsoft. Herramienta gratuita. Mide la equivalencia entre riesgos de seguridad, defensas y la madurez de la organización. Destinado a medianas empresas de hasta 1000 empleados. El resultado son recomendaciones comprobadas y actividades prioritarias para el mejoramiento de la seguridad. Conforme a las normas ISO 17799 y NIST - 800.x. (Microsoft, 2017)
SE Risk	Gestión de Riesgo y controles	De SoftExpert. La evaluación puede ser cualitativa, cuantitativa y a través de una matriz. Herramienta libre. Conforme a la norma ISO 31000: 2009. (Rea-Guaman et al., 2018)

Fuente: Elaboración propia

2.5 Herramienta MSAT

Microsoft Security Assessment es una herramienta diseñada para ayudar a las organizaciones a evaluar los puntos débiles de seguridad de las Tecnologías de la Información (Microsoft, 2017). Por otro lado, MSAT aborda la mayor cantidad de áreas

de riesgo del entorno y proporcionando instrucciones sobre las cuales desarrollar líneas de seguimiento que requieren mayor atención (Rodríguez, 2019).

MSAT es una herramienta gratuita, diseñada para organizaciones con menos de 1.000 empleados, está proyectada para poder identificar y abordar los riesgos existentes en el entorno informático de una organización. Utiliza un enfoque integral para la medición del nivel de seguridad y cubre aspectos como usuarios, procesos y tecnología (Microsoft, 2017).

Se fundamenta en las normas ISO 17799 y NIST -800.x, así como las recomendaciones y orientaciones normativas del Grupo Trustworthy Computing de Microsoft y otras fuentes externas de seguridad (Microsoft, 2017). El fundamento de la norma ISO 17799, es proporcionar una base común para el desarrollo de una serie de normas de seguridad en las organizaciones, y obtener una gestión de la seguridad eficaz.

Una de las medidas que proporciona MSAT, tras su aplicación es la medición de la madurez. Dentro de NIST, existe un modelo llamado NIST CSEAT IT Security Maturity Model, considerado un modelo de madurez enfocado en la definición y posterior implementación y medición de lo definido en los documentos del mismo. El propósito de utilizar un modelo de madurez, aparte de, establecer qué capacidades tiene una empresa, identifica qué desarrollo tiene ésta en las áreas evaluadas, debido a que esto puede influir finalmente en la efectividad de las medidas adoptadas (Rámirez, 2016).

2.5.1. Normativa MSAT

2.5.1.1. Instituto Nacional de Estándares y Tecnología: NIST

Denominada entre 1901 y 1908 como la Oficina Nacional de Normas. NIST es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos, cuya misión es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida (Urruchurtu, 2013).

NIST (2020) menciona que CSRC (Computer Security Resource Center) es la división encargada de proporcionar recursos sobre seguridad y privacidad de la información, informática y cibernética, a través de dos divisiones: seguridad Informática (CSD) y ciberseguridad aplicada (ACD).

La División de Seguridad Informática, comprende los siguientes grupos:

- Tecnología criptográfica
- Sistemas y aplicaciones seguros
- Componentes y mecanismos de seguridad
- Ingeniería de seguridad y gestión de riesgos
- Pruebas, validación y medición de seguridad

La División de Ciberseguridad Aplicada, está compuesta por:

- Aplicaciones de ciberseguridad y privacidad
- Centro Nacional de Excelencia en Ciberseguridad (NCCoE)
- Iniciativa Nacional para la Educación en Ciberseguridad (NICE)

Con la finalidad de dar métodos viables y rentables, mediante la descripción de políticas, procedimientos y pautas de seguridad informática, aparece la serie NIST 800, cuyo objetivo es la optimización de la seguridad de los sistemas y redes de TI (Rouse, 2006).

La serie 800 de la Publicación Especial (SP) de NIST, creada en 1990, desarrolla publicaciones de acuerdo con sus responsabilidades legales bajo la Ley Federal de Modernización de la Seguridad de la información (FISMA) de 2014, 44 U.S.C 3551 y siguientes, Ley Pública (P.L) 113-283. SP 800 informa sobre la investigación, directrices y esfuerzos de divulgación del Laboratorio de TI en seguridad informática y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas (NIST, 2018).

Una alternativa a la norma ISO 27002 como orientación para apoyar los controles de aplicación de la norma ISO 27001 es la serie NIST SP 800, en conclusión, es un conjunto de documentos de libre descarga, facilitadas desde el gobierno federal de los Estados

Unidos, que describe las políticas de seguridad informática, procedimientos y directrices, que son publicadas por el Instituto Nacional de Estándares y Tecnología, que contiene 130 documentos (NIST, 2016).

2.5.1.2. ISO/IEC 17799

La International Organization for Standardization - ISO inició el 23 de febrero de 1947, con el objetivo principal de "facilitar la coordinación internacional y la unificación de los estándares industriales", es decir, con el fin de favorecer la normalización en el mundo (Quintanilla et al., 2016). Tuvieron éxito desde su primera publicación de 1987, estas normas son revisadas al menos una vez, cada 5 años, por el Cómité Técnico ISO/TC 176. La publicación de un Estándar Internacional requiere de la aprobación de por lo menos un 75% de los organismos nacionales que emiten un voto (GlobalSTD, 2017).

ISO/IEC 17799 es una norma internacional que proporciona un marco para el establecimiento de diferentes métodos de evaluación de riesgos; políticas, controles y contramedidas. Otra de las finalidades de esta norma, es la asignación de roles y responsabilidades, documentación de procedimientos operativos, preparación para incidentes y gestión de continuidad del negocio y cumplimiento de requisitos legales y controles de auditoría (Myler y Broadbent, 2006). Esta norma proporciona una declaración autorizada sobre seguridad de la información y los procedimientos necesarios para lograr seguridad de la información en las organizaciones (Ma y Pearson, 2005). Esta norma rige bajo las pautas para preservar los principios de la confidencialidad, integridad y disponibilidad de la información.

La norma ISO/IEC 17799, establece diez dominios, que dan cumplimiento, casi en su totalidad, la Gestión de la Seguridad de la Información, estos dominios comprenden: las Políticas de seguridad, los aspectos organizativos, la clasificación y control de activos, seguridad ligada al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos, desarrollo y mantenimiento de sistemas, gestión de continuidad del negocio, y finalmente, el cumplimiento o conformidad de la legislación (Guzmán, 2015). De los diez dominios que muestran la estructura de la norma ISO/IEC

17799, se derivan 36 objetivos de control y 127 controles que comprenden prácticas, procedimientos o mecanismos que reducen el nivel de riesgo (Quintanilla et al., 2016).

Ma y Pearson (2005) mencionan que el origen de la norma ISO 17799 se remonta a BS 7799, publicado por la British Standards Institution en 1995, proporciona la base para autoevaluación, reevaluación de las prácticas de seguridad de la información de los socios comerciales y evaluación independiente de ISM (Information security management) dentro de la organización empresarial.

En diciembre de 2000, ISO, adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799, lo que llevó a una gran aceptación por parte del sector internacional, obteniendo un gran reconocimiento (Quintanilla et al., 2016). La familia ISO a partir del 2007, adoptó el esquema de numeración, bajo la serie del número 27000 en adelante. Las nuevas ediciones del ISO/IEC 17799 en la actualidad, se encuentran con el nombre ISO/IEC 27002.

2.5.1.3. Trustworthy Computing Group de Microsoft (TwC)

Microsoft tiene como misión, simplificar la forma en la que se trabaja, aumentar la agilidad, impulsar una mayor rendición de cuentas y crear modelos de soporte que sean más magros y eficientes. Con el fin de cambiar los procesos y la cultura de Microsoft para conseguir su misión, se asignó un grupo centralizado, que tenía la responsabilidad de impulsar esta iniciativa (Charney, 2014).

Así TwC es una iniciativa de Microsoft lanzada en 2002 y anunciada por Bill Gates. El grupo TwC implementa los principios de seguridad y privacidad en los procesos de desarrollo de software y la cultura de la empresa (Microsoft, 2011).

TwC, está distribuido en Microsoft en diferentes áreas como, programas de base, el ciclo de vida de desarrollo de seguridad (SDL) y el aseguramiento de la seguridad operativa (OSA), con el fin de integrarse más plenamente en la división de ingeniería más responsable del futuro de la nube y la seguridad (Charney, 2014).

SDL es un proceso de control de seguridad dedicado al desarrollo de software y la introducción de seguridad y privacidad en todas las fases del proceso de desarrollo, también combina un enfoque holístico y práctico destinado a la reducción del número y severidad de las vulnerabilidades de los productos y servicios de Microsoft, para limitar a los atacantes que puedan poner en riesgo los equipos (Microsoft, 2011).

La iniciativa TwC, abarca conceptos como: confianza, estabilidad y seguridad en la plataforma esta última se sustenta sobre pilares básicos como: aislamiento y flexibilidad, calidad, autenticación, autorización y control de accesos, orientación y formación (UNIR, 2018).

El grupo TwC describe el ciclo de vida de desarrollo de seguridad, como un proceso que Microsoft utiliza para desarrollar software que pueda recibir ataques mal intencionados (Vanegas, 2016).

En la actualidad la unidad Twc no existe, lo que ha significado un cambio muy importante para Microsoft, algunos de los empleados fueron reasignados a la división Cloud and Enterprise y otros en el grupo legal, con la finalidad de integrar la experiencia en seguridad y privacidad en el resto de la compañía (Fisher, 2014).

2.6 Evaluación de riesgos con MSAT

MSAT utiliza doscientas preguntas que se subdividen en cuatro categorías: infraestructura, aplicaciones, operaciones y usuarios, que se detallan en la Tabla 4.

Tabla 4: *Áreas de la evaluación de riesgos de seguridad con MSAT*

Infraestructura	
Defensa perimetral	Se centra en la seguridad de los límites de la red, donde la red interna conecta con el mundo exterior. Constituye la primera línea de defensa contra intrusos (Microsoft, 2017).
Autentificación	Son procesos rigurosos en la autentificación de usuarios, administradores y usuarios remotos ayudan a prevenir que alguien ajeno a la red obtenga acceso no autorizado a ella a través de ataques locales o remotos (Microsoft, 2017).

Gestión y monitorización	La gestión, monitorización y recogida de datos adecuada son críticas para el mantenimiento y análisis de entornos tecnológicos. Estas herramientas son importantes si se ha producido un ataque y se requiere un análisis del incidente (Microsoft, 2017).
Estaciones de trabajo	La seguridad de las estaciones de trabajo individuales es un factor clave en la defensa de cualquier entorno, especialmente si se permite el acceso remoto. Las estaciones de trabajo deberían disponer de protección para resistir un ataque común (Microsoft, 2017).
	Aplicaciones
Implementación y uso	Cuando las aplicaciones de negocio críticas se encuentran implementadas en producción, se debe proteger la seguridad y disponibilidad de dichas aplicaciones y de los servidores que las alojan (Microsoft, 2017).
Diseño de aplicaciones	Un diseño que no cumple adecuadamente los mecanismos de autentificación, autorización y validación de datos puede permitir que un atacante aproveche una vulnerabilidad de seguridad y obtenga acceso a información confidencial (Microsoft, 2017). Las metodologías de desarrollo de aplicaciones seguras son clave para cerciorarse de que tanto las aplicaciones desarrolladas internamente como las desarrolladas por terceros cumplen los modelos de seguridad y no dejan a la empresa abierta a posibles ataques (Microsoft, 2017). La integridad y la confidencialidad de los datos son dos de las grandes preocupaciones de cualquier empresa. La pérdida o robo de datos puede influir negativamente en sus beneficios y reputación. Es importante comprender cómo las aplicaciones gestionan los datos críticos y cómo esos datos son protegidos (Microsoft, 2017).
	Operaciones
Entorno	La seguridad de una organización depende de las operaciones, procesos y directrices que se aplican en su entorno. Permiten acentuar la seguridad siempre que incluyan algo más que las propias defensas tecnológicas. Es indispensable disponer de una documentación precisa del entorno para que el equipo de operaciones sepa cómo gestionarlo y mantenerlo (Microsoft, 2017).
Política de seguridad	Se refiere al conjunto de políticas y directrices individuales existentes que permiten dirigir la seguridad y el uso adecuado de tecnología y procesos dentro de la organización. Esta área cubre políticas de seguridad de todo tipo, como las destinadas a usuarios, sistemas o datos (Microsoft, 2017).

Copias de seguridad y recuperación	Son esenciales para asegurar la continuidad del negocio en caso de que ocurra un desastre o un fallo de hardware o software. No disponer de ellas puede suponer una pérdida significativa de datos y productividad. La reputación de la compañía y de la marca podría ser puesta en entredicho (Microsoft, 2017).
Gestión de actualizaciones	Es importante para la seguridad del entorno tecnológico de la organización. Es necesario llevar a cabo actualizaciones periódicas y programadas para evitar que alguien aproveche vulnerabilidades conocidas (Microsoft, 2017).
	Usuarios
Requisitos y evaluación	Los requisitos de seguridad deberían ser entendidos por todas las personas con capacidad de decisión, ya sea en cuestiones de negocio como en cuestiones técnicas, de forma que tanto unos como otros contribuyan a mejorar la seguridad en lugar de pelearse con ella. Llevar a cabo regularmente una evaluación por parte de terceras partes puede ayudar a la compañía a revisar, evaluar e identificar las áreas que necesitan mejorar (Microsoft, 2017).
Políticas y procedimientos	Disponer de unos procedimientos claros y prácticos en la gestión de relaciones con vendors o partners puede evitar que la compañía se exponga a posibles riesgos. Si se aplican también estos procedimientos en los procesos de contratación y terminación de contrato de empleados se puede proteger a la empresa de posibles empleados poco escrupulosos o descontentos (Microsoft, 2017).
Formación y concienciación	Los empleados deberían recibir formación y ser conscientes de las políticas de seguridad existentes y de cómo la aplicación de esas políticas puede ayudarles en sus actividades diarias. De esta forma no expondrán inadvertidamente a la compañía a posibles riesgos (Microsoft, 2017).

Fuente: Adaptado. (Microsoft, 2017).

CAPÍTULO III

3. Metodología

El tipo de estudio fue observacional, tratándose de un diseño de investigación cuyo objetivo fue observar y registrar los acontecimientos del análisis de riesgo dentro de las áreas de infraestructura, aplicaciones, operaciones y personal del Hospital General Universitario Andino de Chimborazo, utilizando la herramienta MSAT. La planificación de la medición fue de carácter retrospectivo, al haberse observado la seguridad informática, para identificar las medidas de seguridad implantadas con anterioridad en el hospital. Finalmente, es un estudio de carácter transversal puesto que los datos se obtuvieron en un único momento, es decir, cuando se aplicó los diferentes componentes del cuestionario y no en instantes diferentes con la intención de compararlos.

Este proyecto tiene un enfoque cualitativo, que es el más utilizado para una evaluación de riesgos, este enfoque está basado en la recolección de información mediante el uso de cuestionarios, donde las preguntas de investigación se realizan al personal especializado en las áreas de estudio.

El método utilizado para la investigación es inductivo, que consistió en el análisis de cada segmentación de las áreas evaluadas para la obtención de la situación actual del Hospital en cuestiones de seguridad.

3.1 Identificación de variables

3.1.1. Variable dependiente

Evaluación de Riesgos

3.1.2. Variable independiente

Herramienta MSAT

3.2 Tipo de estudio

3.2.1. Según la fuente de investigación

Investigación Bibliográfica: Recopilación de información, utilizando técnicas y estrategias para acceder a documentos indexados como: tesis, revistas, libros para la investigación y artículos científicos de diferentes bases de datos, otra fuente primaria que otorgó información de primera mano fue: informantes, fotografías, y documentos proporcionados por el Hospital.

3.2.2. Según el nivel de conocimientos

Investigación Descriptiva: Se analizó como se manifiesta el fenómeno de evaluación de riesgos y sus componentes en el hospital que son las medidas relacionadas con características operacionales, de infraestructura, personal y aplicaciones.

3.2.3. Según las variables

Investigación no Experimental: Se observó el fenómeno investigado tal y como ocurre naturalmente, sin intervenir en su desarrollo.

3.2.4. Operacionalización de variables

Variable	Tipo	Definición Conceptual	Dimensión	Indicadores
Herramienta MSAT	Independiente	Herramienta para la Evaluación de Seguridad (Microsoft, 2017).	Software	• Porcentaje de Perfil de Riesgos de Negocio (BRP). • Porcentaje de Defense-in-Depth Index (DiDI). • Puntuación en las medidas de defensas aplicadas.
Evaluación de Riesgos	Dependiente	Es un proceso que consiste en identificar los peligros que afectan a la seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardas (Areitio, 2008).	Análisis	• Infraestructura • Aplicaciones • Operaciones Personal

Fuente: Elaboración propia

3.2.5. Procesamiento y Análisis

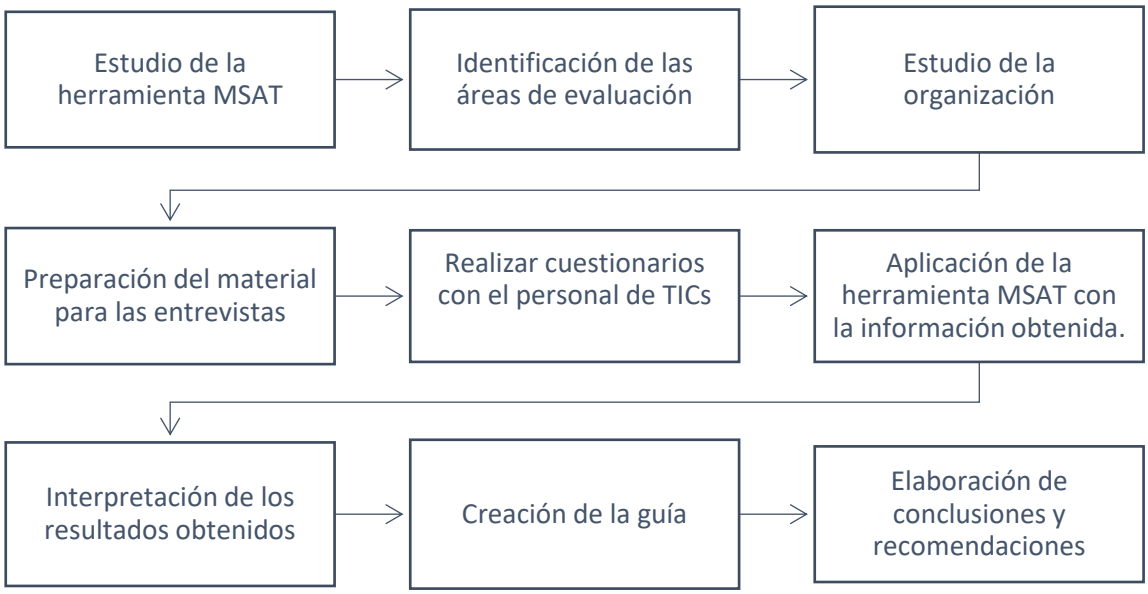


Figura 1. Procedimiento y actividades del proyecto
Fuente: Elaboración propia.

3.3 Caso de estudio: Hospital General Universitario Andino de Chimborazo

Fundado en 1998, el HGUACH, cuenta con servicios médicos integrales, complementado con la medicina alopática, alternativa y andina, es un hospital único en el país, ubicado en la ciudad de Riobamba en las calles Pastaza s/n y Manabí (Cdla. 24 de Mayo), es una organización sin ánimo de lucro.

3.3.1. Misión

“Somos el mejor equipo de salud, enfocados en el cuidado integral del paciente, la familia y la comunidad, con la finalidad de mejorar su calidad de vida”

3.3.2. Visión

“En el 2024 el Hospital General Universitario Andino, será una institución referente en el modelo integral de atención y gestión que ofrece servicios de calidad técnica y calidez humana”

3.3.3. Principios

Los principios que rigen para ofrecer un servicio de calidad en el HGUACH son: Calidad Técnica, Calidez humana, Interculturalidad, Solidaridad, Ética, Equidad, Participativo, Eficiente, Integridad y Sostenibilidad.

3.3.4. Resultados Estratégicos

- Mejora del modelo de gestión
- Fortalecimiento de la infraestructura-equipamiento
- Fortalecimiento de los procesos técnicos administrativos
- Apoyar la docencia, vinculación e investigación

3.3.5. Organigrama Organizacional

En la Figura 2 se puede observar la distribución de la organización del Hospital General Universitario Andino de Chimborazo. En el anexo A se detalla la distribución organizacional del área de Administrativo Financiero (figura 5) y del área de Director Médico (Figura 6).

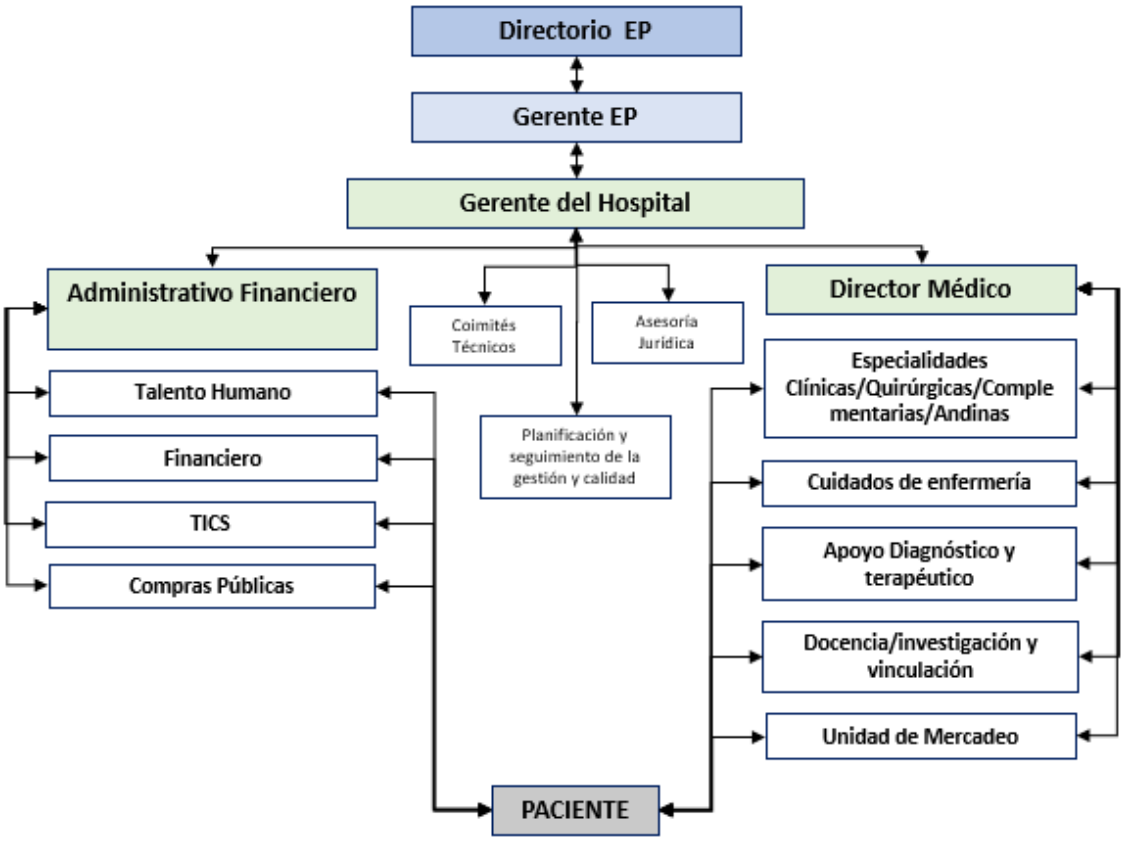


Figura 2. Estructura organizacional HGUACH
Fuente: Elaboración propia

3.3.6. Identificación de activos

Entorno

En la actualidad el HGUACH, cuenta con un total de 42 personas contratadas, más el personal subcontratado para otro tipo de servicios temporales, tiene 3 edificaciones en sus instalaciones, de acuerdo a sus necesidades. Los controles de acceso, están resguardados por personal de seguridad, además cuenta con sistemas de extinción de incendios, climatización y detectores de humo a lo largo de todas sus instalaciones.

Por otro lado, cuenta con un Data Center con acceso controlado, un cuarto de vigilancia, donde se puede observar las diferentes cámaras de seguridad instaladas, por último, cuenta con un sistema electrónico de registro de asistencia.

TIC

La organización tiene una conexión constante a Internet a través de un enlace de fibra óptica proporcionada por el proveedor de internet. Dispone de un servidor local FTP configurado para Windows.

Intelho, es la empresa contratada para proporcionar la planificación de recursos empresariales (ERP), el ERP, utilizado por el hospital se denomina SIGCENTER, que permite el manejo de diferentes componentes como son: pacientes, historia clínica, recetas, laboratorios, farmacia, entre otros.

Dispone de cuatro puntos de conexión: Switch de consulta externa, Switch de imagen, Switch de hospitalización y nutrición y Switch de administración. Para la distribución del cableado estructurado se tuvieron en cuenta los siguientes equipos:

- 58 unidades de cable UTP CAP 6ª
- 4 unidades de Estructura metálica 12 UR, 19”
- 3 unidades de Switches de acceso 24 puertos
- 4 unidades de Patch Panel 24 puertos
- 4 unidades de Multi Toma de 8 tomas para Rack

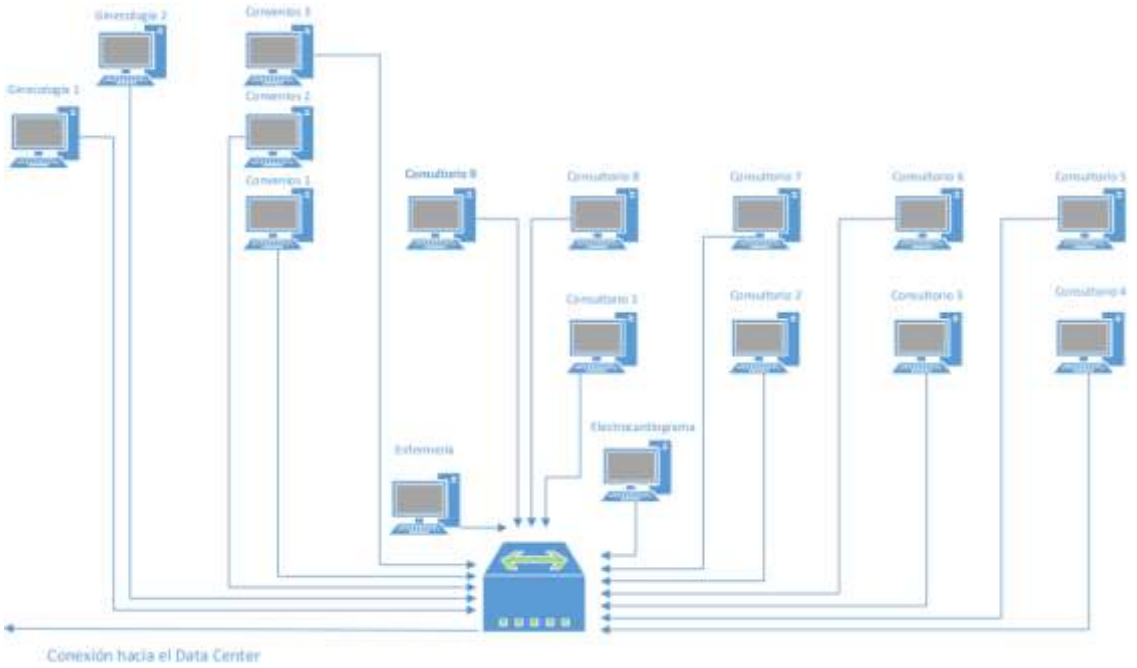


Figura 3. Topografía switch consulta externa
Fuente: Informe Técnico de Cableado Estructurado

El switch de consulta externa mostrado en la figura 3, tiene un total de 17 puntos, distribuidos entre los consultorios del 1 al 9, convenios del 1 al 3, ginecología 1 y 2, encefalograma, enfermería CEXT (Enfermería consulta externa), y finalmente con el switch (PUNTO R).

En el Anexo B, se observa la distribución de los siguientes switches:

El swtich de del departamendo de Imagen, detallado en la Figura 7, se encuentra conectado a 26 puntos: RX Copiadora, RX Copiadora 2, RX Switch, RX Digitación, Ecografía 1, 2 y 3, AUX DIR. Médica, Oficina Imagen 2, Gastroenterología 1 y 2, Estadística 1, 2 y 3, Farmacia Dirección, Biométrico, Caja, Admisiones M1, Admisiones M2, Entrega de resultados Imagen, Farmacia entrega de medicamentos, Farmacia Caja, Quirófano, Emergencia Enfermería, Emergencia Consultorio, y finalmente, Conexión Data Center.

En el área de hospitalización expuesto en la figura 8, existen un total de 6 puntos, adicionalmente, está conectado un switch en el área de nutrición, donde existen 4 puntos.

En hospitalización están los siguientes puntos: Switch Nutrición, Hospitalización Enfermería, Hospitalización Médicos, Hospitalización Router, Nutrición y Conexión con el Data Center. En Nutrición están los siguientes puntos: Aula de Capacitación y Laboratorios 1, 2, 3 y 4.

El switch de administración mostrado en la figura 9, tiene conexión con 5 puntos: Andino complementario, Andino 1, 2 y 3, y finalmente a la Conexión con el Data Center.

3.4 Evaluación de riesgos en el HGUACH

La investigación se llevó a cabo en el ambiente informático del Hospital General Universitario Andino de Chimborazo, mediante la utilización de la herramienta MSAT.

Para el análisis de riesgos se procedió a la realización de varias entrevistas al personal de TI del HGUACH y a la revisión de las instalaciones, en acompañamiento del jefe del área de TI del hospital, obteniendo así, la delimitación de la situación actual de la organización en aspectos de seguridad y la diferenciación de los activos y su distribución. Con MSAT se analizó los resultados obtenidos en base a las respuestas del cuestionario que propone la herramienta.

La metodología utilizada por esta herramienta y aplicada en este proyecto consistió en la creación de un perfil de riesgos para el HGUACH, a través de la evaluación de los riesgos a los que el hospital está expuesto, realizando un estudio de la organización a profundidad, tomando en cuenta, su actividad comercial como punto de partida. Posteriormente se compiló las medidas de seguridad implantadas, estos controles, fomentan a la creación de capas de protección, proporcionando mayor seguridad ante los riesgos que podrían darse. Las capas formadas ayudan a una táctica compaginada de defensa en profundidad (DiDI) (Maliza, s.f.).

Tras el procedimiento anterior, se realizó una relación entre BRP y DiDI, para establecer en general la distribución de los riesgos en las diferentes áreas que se analizan con la herramienta (AoAs), Dichas áreas son: infraestructura, aplicaciones, operaciones y personal (Maliza, s.f.).

Además, esta herramienta también permitió valorar la madurez de la seguridad del HGUACH.

Para la finalización de la investigación se procedió a la creación de la guía de actividades prioritarias, teniendo en cuenta las recomendaciones obtenidas por MSAT, el enfoque de esta herramienta, no se basa en tener una medida de la capacidad que tienen los controles en el hospital para mitigar los riesgos. Por lo que, los datos obtenidos, dan pautas para poner mayor interés en las áreas que lo requieran.

3.4.1. Áreas de análisis en el HGUACH

Previo al análisis de las áreas, también se realizó una encuesta con la finalidad de obtener el perfil empresarial del HGUACH e indagar sobre la relación entre la actividad comercial que el hospital realiza y las áreas más importantes que se podrían ver afectadas. En la Tabla 5 se presenta las características de los cuestionarios aplicados al personal de TI. Por otro lado, los cuestionarios completos con las respuestas obtenidas se pueden observar en el Anexo D.

Tabla 5. *Áreas de análisis del HGUACH*

No.	Áreas	Observaciones
1	Perfil de Riesgos (BRP)	• El cuestionario está compuesto de 56 preguntas. • Preguntas orientadas a la obtención el BRP del HGUACH: Información básica empresarial, seguridad de la infraestructura, aplicaciones, operaciones, personal y entorno. • La aplicación de este cuestionario, tiene como finalidad identificar los riegos de acuerdo, al sector empresarial en que se encuentra ubicado el HGUACH.

2	Infraestructura	• El cuestionario está compuesto de 27 preguntas. • Preguntas orientadas al área de infraestructura y su relación con la defensa del perímetro, autenticación, gestión y control. • Su aplicación favorece a la identificación de las áreas de riesgo e idealización de diferentes métodos para poner fin a las amenazas que se pudieran dar.
3	Aplicaciones	• El cuestionario está compuesto de 26 preguntas. • Preguntas orientadas al área de aplicaciones y su relación con la implementación y uso, diseño de aplicaciones, almacenamiento y comunicaciones de datos. • Su aplicación ayuda a evaluar las tecnologías utilizadas, con el fin de aumentar el índice de defensa en profundidad.
4	Operaciones	• El cuestionario está compuesto de 42 preguntas. • Preguntas orientadas al entorno, directiva de seguridad, gestión de actualizaciones y revisiones, copias de gestión de recuperación. • Con la aplicación de este cuestionario se valoran las prácticas de funcionamiento y las normas utilizadas, para aumentar las estrategias orientadas a la defensa en profundidad.
5	Personal	• El cuestionario está compuesto de 22 preguntas. • Preguntas orientadas a los requisitos y evaluaciones, directiva y procedimiento, formación y conocimiento. • Aplicando este cuestionario, se obtiene una ayuda para la valoración de mitigación de riesgo del área de personal.

Fuente: Elaboración propia

CAPÍTULO IV

4. Resultados y Discusión

En este capítulo se muestra los resultados obtenidos tras la implementación de la herramienta MSAT en el entorno informático del Hospital General Universitario Andino de Chimborazo – HGUACH, permitiendo conocer el estado actual del nivel de seguridad.

La herramienta MSAT ayudó a determinar los riesgos que enfrenta la infraestructura informática, además provee las mejores prácticas y actividades prioritarias para cada área. En el Anexo E, se puede observar la "Guía de actividades prioritarias", donde se especifican recomendaciones a implantar para la mitigación de riesgos, de acuerdo al análisis realizado.

4.1 Distribución de defensa de riesgos

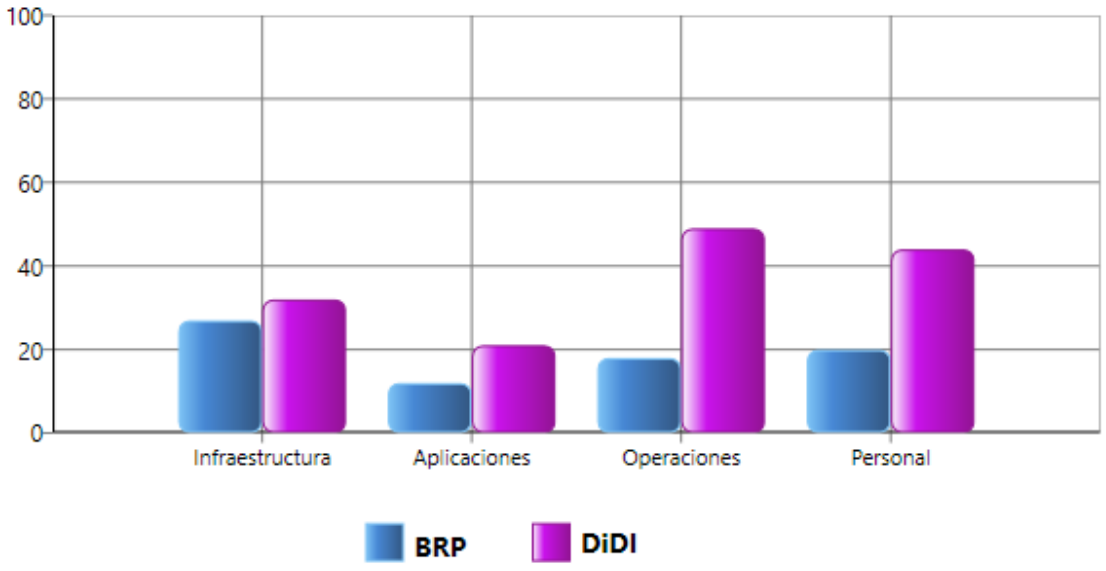


Figura 4. Perfil de riesgos para la empresa vs Índice de defensa en profundidad
Fuente: Informe de la Herramienta MSAT

La puntuación mostrada en la Figura 4, para BRP una puntuación más alta equivalente a un riesgo posible aumentado en la organización dentro del área indicada, mientras que en DiDI, una puntuación alta equivale a que han tomado mayores medidas de seguridad.

En la figura 4, se visualiza la calificación de las las áreas de análisis y el índice de defensa en profundidad. Cabe mencionar, que lo ideal sería, tener en estos dos parámetros el mismo nivel, por área. Se puede observar un desequilibrio significativo en las áreas: operaciones y personal. Esto implicaría la necesidad de volver a alinear las inversiones del HGUACH en estas áreas. Por otro lado, también existe disparidad menos notoria en las áreas de aplicaciones e infraestructuras.

4.2 Madurez de la seguridad

Aunque no necesariamente todas las organizaciones necesitan llegar al nivel óptimo de madurez de la seguridad, ya que una empresa podría estar en un entorno de bajo riesgo, si es necesario determinar una línea de partida de la madurez de seguridad. Tras estos aspectos, se procede al siguiente análisis:

En la Tabla 6, se pueden observar la simbología de puntuación de estos resultados. La Tabla 7, muestra los resultados obtenidos para la distribución de defensa del riesgo y el nivel de madurez.

En cuanto a la distribución de defensa de riesgos, las áreas de personal y operaciones tienen carencias severas, por lo que, requieren una mejora de nivel prioritario. Aplicaciones e infraestructura obtuvieron como resultado que cumplen las mejores prácticas recomendadas.

En cuanto al nivel de madurez, se observa que el área de aplicaciones tiene una madurez de nivel básica con carencias severas, lo que significa, que solo están implantadas algunas medidas eficaces como primer escudo protector. El área de personal necesita mejoras, tiene un nivel estándar en madurez, lo que indica que estás áreas tienen múltiples capas de defensa aplicadas para respaldar una estrategia definida, sin embargo, las áreas de operaciones e infraestructura cumplen con las mejores prácticas, su nivel de madurez es

optimizada, lo cual quiere decir que el HGUACH en estas áreas, ha adquirido protección de tipo efectiva de los asuntos de forma adecuada y uso de buenas prácticas recomendadas.

Tabla 6. *Simbología de tarjeta de puntuación*

Simbología
Cumple las mejores prácticas recomendadas
Necesita mejorar
Carencias severas

Fuente: MSAT

Tabla 7. *Distribución de defensa de riesgos y madurez de seguridad*

Áreas evaluadas	Distribución	Madurez
Infraestructura		
Aplicaciones		
Operaciones		
Personal		

Fuente: MSAT

De acuerdo a las respuestas obtenidas en la evaluación de riesgos, las medidas de defensa del HGUACH se han calificado utilizando la simbología que se observa en la Tabla 6.

4.3 Resultados y recomendaciones de la evaluación para Infraestructura

4.3.1. Defensa del perímetro

Es utilizado como primer escudo de protección ante intrusiones. En la tabla 8, se pueden observar las subcategorías de la Defensa del perímetro y su puntuación correspondiente.

Tabla 8. *Puntuación de la defensa del perímetro*

Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus – Equipos de escritorio	
Antivirus – Servidores	

Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	

Fuente: MSAT

A continuación, se muestra en la Tabla 9, los resultados de cada una de las subcategorías de la defensa del perímetro.

Tabla 9. *Riesgos existentes en la defensa del perímetro*

Subcategoría	Resultados
Reglas y filtros de cortafuegos	• No se han instalado cortafuegos en todas las oficinas. • No se ha creado ningún segmento DMZ para la protección de los activos del hospital. • No se hace uso de ningún software de firewall basado en host en los servidores
Antivirus	• Falta de un software antivirus instalado en los hosts del perímetro de red.
Antivirus – Servidores	• A nivel de los servidores, no se utilizan soluciones antivirus.
Acceso remoto	• Tanto socios como empleados del hospital se conectan de manera remota a la red del HGUACH, por otro lado, no hace uso de ninguna tecnología de red privada virtual para tener un acceso seguro. • Por otro lado, no se utiliza autenticación multifactor como un segundo escudo protector para el acceso de los socios y empleados que acceden desde una cierta distancia a la red del HGUACH y que por otro lado, han decidido utilizar una red privada virtual para acceder.
Segmentación	• La red presenta un solo segmento.
Sistema de detección de intrusiones (IDS)	• Se desconoce el sistema utilizado para la detección de intrusiones ya que lo manejan terceros.
Inalámbrico	• No se encuentra desactivada la difusión del SSID en el punto de acceso. • El acceso a la red no utiliza la restricción por MAC en el entorno inalámbrico.

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de defensa del perímetro:

Reglas y filtros de cortafuegos

Las mejores prácticas recomendadas por MSAT, en cuanto a esta subcategoría son:

- Aplicar el flujo de datos utilizando las reglas de cortafuegos y las listas de control de acceso de red.
- Poner a prueba las reglas de cortafuegos y de la lista de control de accesos de enrutador para determinar que estén contribuyendo a un ataque realizado hacia un conjunto de equipos, o la red, con el fin de dejar inaccesible el acceso a un servicio o recurso para los usuarios que tienen el acceso permitido.
- Aplicar más de una Zona Desmilitarizada (DMZ), en la implementación de firewall.
- Ubicar todos los servidores accesibles desde internet y restringir la conectividad desde y hacia las DMZ.

Antivirus

Es necesario el uso de antivirus en el entorno a nivel servidor y escritorio, dichas soluciones antivirus deben ser de acuerdo a las tareas específicas que se realizan en la organización. Su configuración debe poder detectar virus en el entorno de entrada y salida. La implementación debe seguir un orden: servidores de archivos críticos, servidores de correo, bases de datos y web.

Antivirus – Servidores

Emplear antivirus en los servidores de archivos con valor para la organización, luego, a los de red, base de datos y correo.

Acceso remoto

En la subcategoría de acceso remoto cabe tener en cuenta, la creación de informes de incidentes y respuesta, para una posterior revisión y evaluación. Por otro lado, todos los usuarios deben ser conscientes que es su responsabilidad el de notificar los diferentes problemas e incidentes de seguridad, mediante el seguimiento de un proceso definido.

La utilización de una red privada virtual para la conectividad de acceso de usuario remoto fundamentada en las tecnologías de: “Internet Protocol Security”, “Secure Socket Layer”, Finalmente es importante el uso de la autenticación multifactor y revisar cada cierto periodo de tiempo la lista de acceso de los usuarios en el equipo de red privada virtual.

Sistema de detección de intrusiones

El sistema de detección de intrusiones (IDS) basado en host y en la red, deben ser implantados para poder detectar y notificar los ataques producidos en la organización.

Segmentación

Hacer uso del segmentado con el fin de obstruir el acceso de una red privada, con objetivos de compartir información para fines comerciales u otros. Todo segmento de red externo debe dirigir el tráfico a puertos y host específicos de las aplicaciones dirigidas a los clientes. Producir medidas en la red para delimitar el acceso para la conexión de terceros. Por último, en segmentación, es importante limitar el acceso de los servicios de red suministrados, y el acceso entre los diferentes segmentos de red.

Inalámbrico

El uso del servicio inalámbrico seguro, implica que la red no hace visible al público el denominado, “Service Set Identifier”, la utilización del acceso Wi-fi protegido para el cifrado y, por otro lado, que la red tampoco sea tenida en cuenta como de desconfianza. También es importante considerar como adicional, al uso de autenticación WPA Y la utilización del filtrado MAC. Finalmente intentar agregar a una red privada virtual, a un segmento de red de no confianza, o similar, a la red inalámbrica.

4.3.2. Autenticación

En este apartado se estudia la situación de los procedimientos estrictos de autenticación de los usuarios, administradores y usuarios remotos, En la Tabla 10, se pueden observar las subcategorías de Autenticación y su puntuación correspondiente.

Tabla 10. *Medidas de defensa de autenticación*

Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas – Cuenta de administrador	
Directivas de contraseñas – Cuenta de usuario	
Directivas de contraseñas – Cuenta de acceso remoto	
Cuentas inactivas	

Fuente: MSAT

La Tabla 11, presenta los resultados de cada una de las subcategorías de Autenticación.

Tabla 11. *Riesgos existentes en autenticación*

Subcategoría	Resultado
Usuarios administrativos	• Tienen acceso de tipo administrativo.
Usuarios internos	• Los usuarios no realizan la utilización de contraseñas complejas bajo ciertos criterios, indicados en las recomendaciones para este tipo de usuarios.
Usuarios de acceso remoto	• Los usuarios no realizan la utilización de contraseñas complejas bajo ciertos criterios, indicados en las recomendaciones para este tipo de usuarios. • Empleados. • Terceros.
Directivas de contraseñas	• No existen procedimientos formales.

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad en cada subcategoría de Autenticación

Usuarios administrativos

La directiva de contraseñas de cuentas administrativas debe cumplir una serie de condiciones:

- Alfanumérico
- Minúsculas y mayúsculas
- ≥ un carácter especial
- Mínimo: 14 caracteres

Por otro lado, debe existir una serie de controles que mitiguen los riesgos de ataques: control del vencimiento y el bloqueo de cuenta después de 7 a 10 inicios fallidos de sesión. Otra opción es recurrir a la autenticación multifactor. Es recomendable utilizar controles avanzados de la gestión de cuentas y del registro de acceso a cuentas (prohibir el tener en común una misma cuenta).

Usuarios Internos

Para los usuarios internos, se debe tener en consideración los siguientes parámetros en sus contraseñas:

- Caracteres alfanuméricos
- Minúsculas y mayúsculas
- ≥ un carácter especial
- Mínimo: 8 caracteres

Al igual que los usuarios administrativos para evitar el riesgo de un ataque, se debe implementar controles como: caducidad, bloqueo de la cuenta tras al menos 10 intentos de inicio de sesión erróneos y registro del sistema. Como otra opción adicional a la contraseña compleja, se puede recurrir a la autenticación de varias fases. Se debe implementar medidas avanzadas para gestionar cuentas y registrar los accesos.

Usuarios de acceso remoto

Los usuarios de acceso remoto que acceden a través de tecnologías de acceso telefónico o red privada virtual, deben también establecer controles de contraseñas complejos. Una contraseña compleja debe cumplir:

- Caracteres alfanuméricos
- Minúsculas y mayúsculas
- ≥ un carácter especial
- Mínimo: 8 caracteres

En este tipo de usuarios es necesario implementar una fase de autenticación adicional a las que se les ha otorgado acceso remoto. Tener en cuenta, el uso de controles avanzados para gestionar las cuentas y el registro de acceso a cuentas. En el acceso remoto es importante la protección del entorno a través del uso de prácticas seguras en la gestión de cuentas, buenas prácticas de registro y un entorno con capacidades de detección de eventos. Con la finalidad de reducir los ataques de fuerza bruta, poner en marcha medidas como: registro del sistema, control del vencimiento y el bloqueo de cuenta después de 7 a 10 inicios fallidos de sesión. Los servicios para el acceso remoto deben considerar sistemas utilizados para la obtención de acceso a redes o host. Se debe tener en consideración el uso de controles para host para el acceso a la red de forma remota.

Directivas de contraseñas

El uso de contraseñas complejas forma parte del DiDI, como ya se mencionó anteriormente. El vencimiento se conforma de la siguiente manera:

- Duración hasta 90 días.
- La nueva cuenta debe cambiarse al comienzo de sesión.
- 8 registros del historial de contraseñas (8 días como mínimo).

En las cuentas administrativas y de usuarios remotos, la autenticación multifactor, se considera muy importante.

En toda cuenta debe ser activada un procedimiento para el bloqueo de cuentas tras 10 intentos fallidos. Existen diferentes tipos de controles de bloqueo, entre ellos los que centran su atención a los ataques de fuerza bruta hacia contraseñas y hay los que son desbloqueados desde una cuenta de administrador. Este proceso se aconseja activarlo en las cuentas administrativas. Si fuese el caso este proceso no sería aconsejable para empresas con ubicaciones remotas u otras, más bien sería recomendable ser desbloqueado por un administrador para que los ataques sean detectados durante un largo periodo, sino se dispone de otros medios para la detección de fallos de autenticación. Las normas más eficientes para el bloqueo de cuenta son:

Bloqueado de la cuenta al haber intentado ingresar incorrectamente, posterior a 7 y 10 veces en cuentas de acceso remoto y administrativas.

- Bloqueado de cuenta de un usuario normal, tras 10 ingresos incorrectos.
- Solicitar la actuación del administrador en las cuentas de administrador y acceso remoto, para los usuarios normales solicitar la reactivación en un periodo de cinco minutos.

4.3.3. Gestión y Control

Para mantener y analizar los entornos informáticos es importante tener en cuenta su gestión, supervisión y el registro adecuado de los mismos. En la Tabla 12, se pueden observar las subcategorías de Gestión y control, y su puntuación correspondiente.

Tabla 12. *Medidas de defensa de gestión y control*

Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Fuente: MSAT

A continuación, se muestra en la Tabla 13, los resultados de la categoría de Gestión y control.

Tabla 13. *Riesgos existentes en gestión y control de infraestructura del HGUACH*

Subcategoría	Resultados
Informes sobre incidentes y respuesta	• Los Usuarios deben conocer el actuar ante cualquier problema de seguridad, y seguir los procedimientos marcados.
Creación segura	• No existen firewalls ubicados en cada área de trabajo. • No hay en las áreas de trabajo del cliente conectado de forma remota al hospital, un software de acceso remoto. • No se utiliza ningún software de cifrado de discos en el entorno.
Seguridad física	• No está puesto en marcha, un sistema que sirva para identificar: empleados, visitas, registro, control de acceso y acompañantes de visitantes. • Los servidores del HGUACH, no se encuentra bajo el resguardo de una estructura cerrada. • No existen mecanismos de protección mediante cableado en los puestos de trabajo. • No existen mecanismos de protección mediante cableado en los equipos portátiles del hospital.

Fuente: Elaboración propia.

En la Tabla 16, se indican soluciones recomendadas para el mejoramiento de la seguridad en la en cada subcategoría de Gestión y control.

Informes sobre incidentes y respuesta

Se recomienda crear procesos para la realización de informes ante incidentes y en el caso de que sucediesen, su actuar. Crear un equipo encargado de dar respuesta ante incidentes imprevistos, compuesto por personal de tecnología, RRHH y leyes. Tener en consideración de implementar un programa completo para dar solución a eventos de

equipos de respuesta a incidentes, gestión de contención, correlación y análisis, y procedimientos de respuesta.

El plan de recuperación y puesta en marcha, tiene que contener los procedimientos bien definidos en archivos y con los conocimientos al día para una recuperación en un lapso de tiempo aceptable. Dichos planes deben ser probados en periodos definidos para la validación de la integridad y el grado de corrección. El plan de continuidad de negocio debe ser aplicado en el entorno físico, tecnológico y personal.

La creación de los informes de incidentes y respuesta este hecho con la finalidad de garantizar que los problemas e incidentes son revisados y evaluados coherentemente. Además, todos los usuarios deben entender la obligación que tienen, de notificar cualquier incidente, y saber que hacer en el caso que se diese.

Creación segura

Crear una directiva, encargada de, requerir verificar periódicamente la configuración predeterminada del firewall, para poder observar los cambios de las aplicaciones o servicios.
La utilización de un software de acceso remoto en todas las estaciones individuales sería recomendable utilizar si se necesitara conectividad remota.

Utilizar cifrado de discos, como AES, para la protección de datos.

Seguridad física

Establecer controles de acceso físico, contra personas no autorizadas que quieran acceder al edificio o a la información. Es necesario concientizar al personal en cuestiones de seguridad a nivel global.

Todo equipo informático debe estar protegido anti hurto. Todo equipo de red y servidores, deben estar ubicados en lugares cerrados y bajo control de personal a cargo.

El acceso a los edificios, datos confidenciales y sistemas, debe estar estrictamente controlado para un acceso no autorizado.

4.4 Resultados y recomendaciones de la evaluación para el área de Aplicaciones

4.4.1. Implementación y uso

El uso de aplicaciones requiere un aseguramiento en cuestiones de seguridad y disponibilidad de esas aplicaciones y los servidores. En la Tabla 14, se pueden observar las subcategorías de Implementación y uso, y su puntuación correspondiente.

Tabla 14. *Medidas de defensa de implementación y uso*

Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicaciones y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	

Fuente: MSAT

La Tabla 15, muestra los resultados de cada una de las subcategorías de Implementación y uso.

Tabla 15. *Riesgos existentes en implementación y uso*

Subcategoría	Resultados
Equilibrio de carga	• No existen balanceadores de carga.
Clústeres	• La agrupación en clústeres no se realiza.
Fabricante de software independiente (ISV)	• Los fabricantes independientes de software no suelen ofrecer al HGUACH revisiones ni actualizaciones de seguridad.
Vulnerabilidades	• No existen procedimientos que aborden los aspectos vulnerables de la seguridad conocidos.

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de Implementación y uso.

Equilibrio de carga

Es recomendable utilizar balanceadores de carga de hardware en el servidor web de primer nivel para mejorar la disponibilidad. El balanceador dispone de una IP (virtual) en la parte externa, le es atribuido las direcciones de cada servidor web en el clúster.

Clústeres

Con la finalidad de garantizar una alta disponibilidad de bases de datos críticas y archivos compartidos emplear mecanismos de clúster.

Fabricante de software independiente (ISV)

Los ISV tienen que verificar y actualizar periódicamente y explicar su propósito y las consecuencias de su uso en términos de función, configuración y seguridad. Por otro lado, tiene que tener a consideración las actualizaciones más relevantes. También debe describir los distintos mecanismos de seguridad de la aplicación y proporcionar la documentación más reciente. La empresa debe conocer las configuraciones necesarias para garantizar el nivel de seguridad más alto.

Desarrollado internamente

En el caso que hubiese equipo de desarrollo interno, debe proporcionar el equipo, actualizaciones y revisiones e indicar el propósito de las actualizaciones y las consecuencias de usarlo, debe tener en consideración la misma normativa que ofrece un ISV. Finalmente, plantearse adquirir servicios de terceros para examinar la arquitectura, y la identificación de posibles fallos.

Vulnerabilidades

Solventar los ya identificados con anterioridad. Es importante a los fabricantes y proveedores en estas cuestiones con la finalidad de adquirir conocimientos sobre nuevas vulnerabilidades.
Si no existen actualizaciones para las vulnerabilidades existentes, buscar o crear un plan de actuación temporal.

Contratar servicios independientes para revisar regularmente el diseño de la seguridad de la aplicación.

4.4.2. Diseño de aplicaciones

El diseño de las aplicaciones lleva consigo un buen manejo en la autenticación, autorización y validación de datos, el conjunto de los mismos, ayudará a que los atacantes no puedan aprovechar las vulnerabilidades de seguridad. En la Tabla 16, se pueden observar las subcategorías de Diseño de aplicaciones y su puntuación correspondiente.

Tabla 16. *Medidas de defensa en diseño de aplicaciones*

Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	

Fuente: MSAT

La Tabla 17, muestra los resultados cada una de las subcategorías de Diseño de aplicaciones.

Tabla 17. *Riesgos existentes en diseño de aplicaciones*

Subcategoría	Resultados
Autenticación	• No se usan directivas de contraseñas en las aplicaciones principales para la autenticación
Directivas de contraseñas	• No se usan controles de contraseñas en las aplicaciones principales
Registro	• No se registran todos los eventos, intentos fallidos de autenticación, errores, accesos denegados y correctos, ni cambios en las cuentas.
Validación de datos de entrada	• Los datos de entrada no son validados. • Los datos de entrada provenientes de un feed de datos no son validados.
Metodologías de desarrollo de seguridad de software	• No existe formación en esta subcategoría.

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de diseño de aplicaciones.

Autenticación

Toda aplicación debe implementar un mecanismo de autenticación directamente proporcional a la importancia de sus datos o uso. Las contraseñas deben ser complejas. Todo componente de acceso a datos o funciones tiene que ser autentificado. Debe estar protegido en todo momento el acceso administrativo con sistemas de autenticación robustos y el uso de contraseñas solidas con directivas de contraseñas debería tenerse en consideración la autenticación multifactor para aumentar la seguridad. Las cuentas administrativas deben ser más restrictivas que las de las cuentas normales.

Directivas de contraseñas

Con las mismas características marcadas para directivas de contraseñas como ya se mencionó anteriormente. El vencimiento se conforma de la siguiente manera:

- Duración hasta 90 días.
- La nueva cuenta debe cambiarse al comienzo de sesión.
- 8 registros del historial de contraseñas (8 días como mínimo).

Protección de autenticación con sistemas robustos. Estas son más restrictivas. Si una cuenta normal requiere 8 caracteres, las administrativas deben contener 14.
Activar el bloqueo de cuentas tras 10 intentos fallidos en todas las cuentas de usuario. Las políticas aplicadas para el bloqueo son:

- Bloqueado después de 10 intentos fallidos de registro de la cuenta de usuario.
- Intervención del administrador para desbloqueo de acceso a aplicaciones importantes y reactivación automática después de 5 minutos en cuentas de usuario común.
- En cuentas de usuarios comunes: 30 minutos para almacenamiento en caché.

Registro

El total de las aplicaciones deben tener activado archivos de registro. Los datos de archivos de registro servirán para los análisis de incidentes, tendencias y auditorías. Se debe registrar toda la gestión relacionada con la autenticación, datos y cuentas. Al ingresar información en los archivos de registro, se debe restringir los de carácter confidencial.

Validación de datos de entrada

El aplicativo admitirá el ingreso de datos desde diferentes fuentes externas. Sintaxis y semántica exactas. El servidor será el encargado de validar los campos suministrados por el usuario.

Metodologías de desarrollo de seguridad de software

Emplear las más adecuadas, con la finalidad de aumentar la seguridad.
En el caso de utilizar terceros, verificar que tengan los conocimientos adecuados en este tema.

Las personas encargadas de desarrollo, administradores de desarrollo, evaluadores, y de control y calidad deberán recibir capacitaciones que contengan la metodología utilizada. Se considera importante ir actualizando los conocimientos cada año en cuestiones de modelos de amenaza, uso de herramientas de prueba y metodologías de desarrollo de seguridad de software. Hacer uso de aplicativos que ponen a prueba la eficacia de la seguridad.

4.4.3. Almacenamiento y comunicaciones de datos

En este apartado se pretende tratar la integridad y confidencialidad de los datos, si estos no se manejasen correctamente, podría afectar negativamente a la reputación y economía del HGUACH. En la Tabla 18, se pueden observar las subcategorías de almacenamiento y comunicaciones de datos, y su puntuación correspondiente.

Tabla 18. *Medidas de defensa de almacenamiento y comunicaciones de datos*

Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado – Algoritmo	

Fuente: MSAT

La Tabla 19, presenta los resultados de cada una de las subcategorías de almacenamiento y comunicaciones de datos.

Tabla 19. *Riesgos existentes en almacenamiento y comunicaciones de datos*

Subcategoría	Resultados
Cifrado	• Esta información no es conocida por el personal de TI del HGUACH
Cifrado – Algoritmo	• El uso de algoritmos de cifrado adecuado, no se realiza.

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de almacenamiento y comunicaciones de datos

Cifrado

Los datos de carácter reservado deben estar cifrados o codificados en la base de datos y en el sistema de archivos mediante un algoritmo que tenga la misma longitud de los datos de entrada, en la salida. La aplicación debe ser capaz de diferenciar los diferentes tipos de datos: los expuestos a divulgación, los manipulables y los que puedan ser cambiados. El lugar de almacenamiento de las claves para descifrar, deberá ser diferente al de la información cifrada.

Los datos confidenciales deberían ser cifrados antes de ser compartidos. Comprobar que los componentes intermedios que gestionan todo el proceso de transmisión de datos, no sean una amenaza potencial.

Cifrado – Algoritmo

La aplicación debe tener algoritmos de cifrados estándares existentes en el sector, con modelos y tamaños adecuados.

4.5 Resultados y recomendaciones de la evaluación para el área de Operaciones

4.5.1. Entorno

La seguridad del HGUACH depende en mayor parte de los operativos, procesos y las pautas. Por otro lado, es de vital importancia tener una documentación clara y exacta del entorno y las pautas. En la Tabla 20, se pueden observar las subcategorías del entorno y su puntuación correspondiente.

Tabla 20. *Medidas de defensa del entorno*

Entorno	●
Host de gestión	●
Host de gestión – Servidores	●
Host de gestión - Dispositivos de red	●

Fuente: MSAT

La Tabla 21, muestra los resultados de cada una de las subcategorías del entorno.

Tabla 21. *Riesgos existentes en el entorno*

Subcategoría	Resultados
Host de gestión	• No existe ningún host de gestión
Host de gestión – Servidores	• No existe ningún host de gestión dedicado a los servidores
Host de gestión – Dispositivos de red	• No existe ningún host de gestión dedicado a los dispositivos de red

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría en el entorno.

Entorno

Todo plan de recuperación ante desastres y reanudación del mismo, debe estar documentado y actualizado. Deben ser aprobado periódicamente, en el caso de los de continuidad en la actividad, su enfoque debe ser en el entorno: físico, técnico y personal.

4.5.2. Directiva de seguridad

En la Tabla 22, se pueden observar las subcategorías de la directiva de seguridad y su puntuación correspondiente.

Tabla 22. *Medidas de defensa de la directiva de seguridad*

Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	

Fuente: MSAT

La Tabla 23, muestra los resultados de cada una de las subcategorías de la directiva de seguridad.

Tabla 23. *Riesgos existentes en la defensa de la directiva de seguridad*

Subcategoría	**Resultados**
Eliminación de datos	• El hospital no dispone de un procedimiento formal documentado para la destrucción de datos.

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad en la en cada subcategoría de directiva de seguridad.

Eliminación de datos

Se debe generar procesos para la destrucción de datos, dirigidos a todos los usuarios.

4.5.3. Gestión de actualizaciones y revisiones

El HGUACH, debe tener como un punto importante, un plan de actualizaciones y revisiones para cubrir la seguridad del entorno informático para su funcionamiento correcto. La aplicación de estos, hace que el entorno este protegido contra las vulnerabilidades ya conocidas o incluso podría hacer frente a nuevas que puedan aparecer. En la Tabla 24, se pueden observar las subcategorías de la gestión de actualizaciones y su puntuación correspondiente.

Tabla 24. *Medidas de defensa de la gestión de actualizaciones y revisiones*

Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	

Fuente: MSAT

La Tabla 25, presenta los resultados de cada una de las subcategorías de la gestión de actualizaciones y revisiones.

Tabla 25. *Riesgos existentes en la gestión de actualizaciones y revisiones*

Subcategoría	Resultados
Documentación de la red	• El hospital no dispone de documentación de configuración precisa para la infraestructura de red. No dispone de diagramas actualizados
Flujo de datos de la aplicación	• Carencia de esquemas que definan la arquitectura y el flujo de datos
Gestión de actualizaciones	• No se prueban las actualizaciones y revisiones antes de aplicarlas

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de gestión de actualizaciones y revisiones.

Gestión de cambios y configuración

Los procesos de gestión de cambios y configuraciones permiten asegurar que los cambios en el entorno de producción, se han probado y documentado exhaustivamente antes de utilizarse.

4.5.4. Copias de seguridad y recuperación

Este apartado está basado en la planificación de recuperación ante desastres que pudiesen ocurrir y a la reanudación de los procesos del HGUACH, ante la ocurrencia de los mismos. En la Tabla 26, se pueden observar las subcategorías de copias de seguridad y recuperación y su puntuación correspondiente.

Tabla 26. *Medidas de defensa de las copias de seguridad y recuperación*

Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación del negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Fuente: MSAT

La Tabla 27, muestra los resultados de cada una de las subcategorías de copias de seguridad y recuperación.

Tabla 27. *Riesgos existentes en copias de seguridad y recuperación*

Subcategoría	Resultados
Planificación de recuperación ante desastres y reanudación del negocio	• Existen pero no están documentadas

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de copias de seguridad y recuperación.

Planificación de recuperación ante desastres y reanudación del negocio

Se recomienda documentar los procedimientos para una evaluación periódica.

4.6 Resultados y recomendaciones de la evaluación para el área de personal

4.6.1. Requisitos y evaluaciones

Todo encargado del área de TI que tome decisiones, debe comprender los requisitos de seguridad, para una gestión correcta y aumento de la seguridad. En la Tabla 28, se pueden observar las subcategorías de requisitos y evaluaciones, y su puntuación correspondiente.

Tabla 28. *Medidas de defensa de requisitos y evaluaciones*

Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	

Fuente: MSAT

La Tabla 29, muestra los resultados de cada una de las subcategorías de requisitos y evaluaciones.

Tabla 29. *Riesgos existentes en requisitos y evaluaciones*

Subcategoría	Resultados
Requisitos de seguridad	• El equipo de seguridad no participa en la fase de planificación ni diseño del ciclo de vida de la tecnología • El equipo de seguridad no participa en la fase de implantación del ciclo de vida de la tecnología • El equipo de seguridad no participa en la fase de comprobación del ciclo de vida de la tecnología
Evaluaciones de seguridad	• El HGUACH no encomienda esta tarea a terceros

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de requisitos y evaluaciones.

Requisitos de seguridad

El HGUACH debe identificar a las personas experimentadas en cuestiones de seguridad que formen parte en reuniones y decisiones. Deben protegerse, de acuerdo al valor del recurso y el nivel de seguridad que se requiera. Dentro del análisis se deben incluir todo aquello que afecte a los activos. Una buena estrategia equilibra costes y beneficios de las salvaguardas utilizadas y su resultado puede ser la aceptación o rechazo del riesgo. Los requisitos de seguridad definidos por los técnicos y representantes comerciales, deben estar debidamente documentados y publicados para que el personal, pueda consultarlos y contrastar para diseños futuros.

Evaluaciones de seguridad

Una evaluación por terceros, aporta un punto de vista objetivo muy valioso para las medidas de seguridad de una organización, también podrían ser beneficiosas para el cumplimiento de los términos en políticas y los requisitos planteados.

La evaluación debe centrarse en el reconocimiento de las debilidades presentes en los activos. Se deben examinar las directivas y los procedimientos de seguridad para identificar procesos faltantes, o no definidos.

4.6.2. Directiva y procedimientos

Para minimizar el nivel de riesgo, se deben tener los procedimientos claros y prácticos, en cuanto al manejo con fabricantes y socios. Al igual, a la hora de contratar personal con procedimientos adecuados y finalizar su contrato de la manera correcta, evitará inconvenientes para la organización. En la Tabla 30, se pueden observar las subcategorías de directiva y procedimientos, y su puntuación correspondiente.

Tabla 30. *Medidas de defensa de directiva y procedimientos*

Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	

Fuente: MSAT

La Tabla 31, muestra los resultados de cada una de las subcategorías de directiva y procedimientos.

Tabla 31. *Riesgos existentes en directiva y procedimientos*

Subcategoría	**Resultados**
Relaciones con terceros	• No están incluidas condiciones específicas de seguridad en los SLA (Acuerdos de nivel de servicio) • No existe ninguna directiva para las relaciones con terceros

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de directiva y procedimientos.

Relaciones con terceros

En el caso de no tener, crear directrices y procedimientos formales para las relaciones con terceros, con el fin de identificar problemas y adjudicar responsabilidades por parte y parte al solventarlos. Estas deben integrar:

- Nivel de conexión y acceso.
- Presentación y procesamiento de datos.
- Roles, responsabilidades y permisos definidos.
- Gestión de relaciones: creación, mantenimiento y cese.

4.6.3. Formación y conocimiento

Con la finalidad de divulgar las medidas de seguridad que tiene el HGUACH, se procede al análisis de este apartado. En la Tabla 32, se pueden observar las subcategorías de formación y conocimiento, y su puntuación correspondiente.

Tabla 32. *Medidas de defensa de formación y conocimiento*

Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

Fuente: MSAT

La Tabla 33, presenta los resultados de cada una de las subcategorías de directiva y procedimientos.

Tabla 33. *Riesgos existentes en directiva y procedimientos*

Subcategoría	Resultados
Conocimientos de seguridad	• El equipo de seguridad no participa en la definición de los requisitos para las nuevas tecnologías o para las ya existentes • Carece de un plan de divulgación de medidas en esta área.
Formación sobre seguridad	• La formación de seguridad de aplicaciones no se ofrece a los empleados en función de su puesto en la empresa • La formación de preparación para incidentes y reacción no se ofrece a los empleados en función de su puesto en la empresa • La formación de seguridad de infraestructura no se ofrece a los empleados en función de su puesto de trabajo

Fuente: Elaboración propia.

A continuación, se indican soluciones recomendadas para el mejoramiento de la seguridad para cada subcategoría de formación y conocimiento.

Conocimiento sobre seguridad

Existencia de un programa formal para la divulgación de las medidas de seguridad, que ayude a la seguridad global organizacional. Por otro lado, se deben también incluir en el curso los empleados nuevos. Se debe divulgar los conocimientos actualizados y cursos que fomenten buenas prácticas y los riesgos más actuales. Realizar evaluaciones destinadas al personal, para comprobar que han entendido la información dada.

Formación sobre seguridad

Analizar con los propietarios de la organización, la determinación del tiempo de inactividad de aplicaciones críticas. Al utilizar balanceadores de carga frente a los servidores web, se ve mejorada la disponibilidad y rendimiento. Para el equilibrio de la carga del servidor, el balanceo de la carga reparte las peticiones entre los nodos en el clúster optimizando el rendimiento del sistema. Lo mismo ocurriría si se diese un error en un servidor web, otro servidor tomaría la solicitud.

4.7 Subcategorías que requieren atención en la seguridad del HGUACH

En la Tabla 34, se muestran en orden de prioridad las subcategorías que no cumplen las mejores prácticas recomendadas.

Tabla 34. *Subcategorías que presentan problemas de seguridad en el HGUACH*

Prioridad alta	Prioridad intermedia	Prioridad baja
• Gestión de actualizaciones • Relaciones con terceros • Conocimiento de seguridad • Usuarios administrativos • Acceso remoto	• Seguridad física • Requisitos de seguridad • Evaluaciones de seguridad • Gestión de cambios y configuración • Registro	• Protocolos y servicios • Uso aceptable • Copias de seguridad • Antivirus – Equipos de escritorio • Autorización y control de acceso

Fuente: Adaptado. Informe completo de MSAT.

A continuación, se describen por sector, las prácticas más destacadas:

4.7.1. Acciones recomendadas de prioridad alta

Gestión de actualizaciones (Operaciones): seguir la práctica actual y revisar la información en la sección de mejores prácticas recomendadas para hacer todos los cambios necesarios en sus directivas. Plantearse una evaluación de SMS y WSUS para la administración y utilización automática de actualizaciones para servidores de Windows.

Relaciones con terceros (Personal): para reducir los riesgos que implica la ejecución de los servicios predeterminados, el personal interno debería configurar lo sistemas siguiendo una simulación de creación.

Conocimiento de seguridad (Personal): El HGUACH, debe proporcionar un medio a todo el personal para indicarles las medidas de seguridad adoptadas y sus riesgos para así

poder cumplirlas. Por otro lado, continuar asegurándose que el HGUACH tenga una persona o equipo responsable de la seguridad y requiera que se consulte a este equipo antes de realizar cambios en el entorno informático

Usuarios administrativos (Infraestructura): distinguir las cuentas de usuario, por prioridad de administración o gestión y tener en cuenta las directivas de contraseñas para cada una de ellas.

Acceso remoto (Infraestructura): emplear red privada virtual basadas en "Internet Protocol Security", "Secure Socket Layer" o "Secure Shell", para la conexión de acceso de usuario remoto. Con el fin de restringir el acceso a los recursos de la organización crear listas de acceso a redes y de usuario.

4.7.2. Acciones recomendadas de prioridad intermedia

Seguridad física (Infraestructura): emplear diferentes controles físicos y plantearse su uso los equipos de la organización.

Requisitos de seguridad (Personal): continuar asignando niveles de importancia a los componentes y asegurarse de actualizar el modelo según se añada al equipo nuevo.

Evaluaciones de seguridad (Personal): evaluar la infraestructura crítica de red y aplicaciones.

Gestión de cambios y configuración (Operaciones): previo a la puesta en marcha, utilizar un proceso formal de gestión de las configuraciones y de los cambios para su verificación y documentación.

Registro (Aplicaciones): para facilitar la gestión y el análisis de los archivos de registro, puede integrarlos en un mecanismo de registro central. Este mecanismo guarda estos archivos según la directiva corporativa de retención de datos.

4.7.3. Acciones recomendadas de prioridad baja

Protocolos y servicios (Operaciones): documentar las pautas de los protocolos y servicios permitidos y publicar esta información en la intranet corporativa. Considerar la implantación de directivas que regulen los cambios en las pautas.

Uso aceptable (Operaciones): todos los empleados y clientes que hacen uso de los recursos corporativos deberán estar familiarizados con estas directivas. Publicarlos en la intranet y estudiar introducirlas en el curso de orientación de empleados nuevos.

Copias de seguridad (Operaciones): auditar estos procesos regularmente, y comprobar que son aplicados a los recursos más delicados.

Equipos de escritorio (Infraestructura): utilizar unas directrices, que lleven al usuario a renovar la licencia de antivirus.

Autorización y control de acceso (Aplicaciones): examinar las principales aplicaciones para los usuarios que acceden desde internet.

CONCLUSIONES

- La evaluación realizada cumple con los objetivos del proyecto dando a conocer los riesgos del ambiente informático del HGUACH mediante el uso de la herramienta MSAT. La herramienta MSAT está diseñada para empresas medianas que disponen de entre 50 a 500 equipos informáticos.

- La información recibida por la herramienta, sirve como antecedente para tener en consideración las partes del entorno informático que requieren ser modificadas o mejoradas, por lo tanto, el uso de la herramienta MSAT, no puede medir la eficacia de las medidas de seguridad utilizadas.

- Al obtener el resultado de BRP, se debe tener en cuenta que una puntuación de 0, no existe, toda actividad comercial implica un riesgo. Por otro lado, el resultado de DiDI, no es sinónimo de eficacia en seguridad, más bien cuantifica la estrategia global utilizada para la defensa del entorno informático.

- En los resultados se puede observar un desequilibrio significativo en las áreas de operaciones y personal, esto implicaría la necesidad de volver a alinear las inversiones del HGUACH en estas áreas.

RECOMENDACIONES

- Implementar las acciones descritas en la guía de actividades prioritarias para cada área establecida, con el fin de proteger los activos del HGUACH, y así ayudar a cumplir los objetivos de la organización.

- Crear un equipo de respuestas de emergencia en la organización, donde estén incluidos representantes especializados en tecnología, recursos humanos y legal, a fin de crear responder a todos los incidentes y problemas de seguridad que puedan aparecer en la organización.

- Programas de capacitación para el personal de TI, y para toda aquella persona nueva, que se incorpore a un puesto en el área de TI.

- Para mejorar la seguridad de TI se recomienda realizar evaluaciones periódicas en las áreas de TI, que permitan mejorar e implementarse medidas.

- Aplicar la segmentación de la red, con la finalidad de impedir el acceso a extranets específicas, como es el caso de fabricantes, socios o clientes.

- Se recomienda la utilización de controles formales que permitan el cumplimiento de las directivas de contraseñas en todas las cuentas del HGUACH.

- Teniendo en cuenta que la normativa en cuestiones de seguridad, va cambiando constantemente a lo largo del tiempo, es importante volver a realizar periódicamente nuevas evaluaciones de riesgos o procesos de auditoría.

BIBLIOGRAFÍA

Adnan Diwan, S., Ghaleb, M., & Hasan Abd, M. (2018). *Risk Management Framework and Evaluation: Detail Site Study and Governance of Information Security Risk Management in Medical Information Technology Infrastructure in Hospitals*. *Indian Journal of Science and Technology*.

Alemán Novoa, H., & Rodríguez Barrera, C. (2015). *Metodologías para el análisis de riesgos en los sgsi.* Publicaciones E Investigación, 9, 73 - 86. https://doi.org/10.22490/25394088.1435

Andrade de Freitas, S. A., Canedo, E. D., Santos Felisdório, R. C., & Leão, H. A. T. (2018). *Analysis of the risk management process on the development of the public sector information technology master plan. Information*, *9*(10), 248.

Areitio, J.. (2008). *Seguridad en la Información. Redes, informática y sistemas de información* Madrid: Paraninfo.

Arismendi Ramírez, J. (2018). *Análisis de riesgos y diagnóstico de la seguridad de la información de la ESE Hospital Santa Mónica, bajo los parámetros de la seguridad informática.*

Bischoff, P.. (2020). *Which countries have the worst (and best) cybersecurity?*. 2020, agosto 01, de comparitech Recuperado de https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Calderón Ramos, V. P. (2016). *Análisis de riesgos informáticos y desarrollo de un plan de seguridad de la información para el gobierno autónomo descentralizado municipal de Catamayo* (Doctoral dissertation, Tesis de Grado. Loja: Universidad Nacional de Loja).

De Freitas, V. (2009). *Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Enl@ ce: Revista Venezolana de Información, Tecnología y Conocimiento*, *6*(1), 43-56.

Dennis Fisher. (2014). *Era termina con la ruptura de un grupo de computación confiable en Microsoft*. 2020, septiembre 18, de threat post Recuperado de https://threatpost.com/era-ends-with-break-up-of-trustworthy-computing-group-at-microsoft/108404/

Docplayer. (2016). Conceptos generales sobre seguridad informática, febrero 27, de Docplayer Recuperado de https://docplayer.es/10590254-Conceptos-generales-sobre-seguridad-informatica.html.

ESET. (2018). *ESET Security Report 2018.* 2020, agosto 01, de ESET Recuperado de https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

Force, J. T. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology (NIST) Special Publication 800–37*. DOI: 10.6028/NIST.SP.800-37r2.

García, G. L. (2015). ANÁLISIS Y DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA REDES DE DATOS MEDIANTE ENFOQUES ISO 27001 Y LA UTILIZACIÓN DE TÉCNICAS DE DEFENSA. CASO DE ESTUDIO: EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN NICOLÁS. Universidad de Córdoba.

https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/283/Trabajo_de_Grado.pdf?sequence=1&isAllowed=y

Guzmán Pacheco, G. F. (2015). *Metodología para la Seguridad de Tecnologías de Información y Comunicaciones en la Clínica Ortega*, febrero 27, de Universidad Nacional del Centro de Perú Recuperado de http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/1478/Tesis-Goyo%20Francisco%20Guzman%20Pacheco.pdf?sequence=1&isAllowed=y

Global STD. (2017). *HISTORIA DE LA FAMILIA ISO 9000. 2020*, diciembre 1, de Global STD CERTIFICATION Recuperado de https://www.globalstd.com/blog/historia-de-la-familia-de-normas-iso-9001/

Harán, J.. (2020). *Hospitales: uno de los principales blancos de ciberataques*. 2020, agosto 05, de welivesecurity Recuperado de https://www.welivesecurity.com/la-es/2020/04/22/por-que-hospitales-blanco-atractivo-cibercriminales/

Imbaquingo, D. E., Herrera-Granda, E. P., Herrera-Granda, I. D., Arciniega, S. R., Guamán, V. L., & Ortega-Bustamante, M. C. (2019). *Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente*. Revista Ibérica de Sistemas e Tecnologias de Informação, (E22), 349-362.

INCIBE. (2016). *Las 5 medidas básicas para proteger tu principal activo: la información*. 2020, agosto 08, de INCIBE Recuperado de https://www.incibe.es/protege-tu-empresa/blog/las-5-medidas-basicas-proteger-tu-principal-activo-informacion

INTERNATIONAL STANDART ISO/IEC 27000. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary. Switzerland: ISO/IEC.*

ISOTools. (2019). *Análisis y evaluación de riesgos de seguridad de la información: identificación de amenazas, consecuencias y criticidad*. 2020, diciembre 1, de ISOTools Recuperado de https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/

Ladd, D. & Simorjay, F. & Pulikkathara, G & Jones, J. & Miller, M. & Lipner, S. & Rains, T.. (2011). *Informe de progreso del proceso SDL*. Redmond, Washington: Microsoft.

Liñan, R. (2017). DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, DE LA IPS MEDICSALUD DE LA CIUDAD DE VALLEDUPAR – CESAR, febrero 27, de UNAD Recuperado de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12927/1/1065573091.pdf

Ma, Q., & Pearson, J. M. (2005). *ISO 17799:" Best Practices" in Information Security Management?*. *Communications of the Association for Information Systems*, *15*(1), 32.

Maliza, A., nd *PLAN DE SEGURIDAD INFORMÁTICA.*

Marcos Carvajal, R. (2015). Estudio de las normas españolas y estadounidenses de seguridad de la información.

Microsoft. (2017). *Herramienta de Evaluación de Seguridad de Microsoft (MSAT).* 2020, agosto 18, de Microsoft Recuperado de https://docs.microsoft.com/es-es/security-updates/security/technetsecurityherramientadeevaluacindeseguridaddemicrosoftmsat

Microsoft. (2006). Microsoft Security Assessment Tool. Microsoft Downloads. https://www.microsoft.com/es-es/download/details.aspx?id=12273

Microsoft. (2017). *Herramienta de Evaluación de Seguridad de Microsoft (MSAT).* 2020, septiembre 18, de Microsoft Recuperado de https://docs.microsoft.com/es-es/security-updates/security/technetsecurityherramientadeevaluacindeseguridaddemicrosoftmsat#mainsection

Molina-Miranda, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. *Espirales revista multidisciplinaria de investigación*, *1*(11).

Myler, E., & Broadbent, G. (2006). ISO 17799: Standard for security. *Information Management*, *40*(6), 43.

NIST. (2018). *Información General de la Publicación Especial del NIST serie 800*. 2020, diciembre 1, de NIST Recuperado de https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

NIST. (2020). *About CSRC*. 2020, septiembre 03, de NIST Recuperado de https://csrc.nist.gov/about

PMG SSI. (2016). ¿Cómo utilizar la serie SP 800 de la norma ISO 27001?. 2020, diciembre 1, de PMG SSI Recuperado de https://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/

Quintanilla Romero, M. A., Quintana Sánchez, A. M., Ojeda Escobar, J. A., & Trujillo Calero, G. E. (2016). Estandares Internacionales para el Control en las ISO.

Rafael, S. G., Pedro, V. L., & Alejandra, O. (2018). *La gestión de riesgo: el ausente recurrente de la administración de empresas.* Revista Ciencia Unemi, 11(26), 51-62.

Ramírez Montealegre, B. J. (2016).)Medición de madurez de ciberseguridad en pymes colombianas. *Departamento de Ingeniería de Sistemas e Industrial*.

Rea-Guaman, M., Calvo-Manzano, J. A., & San Feliu, T. (2018). *Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas A Prototype to Manage Cybersecurity in Small Companies.*

Reinoso Córdova, A. R. (2017). *Análisis y evaluación de riesgos de seguridad informática a través del análisis de tráfico en redes de área local. Aplicación a un caso de estudio* (Bachelor's thesis, Quito, 2017.).

Rodríguez Grefa, M. Y. (2019). Control interno basada en la norma ISSAI 5300 para procesos informáticos en la dirección distrital 16d01 de Pastaza.

Rouse, M. (2006). *NIST 800 Series.* 2020, agosto 20, de WhatIs.com Recuperado de https://whatis.techtarget.com/definition/NIST-800-Series

Santa Cruz Quiroz, H. M. (2016). *Implementación de gestión de riesgos de ti para obtener la certificación ISO 27001 en el Hospital Regional Lambayeque.*

Scott Charney. (2014). *Looking Forward: Trustworthy Computing*. 2020, octubre 10, de Microsoft Recuperado de

https://www.microsoft.com/security/blog/2014/09/22/looking-forward-trustworthy-computing/

Serrano, J. E. R., Salazar, V. H., Ruiz, X. N., & Guillén, C. N. (2019). *Gestión de Riesgos de TIC en hospitales públicos*. Revista Ibérica de Sistemas e Tecnologias de Informação, (E20), 280-291.

UNIR. (2018). *Metodologías de Desarrollo Web Seguro*. 2020, septiembre 15, de Universidad Internacional de la Rrioja Recuperado de http://manosnegras.com/unir2018/wp-content/uploads/2017/11/T1.Metodolog%C3%ADas.pdf

Urruchurtu, M. (2013). "Plan estratégico de seguridad de información den una empresa del sector industrial basado en ISO/IEC 27001" Caso de estudio: COTEMAR (Corporación de Ciencia y Tecnología para el desarrollo de la industria naval, marítima y fluvial), febrero 27, de Universidad Tecnológica de Bolívar Recuperado de https://biblioteca.utb.edu.co/notas/tesis/0065348.pdf

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo editorial PATRIA.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI*-Revista Ibérica de Sistemas e Tecnologias de Informação, (22), 73-88.

Vanegas Barrero, A. (2016). *Seguridad para minimizar riesgos en el desarrollo del software* (Bachelor's thesis, Universidad Piloto de Colombia).

ANEXOS

Anexo A: Distribución organizacional segmentada del HGUACH

1.1 Organigrama de la distribución del departamento Administrativo Financiero

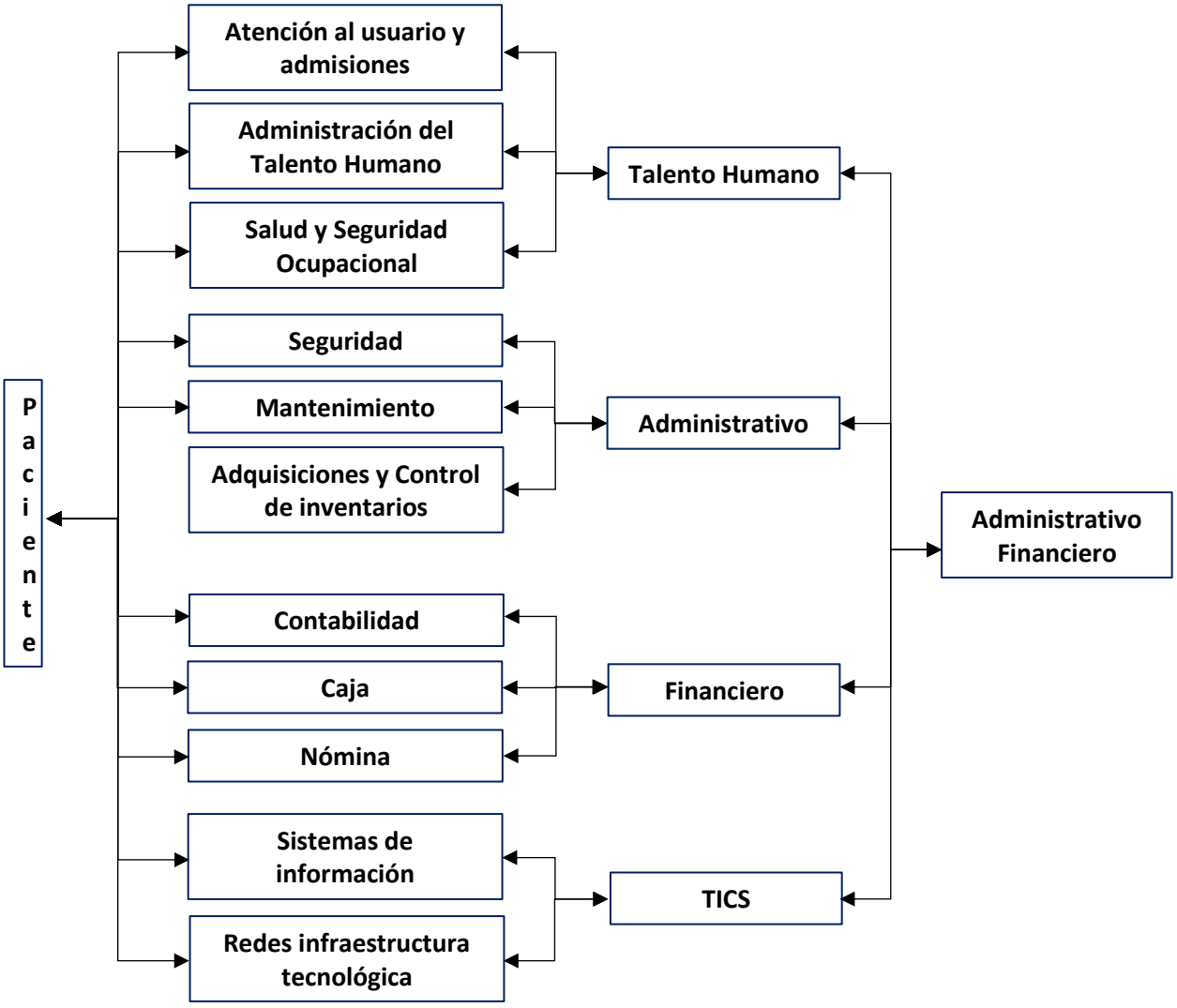


Figura 5. Organigrama del departamento Administrativo Financiero
Fuente: Elaboración propia

1.2 Organigrama de la distribución del departamento de Director Médico

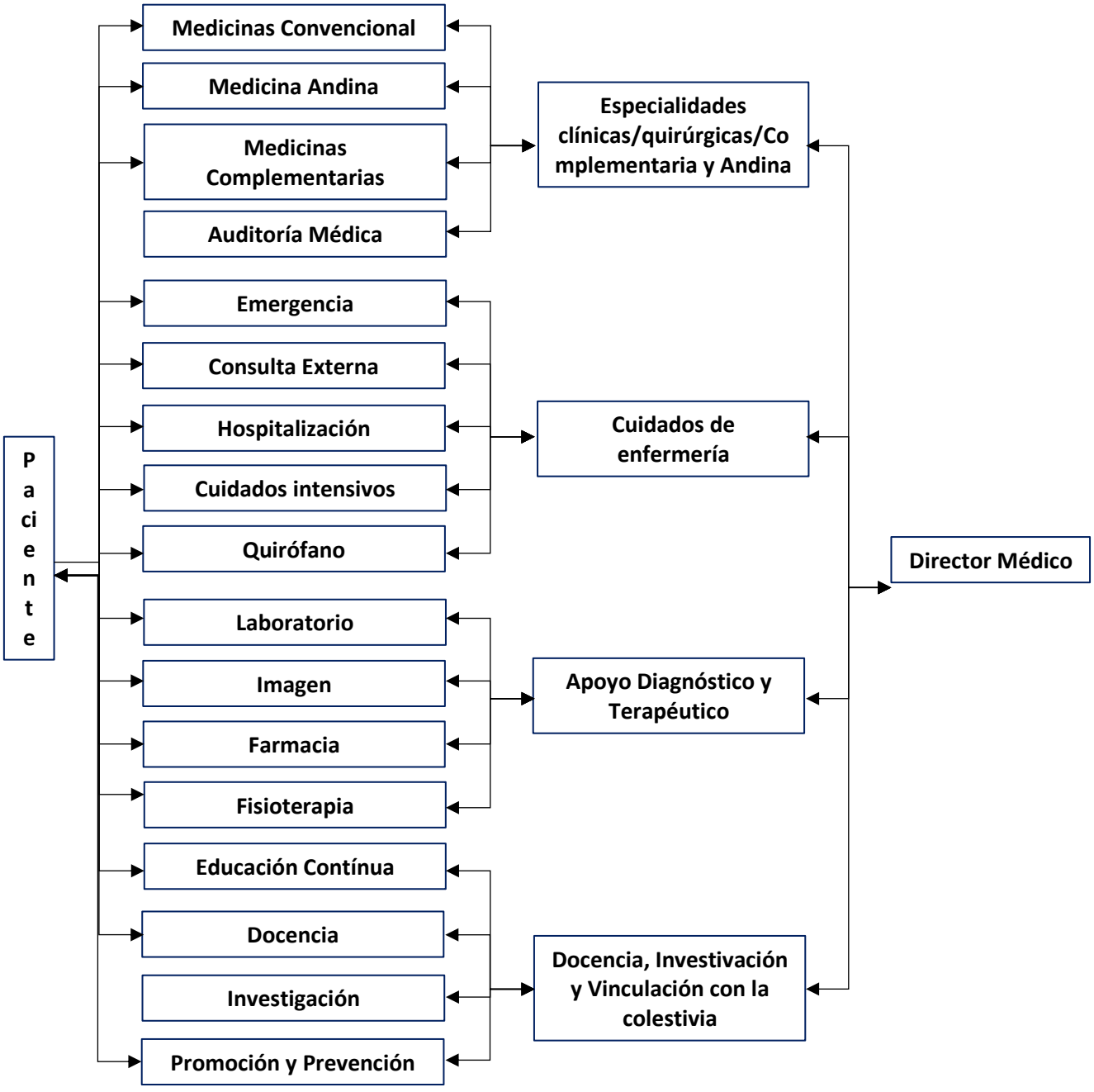


Figura 6. Organigrama de Director Médico
Fuente: Elaboración propia

Anexo B: Distribución de los Switches del HGUACH

2.1 Topografía de red del Switch de Imagen

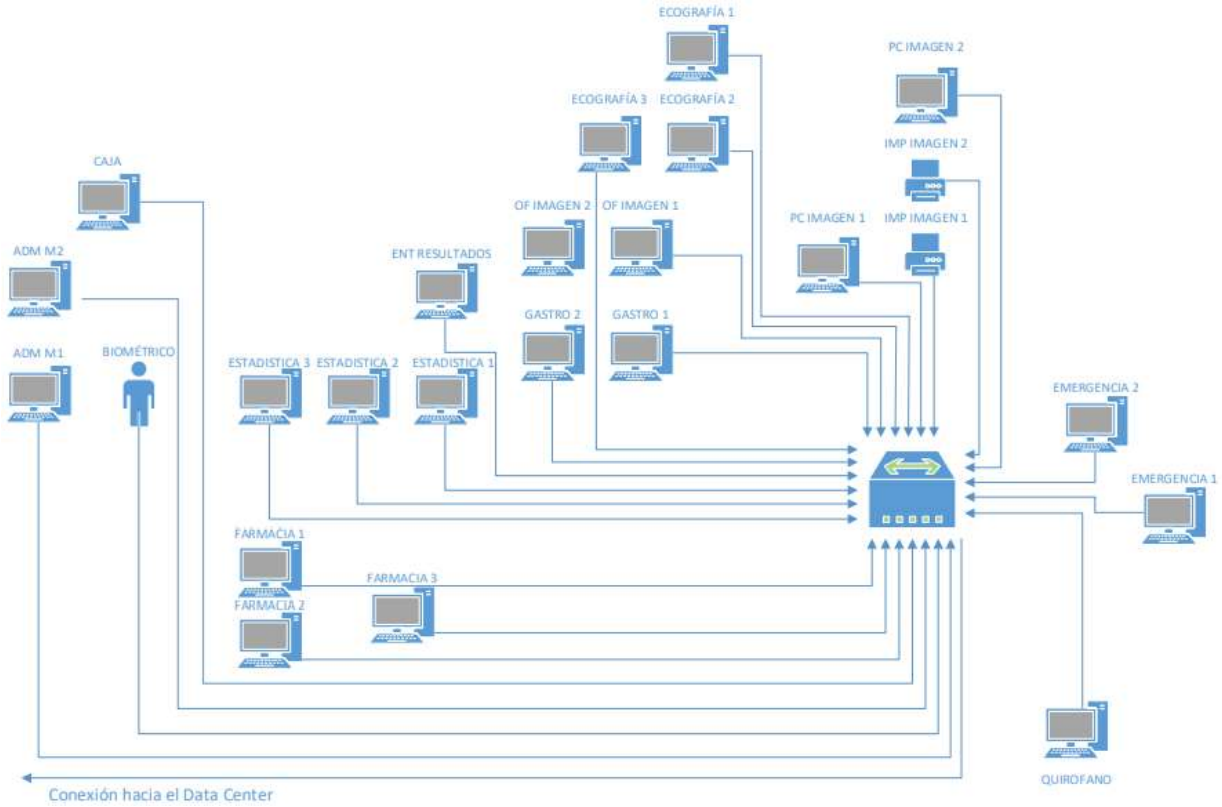


Figura 7. Topografía switch del departamento de Imagen
Fuente: Informe Técnico de Cableado Estructurado

2.2 Topografía de red del Switch de Hospitalización y nutrición

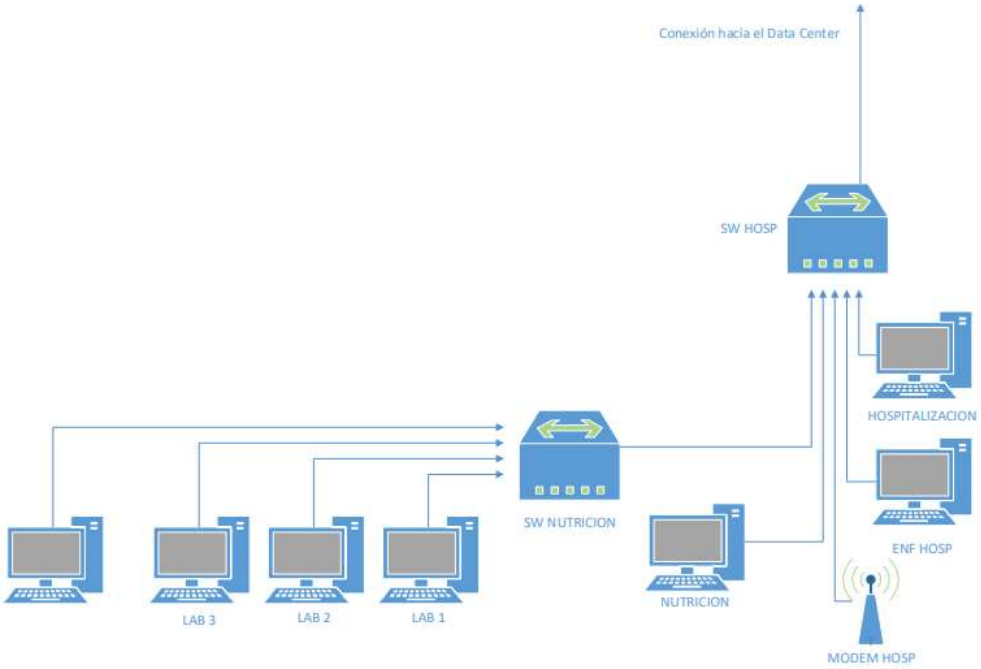


Figura 8. Topografía switch hospitalización y switch nutrición
Fuente: Informe Técnico de Cableado Estructurado

2.3 Topografía de red del Switch del departamento Administrativo

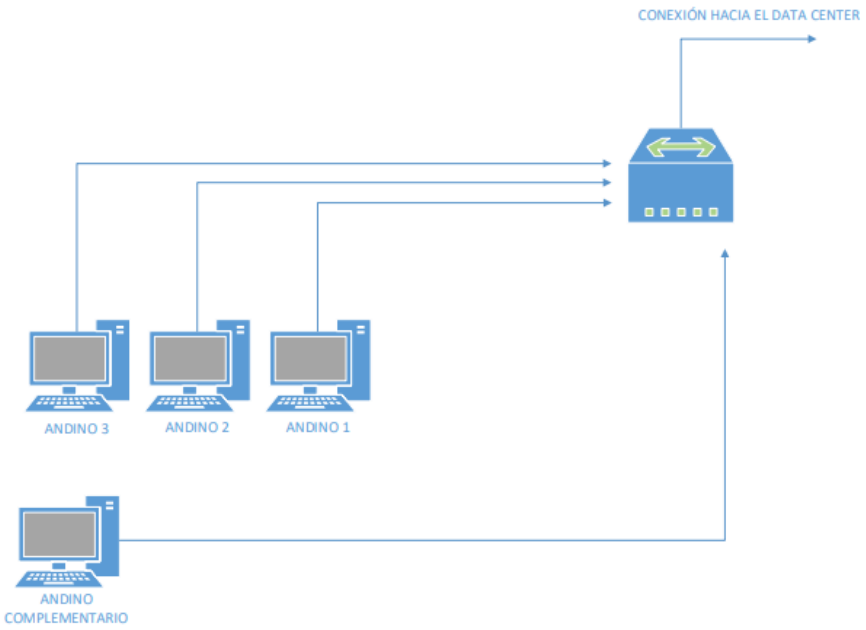


Figura 9. Topografía switch Administración.
Fuente: Informe Técnico de Cableado Estructurado

Anexo C: Instalación y aplicación de MSAT

3.1. Requisitos mínimos del sistema

- 4.2 MB
- Sistemas compatibles: Windows 2000 Professional Edition; Windows Vista; Windows XP Professional Edition SP2; Windows 7; Windows Server 2003 Service Pack 2; Windows Server 2008; Windows Vista; Windows Vista 64-bit Editions Service Pack 1; Windows Vista Business; Windows Vista Business 64-bit edition; Windows Vista Enterprise; Windows Vista Enterprise 64-bit edition; Windows Vista Home Basic 64-bit edition; Windows Vista Home Premium 64-bit edition; Windows Vista Service Pack 1; Windows Vista Ultimate; Windows Vista Ultimate 64-bit edition; Windows XP Service Pack 2 (Microsoft, 2006).
- NET Framework Versión 3.5
- Internet Explorer 6.0
- SQL Server CE 3.5
- Se debe tener instalado los últimos paquetes de servicio para el sistema operativo y navegador.
- Una vez instalada la herramienta MSAT, no se requiere una conexión a internet, únicamente se necesita conexión para cargar los resultados y comprobar la existencia de actualizaciones.

3.2. Instalación de MSAT

a. Descargar de Microsoft

https://www.microsoft.com/es-es/download/details.aspx?id=12273

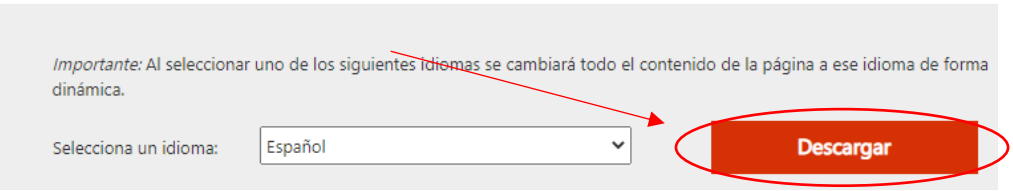


Figura 10. Fuente de descarga de MSAT

b. Descomprimir el archivo .zip y ejecutar el archivo .msi

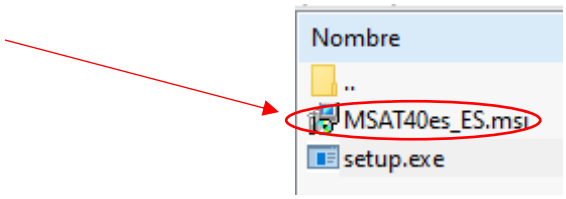


Figura 11. Archivos ejecutables de MSAT

c. Proceder con el asistente de instalación, y dar click, sobre "Siguiente"

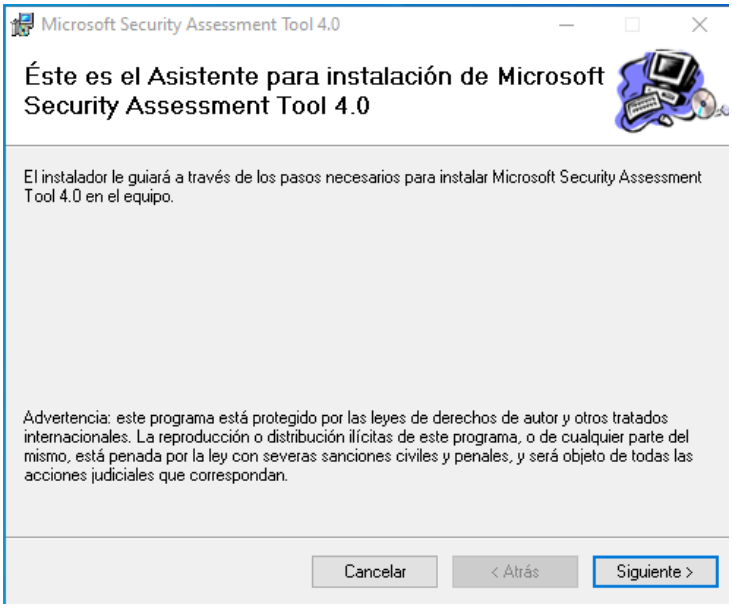


Figura 12. Asistente de instalación 1

d. Aceptar los términos y condiciones, y dar click sobre "Siguiente" hasta culminar la instalación

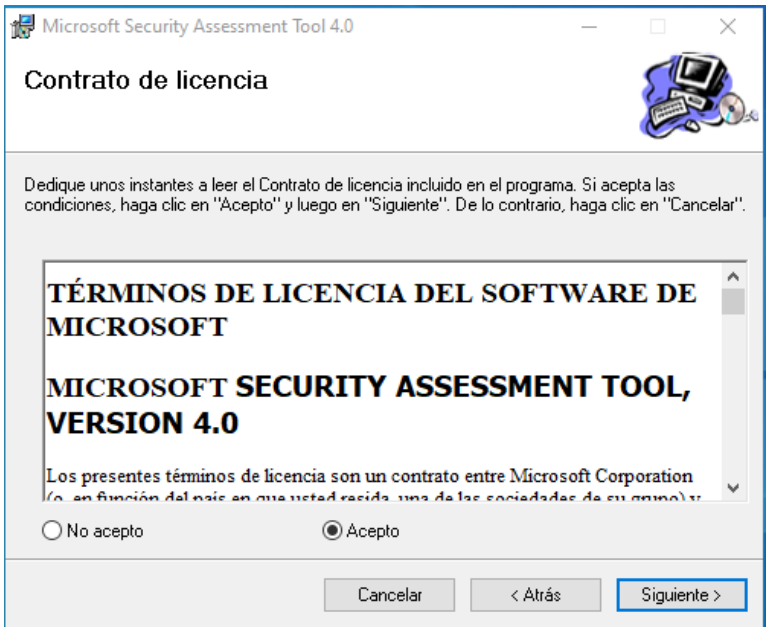


Figura 13. Asistente de instalación 2

e. Finalizar el proceso de instalación, seleccionar “Cerrar”

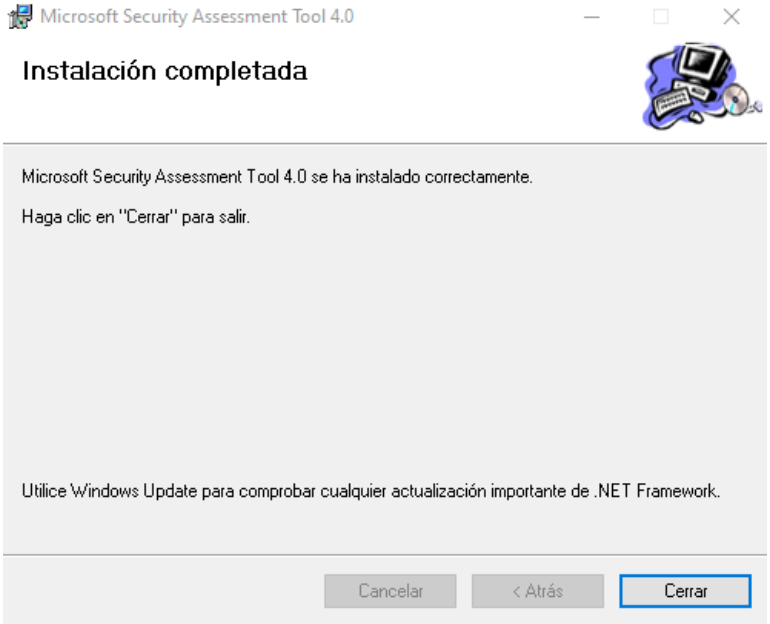


Figura 14. Asistente de instalación 3

f. Abrir MSAT, posteriormente generar un perfil y empezar a utilizar la herramienta.

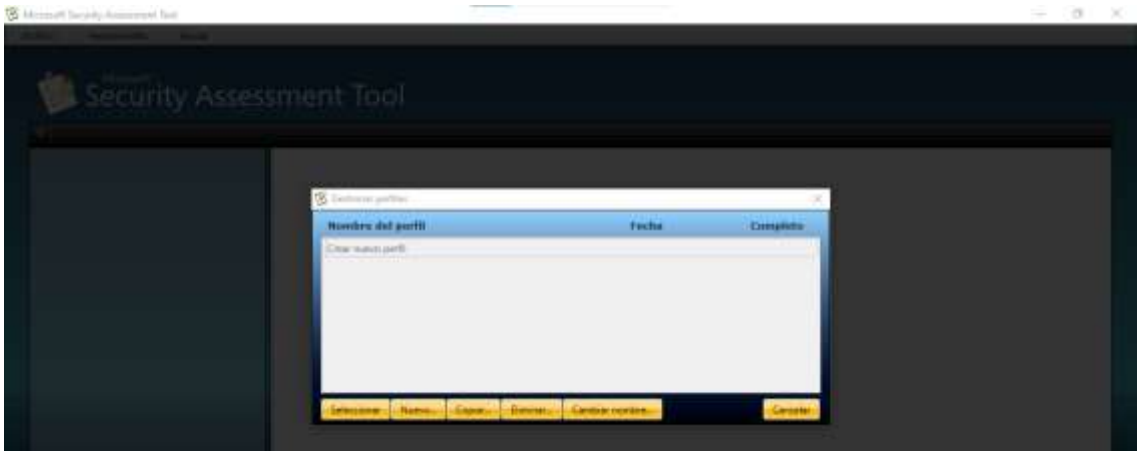


Figura 15. Inicio de MSAT una vez instalado

3.3. Aplicación de MSAT

MSAT está diseñado únicamente para la realización de una evaluación de riesgos, por lo que dispone de dos opciones: creación de perfiles y creación de evaluaciones.

Creación de un Perfil

a. Dar click en la esquina superior izquierda en “Archivo”. Seleccionar “Gestionar perfiles”

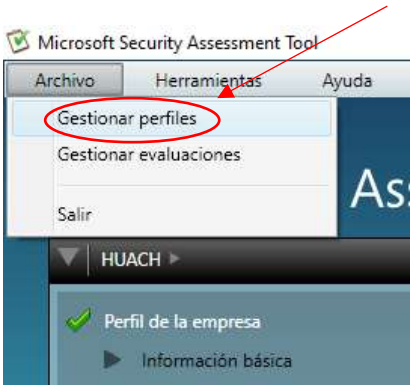


Figura 16. Proceso de Gestión de perfiles

b. Seleccionar “Nuevo”

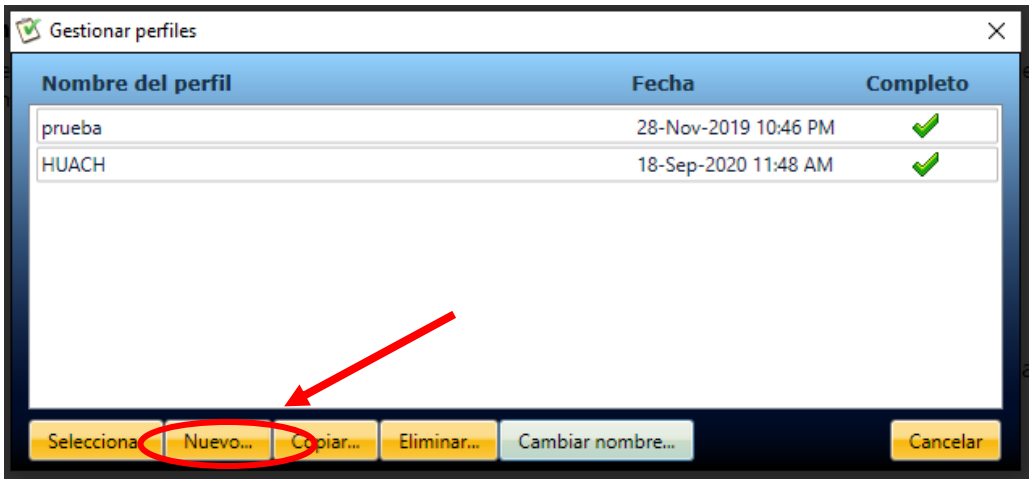


Figura 17. Asistente para la administración de perfiles

Así mismo en esta ventana, se puede editar, copiar, eliminar y seleccionar un perfil.

c. Añadir el nombre de la organización, y dar click en "Aceptar"

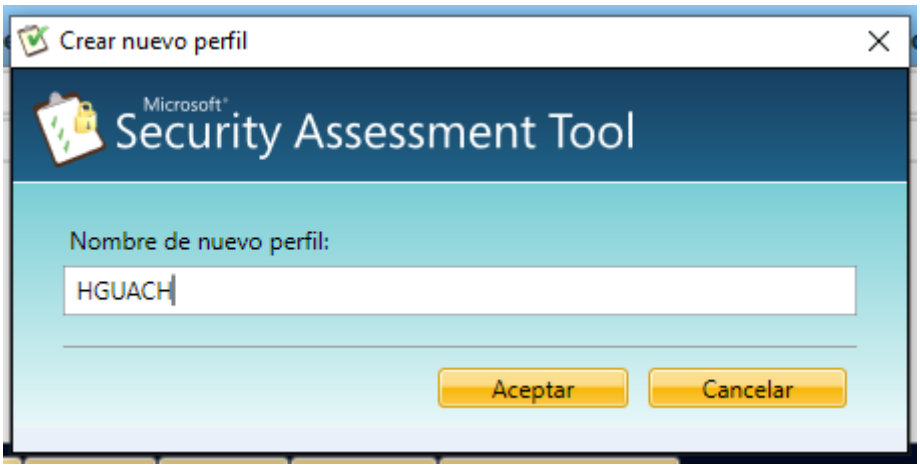


Figura 18. Asignación de nombre al perfil

d. Se procede a la elaboración del perfil de la empresa mediante la introducción de datos de la siguiente manera:

Figura 19. Introducción de datos del perfil creado

Creación de una evaluación sobre un perfil

a. Dar click en “Archivo”. Dar clic en “Gestionar evaluaciones”

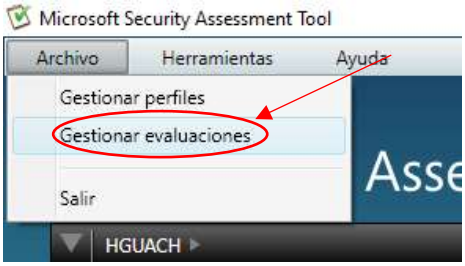


Figura 20. Proceso de Gestión de evaluaciones

b. Seleccionar “Nuevo”

Figura 21. Asistente para la administración de evaluaciones

c. Dar un nombre a la evaluación de la organización que ya se complementó el perfil

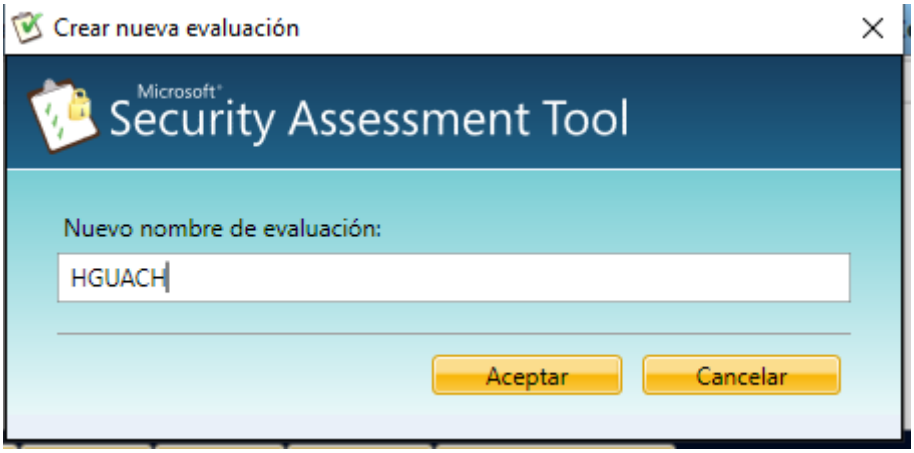


Figura 22. Asignación de nombre a la evaluación.

d. Iniciar con la introducción de datos referente a las áreas de estudio de la herramienta.

Figura 23. Página principal de evaluaciones

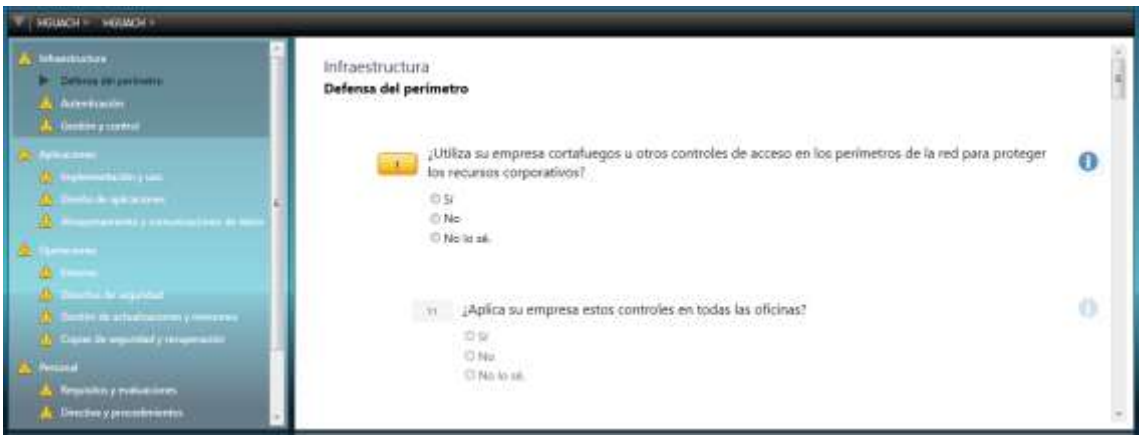


Figura 24. Introducción de datos de la evaluación creada

e. Una vez complementada la información, se procede a la creación de los informes. Dar click en “Informes”

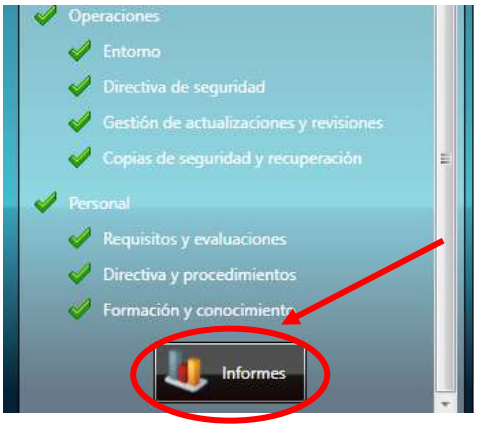


Figura 25. Generador de Informes

Anexo D: Cuestionarios aplicados al personal de TI

4.1. BRP

DIRECCIÓN ACADÉMICA
VICERRECTORADO ACADÉMICO

SGC

UNACH-RGF-01-04-02.10

CUESTIONARIO PARA LA EVALUACIÓN DE RIESGOS EN EL AMBIENTE INFORMÁTICO DEL HOSPITAL GENERAL UNIVERSITARIO ANDINO DE CHIMBORAZO

Fecha: 26/09/2020 - 03/10/2020
Persona entrevistada: Ing. Milton López
Cargo: Encargado de área de TIC's del Hospital General Universitario Andino de Chimborazo
A continuación, se muestran las diferentes preguntas planteadas y respondidas para la evaluación de Riesgo:

PERFIL DE LA EMPRESA

1	Número de equipos de escritorio y portátiles dentro del Hospital Universitario Andino de Chimborazo (HUACH).	Menos de 50 **Entre 50 y 149** Entre 150 y 299 Entre 300 y 399 Entre 400 y 500 Más de 500
2	Número de servidores que se utilizan en el Hospital Universitario Andino de Chimborazo	0 servidores **Entre 1 y 5** Entre 6 y 10 Entre 11 y 25 Más de 25 servidores
SEGURIDAD DE LA INFRAESTRUCTURA		
1	¿Tiene su empresa una conexión permanente a Internet?	**Si** No No lo sé.
2	¿Acceden los clientes y fabricantes a su red o sistemas internos a través de Internet?	Si **No** No lo sé.
3	¿Alberga el HUACH algunos servicios de aplicaciones externas, como por ejemplo, un portal o un sitio Web, para sus socios o clientes externos?	**Si** No No lo sé.
4	¿Dispone el HUACH de servicios que usen los clientes internos y externos en el mismo segmento de red?	**Si** No No lo sé.
5	¿Se conectan directamente los socios o clientes externos a los sistemas internos de la aplicación para acceder a los datos, actualizar los registros o gestionar de cualquier otra forma la información?	**Si** No No lo sé.
6	¿Se utilizan los mismos componentes de infraestructura de aplicación, como por ejemplo, bases de datos en apoyo de las aplicaciones externas y los servicios corporativos internos?	**Si** No No lo sé.
7	¿Permite el HUACH que los empleados o los contratistas accedan remotamente a la red corporativa interna?	**Si** No No lo sé.
8	¿Se permiten que los empleados puedan utilizar sistemas que no sean de producción en la red corporativa general, como por ejemplo, servidores Web personales o equipos que actúen como host de "proyectos personales"?	Si **No** No lo sé.
9	Aparte de los dispositivos de cinta y de copia de seguridad, ¿permite el HUACH procesar la información confidencial o de propiedad fuera de las instalaciones?	Si **No** No lo sé.
10	En el caso de que los sistemas de seguridad se vieran comprometidos, ¿afectaría ello significativamente la capacidad comercial del HUACH?	**Si** No No lo sé.
11	¿Comparte su empresa espacio de oficinas con otras entidades?	**Si** No No lo sé.
SEGURIDAD DE LAS APLICACIONES		
12	¿Se desarrollan aplicaciones en el HUACH?	Si **No** No lo sé.

Campus Norte | Av. Antonio José de Sucre, Km 1 ½ vía a Guano | Teléfonos: (593-3) 3730880 - Ext. 1056 - 1212

13	¿Permite el HUACH que los desarrolladores de software se conecten de forma remota a los recursos de desarrollo corporativo o que se desarrollen remotamente código para aplicaciones?	Si **No** No lo sé.
14	¿Desarrolla o pone en venta el HUACH algunos productos de software para el uso de clientes, socios o mercado en general?	Si **No** No lo sé.
15	¿Se permite que los desarrolladores prueben o desarrollen los sistemas en sitios remotos o inseguros?	Si **No** No lo sé.
16	¿Actúa el personal de TI como guardianes (en contraposición a los desarrolladores) de la línea de aplicaciones comerciales?	Si **No** No lo sé.
17	Según los procedimientos de su empresa, ¿es necesario la actuación de un tercero para almacenar, procesar o distribuir los datos?	**Si** No No lo sé.
18	¿Se almacenan o procesan los datos del cliente en un entorno compartido con los recursos corporativos?	Si **No** No lo sé.
19	¿Recurre a fabricantes independientes de software para complementar la oferta de servicios del HUACH?	**Si** No No lo sé.
20	¿Obtiene el HUACH ingresos por ofrecer servicios que incluyen el procesamiento o la minería de datos?	Si **No** No lo sé.
21	Los datos que procesan las aplicaciones del HUACH, ¿se consideran confidenciales o vitales para las operaciones comerciales de sus clientes?	**Si** No No lo sé.
22	¿Se ofrecen aplicaciones comerciales críticas a través de conexiones a internet?	Si **No** No lo sé.
23	¿Quiénes son los usuarios objetivos de las aplicaciones principales de su entorno?	**Empleados internos** Clientes, fabricantes y socios externos Empleados internos y clientes, fabricantes y socios externos No lo sé.
24	¿Cómo acceden los usuarios a las aplicaciones principales?	Solamente desde la red interna **Tanto desde la red interna como de forma remota** No lo sé
SEGURIDAD DE LAS OPERACIONES		
25	¿Está conectada su red corporativa a otras redes (ya sean de clientes, de socios o de terceros) mediante enlaces de red públicos o privados?	**Si** No No lo sé.
26	¿Obtiene el HUACH ingresos por servicios basados en el almacenamiento o la distribución electrónica de datos, como por ejemplo, archivos de medios o documentación?	Si **No** No lo sé.
27	En los últimos seis meses, ¿se ha sustituido radicalmente algún componente tecnológico de gran importancia?	**Si** No No lo sé.
28	¿La actividad del HUACH depende de la recepción o el procesamiento de datos por parte de socios, fabricantes o terceros?	Si **No** No lo sé.
29	Un incidente que afecte a las aplicaciones o a las infraestructuras orientadas a los clientes, como un apagón o el fallo de la aplicación o hardware, ¿afectaría significativamente a sus ingresos?	**Si** No No lo sé.
30	¿Almacena el HUACH datos confidenciales de sus clientes o de importancia vital?	**Si** No
31	Los componentes de infraestructura y las aplicaciones del cliente, ¿dependen del acceso a recursos de su entorno?	Si **No**
32	¿Comparte el HUACH los componentes de infraestructura y aplicaciones entre varios clientes?	Si **No**
SEGURIDAD DEL PERSONAL		
33	¿Considera que los recursos de TI son un requisito para su empresa?	**Si** No No lo sé.

34	¿Utilizan todos los empleados de su empresa equipos informáticos para desarrollar su trabajo?	Si **No** No lo sé.
35	¿Subcontrata el HUACH el mantenimiento o la propiedad de alguna parte de su infraestructura?	**Si** No No lo sé.
36	¿Tiene el HUACH algún plan a medio o largo plazo para la selección y utilización de componentes de nuevas tecnologías?	Si **No**
37	¿Cree que su empresa participa en la adopción rápida de las nuevas tecnologías?	Si **No**
38	¿Selecciona e implanta el HUACH nuevas tecnologías basadas en acuerdos de licencias y asociaciones existentes?	Si **No** No lo sé.
39	¿Limita el HUACH las opciones relacionadas con la tecnología a aquellas que conoce actualmente el personal de TI?	**Si** No No lo sé.
40	¿Amplía su empresa su red mediante la adquisición de nuevas empresas con sus entornos correspondientes?	Si **No** No lo sé.
41	¿Permite su empresa que los empleados descarguen a sus estaciones de trabajo datos corporativos o datos confidenciales de los clientes?	**Si** No No lo sé.
42	¿Limita el HUACH el acceso a la información en función de los roles de los usuarios?	**Si** No No lo sé.
43	¿Implanta el HUACH nuevos servicios o aplicaciones antes de evaluar los posibles riesgos para la seguridad?	Si **No** No lo sé.
44	¿Cambia el HUACH periódicamente las credenciales de las cuentas con privilegios?	Si **No** No lo sé.
45	¿Cambia el HUACH las credenciales de las cuentas con privilegios cuando el personal deja de trabajar en la empresa?	Si **No** No lo sé.
ENTORNO		
46	Seleccione la opción que mejor defina el sector profesional del HUACH	Servicios TI Servicios financieros Fabricación (discreto) Servicios jurídicos Publicidad Venta **Otro**
47	Selecciones el número de empleados de su empresa:	> 10 Entre 10 y 49 **Entre 50 y 149** Entre 150 y 299 Entre 300 y 399 Entre 400 y 500 Más de 500
48	¿El HUACH tiene más de una oficina?	**Si** No
49	¿La actividad del HUACH se desarrolla en un mercado de gran competencia o de investigación, en el que el robo de material intelectual o el espionaje son temas de gran preocupación?	Si **No**
50	¿Cambia muy a menudo el personal técnico de su empresa	Si **No**
51	¿Los productos o las marcas del HUACH tienen reconocimiento?	Si **No**
52	¿Utiliza el HUACH versiones obsoletas de software que ya no cuenten con el servicio técnico del fabricante	**Si** No
53	¿Adquiere su empresa el software de fabricante o proveedores conocidos y fiables?	**Si** No

Ing. Milton López

Figura 26. Cuestionario de BRP

4.2. Infraestructura

Fecha: 10/10/2020
Persona entrevistada: Ing. Milton López
Cargo: Encargado de área de TIC`s del Hospital General Universitario Andino de Chimborazo
A continuación, se muestran las diferentes preguntas planteadas y respondidas para la evaluación de Riesgo:

INFRAESTRUCTURA

Este apartado se centra en cómo debe funcionar la red, los procesos comerciales (internos o externos) que debe favorecer, cómo se construyen y utilizan los host, y la gestión y el mantenimiento efectivos de la red. Al diseñar una infraestructura que todos puedan comprender y seguir, la empresa podrá identificar las áreas de riesgo e idear métodos para acabar con las amenazas.		
DEFENSA DEL PERÍMETRO		**OPCIONES**
1	¿Utiliza el HUACH cortafuegos u otros controles de acceso en los perímetros de la red para proteger los recursos corporativos	**Si** No No lo sé.
1.1	¿Aplica su empresa estos controles en todas las oficinas?	Si **No** No lo sé.
1.2	¿Utiliza el HUACH una zona neutral (normalmente conocida como 'zona desmilitarizada' o DMZ) para separar las redes internas y externas de los servicios albergados?	Si **No** No lo sé.
2	¿Alberga el HUACH servicios relacionados con Internet en la red corporativa?	**Si** No No lo sé.
3	¿Utiliza el HUACH software de cortafuegos basado en host para proteger los servidores?	Si **No** No lo sé.
4	¿Utiliza el HUACH hardware o software de detección de intrusiones para identificar los ataques a la seguridad?	Si No **No lo sé.**
4.1	Seleccione los tipos de sistemas de detección de intrusiones (IDS) UTILIZADOS	IDS basado en red (NIDS) IDS basado en host (HIDS)
5	¿Se utilizan soluciones antivirus en el entorno?	**Si** No No lo sé.
5.1	Seleccione los sistemas que utilizan soluciones antivirus:	Servidores de correo electrónico Host del perímetro (pasarelas, proxies, relés, etc.) **Equipos de escritorio** Servidores
6	¿Se puede acceder a la red de la empresa de forma remota?	**Si** No No lo sé.
6.1	Seleccione quién se puede conectar a la red de forma remota:	**Empleados** Contratistas **Terceros, como fabricantes, socios o clientes**
6.1.1	¿Se utiliza la tecnología de red privada virtual (VPN) para la conectividad segura a los recursos corporativos de los usuarios remotos?	Si **No**
6.1.1.1	¿Puede la VPN limitar la conectividad a una red aislada en cuarentena hasta que el cliente haya superado todas las comprobaciones de seguridad necesarias?	Si No No lo sé.
6.2	¿Se utiliza autenticación multifactor (token o tarjeta inteligente, etc.) para los usuarios remotos?	Si **No** No lo sé.
7	¿Tiene la red más de un segmento?	Si **No** No lo sé.
7.1	¿Se segmenta la red para separar los servicios de clientes externos y servicios extranet de los recursos corporativos?	Si No No lo sé.
7.1.1	¿Agrupa su empresa los host en segmentos de redes según los roles o servicios similares ofrecidos?	Si No No lo sé.

7.1.2	¿Agrupa su empresa los host en segmentos de redes para ofrecer únicamente los servicios necesarios a los usuarios que se conectan?	Si No No lo sé.
7.1.3	¿Se ha creado y documentado a un plan para regular la asignación de direcciónes TCP/IP a los sistemas según los segmentos necesarios?	Si No No lo sé.
8	¿Dispone la red de opciones de conexión inalámbrica?	**Si** No No lo sé.
8.1	¿Cuáles de los siguientes controles de seguridad se usan para regular las conexiones a las redes inalámbricas?	**Cambio de nombre de red predeterminado/predefinido (conocido también como Identificador del conjunto de servicio o SSID) del punto de acceso** Desactivar la difusión del SSID Activar Privacidad equivalente al cable (WEP) **Activar Acceso protegido de fidelidad inalámbrica (WPA)** Activar restricciones de dirección por hardware (también conocido como Control de acceso al medio, o MAC) Conectar el punto de acceso a la red fuera del cortafuegos o en un segmento separado de la red de cable.
AUTENTICACIÓN		
9	¿Existen controles para hacer cumplir las directivas de contraseñas en todas las cuentas?	Si **No** No lo sé.
9.1	Seleccione las cuentas para las que existen controles que hagan cumplir las directivas de contraseñas	Administrador Usuario Acceso remoto
9.1.1	Indique cuál es la opción de autenticación para el acceso administrativo que gestiona los dispositivos y host:	Autenticación multifactor Ninguno Contraseña sencilla Contraseña Compleja
9.1.2	Indique cuál es la opción de autenticación para el acceso a la red y host internos de los usuarios internos	Autenticación multifactor Ninguno Contraseña sencilla Contraseña Compleja
9.1.2	Indique cuál es la opción de autenticación para el acceso remoto de los usuarios:	Autenticación multifactor Ninguno Contraseña sencilla Contraseña Compleja
9.2	¿Está activado el bloqueo de cuenta para impedir el acceso a las cuentas tras una serie de intentos de registro fallidos?	Si No No lo sé.
10	¿Su organización dispone de procesos para revisar cuentas administrativas inactivas, de uso interno, de proveedor y de usuario remoto?	**Si** No No lo sé.
GESTIÓN Y CONTROL		
11	¿Es el HUACH, el que configura los sistemas o esta tarea la efectúan otros proveedores o revendedores de hardware	Configurado por personal interno **Configurado por un proveedor/distribuidor de hardware**
12	¿Cuáles de los siguientes elementos se han creado basándose en una configuración documentada o en una simulación formal?	Estaciones de trabajo y portátiles Servidores **Ninguno**
12.1	¿Incluye esta configuración procedimientos para 'reforzar el host'?	Si No No lo sé.
13	¿Cuáles de las soluciones siguientes se han instalado en las estaciones de trabajo y los portátiles de los empleados?	**Software de cortafuegos particular** Software de detección y eliminación de Spyware Software de cifrado de discos Software de gestión/control remoto **Protector de pantalla protegido por contraseña** Modém
14	¿La organización cuenta con procedimientos de respuesta ante incidentes formales?	Si **No** No lo sé.

14.1	¿Su organización cuenta con directivas y procedimientos para notificar problemas o incidentes de seguridad?	Si No No lo sé.
15	¿Se han aplicado controles de seguridad físicos para garantizar la seguridad de los activos de la empresa?	**Si** No No lo sé.
15.1	¿Cuáles de los siguientes controles de seguridad se utilizan?	**Sistema de alarma instalado para detectar e informar de intrusiones** **Equipos de red (conmutadores, cableado, conexión a Internet) en habitaciones cerradas con acceso restringido** **Los equipos de red se encuentran además en un armario cerrado** **Los servidores están en una habitación cerrada con acceso restringido** Los servidores se hallan también en armarios cerrados Las estaciones de trabajo se protegen con cables de seguridad Los equipos portátiles se protegen con cables de seguridad **Los materiales impresos confidenciales se almacenan en armarios cerrados.**
15.2	¿Cuáles de los siguientes controles de acceso físico se utilizan?	Tarjetas de identificación para empleados y visitantes **Acompañantes de visitas** Registros de visitas Controles de entrada

Ing. Milton López

Figura 27. Cuestionario de Infraestructura

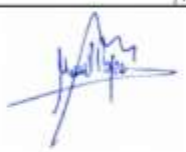
4.3. Aplicaciones

Fecha: 17/10/2020
Persona entrevistada: Ing. Milton López
Cargo: Encargado de área de TIC´s del Hospital General Universitario Andino de Chimborazo
A continuación, se muestran las diferentes preguntas planteadas y respondidas para la evaluación de Riesgo:

APLICACIONES

Este apartado estudia las aplicaciones de su entorno que son esenciales para la empresa y valora desde el punto de vista de la seguridad y disponibilidad. Se examinan las tecnologías utilizadas para aumentar el índice de defensa en profundidad.		
IMPLEMENTACIÓN Y USO		**OPCIONES**
1	¿Dispone el HUACH de una línea de aplicaciones comerciales (LOB)?	Si **No** No lo sé.
2	¿Utiliza marcos personalizados para las aplicaciones de Office (como, por ejemplo, Word Excel o Access)?	Si **No** No lo sé.
3	¿Qué mecanismos tiene el HUACH para asegurar una disponibilidad alta de las aplicaciones? Seleccione los mecanismos utilizados de la lista siguiente:	Equilibrado de carga Clústeres **Pruebas periódicas de la recuperación de aplicaciones y datos** Ninguno
4	¿Ha desarrollado un equipo interno de desarrollo algunas de las aplicaciones principales de su entorno?	Si **No** No lo sé.
4.1	¿Proporciona con regularidad el equipo de desarrollo interno las actualizaciones de software y seguridad, así como la documentación sobre los mecanismos de seguridad?	Si No No lo sé.
5	¿Los consultores/proveedores de terceros han desarrollado alguna aplicación clave implementada en su entorno?	**Si** No No lo sé.
5.1	¿El consultor/proveedor de terceros proporciona actualizaciones de software, revisiones de seguridad y documentación sobre mecanismos de seguridad? (sigue siendo compatible)	**Diseño** **Desarrollo del código** Prueba / Control de calidad Revisión final
5.2	¿Proporcionan con regularidad los fabricantes independientes las actualizaciones de software y seguridad, así como la documentación sobre los mecanismos de seguridad? (todavía se admite)	Si **No** No lo sé.
6	¿Qué metodologías de desarrollo de seguridad de software se practican en su empresa? (Seleccione todas las respuestas que correspondan)	CLASP Cigital - Touchpoints Microsoft Security Development Lifecycle TSP(SM) para desarrollo de sistemas seguros Otras **Ninguna**
7	¿Conoce el HUACH las vulnerabilidades de seguridad que existen actualmente en las aplicaciones de su entorno?	**Si** No
7.1	¿Tiene el HUACH procedimientos para abordar dichas vulnerabilidades de seguridad?	Si **No**
8	¿El HUACH proporciona formación sobre seguridad para el personal de desarrollo y pruebas?	Si **No** No lo sé
8.1	¿Qué porcentaje del personal de desarrollo y de pruebas de la empresa tiene formación en prácticas de desarrollo de seguridad?	100% 75% 50% 25% 10% Ninguna
8.2	¿El HUACH actualiza la formación sobre desarrollo de seguridad propiciada al personal de desarrollo anualmente?	Si, obligatorio Si, opcional No
9	¿El HUACH confía en herramientas de software como parte del proceso de prueba y auditoría para el desarrollo de software seguro?	Si, para todos los proyectos Si, para algunos proyectos **No**
DISEÑO DE APLICACIONES		
10	¿Existen controles para hacer cumplir las directivas de contraseñas de las aplicaciones principales?	Si **No** No lo sé.

10.1	Seleccione los controles de contraseña implantados en las aplicaciones principales:	Contraseñas complejas Caducidad de las contraseñas Bloqueo de cuenta
10.2	En la siguiente lista, seleccione el método de autenticación más común de las aplicaciones principales:	Autenticación multifactor Ninguno Contraseña sencilla Contraseña compleja
11	¿Tienen las aplicaciones principales del entorno mecanismos para limitar el acceso a los datos y las funciones confidenciales?	Si No No lo sé
12	¿Guardan las aplicaciones principales del entorno mensajes en archivo de registro para su análisis y auditoría?	Si No No lo sé.
12.1	Seleccione los tipos de eventos que se registran:	Intentos de autenticación fallidos Autenticaciones correctas Errores de la aplicación Acceso a recursos denegado Acceso a recursos permitido Cambios en los datos Cambios en las cuentas de usuario
13	¿Las aplicaciones utilizadas validan los datos de entrada?	Si No No lo sé.
13.1	Seleccione los tipos de entrada que validan las aplicaciones	Usuarios finales Aplicaciones de cliente Feed de datos
ALMACENAMIENTO Y COMUNICACIONES DE DATOS		
14	¿Cifran las aplicaciones principales los datos confidenciales y críticos de la empresa que se encargan de procesar?	Si No No lo sé.
14.1	Seleccione las diferentes etapas en que se cifran los datos:	Transmisión y almacenamiento Transmisión Almacenamiento
14.2	¿Cuáles de los siguientes algoritmos de cifrado se utilizan?	Estándar de cifrado de datos (DES) DES triple (3DES) RC2, RC4, o RC5 Estándar de cifrado avanzado (AES4)/Rijndael MD5 Hash SHA-1 Hash Twofish Blowfish Algoritmo propio No lo sé



Ing. Milton López

Figura 28. Cuestionario de Aplicaciones

4.4. Operaciones

DIRECCIÓN ACADÉMICA
VICERRECTORADO ACADÉMICO

SGC

UNACH-RGF-01-04-02.10

Fecha: 24/10/2020
Persona entrevistada: Ing. Milton López
Cargo: Encargado de área de TIC´s del Hospital General Universitario Andino de Chimborazo
A continuación, se muestran las diferentes preguntas planteadas y respondidas para la evaluación de Riesgo:

OPERACIONES

ESTE APARTADO VALORA LAS PRÁCTICAS DE FUNCIONAMIENTO Y LAS NORMAS QUE SIGUE LA EMPRESA PARA AUMENTAR LAS ESTRATEGIAS DE DEFENSA EN PROFUNDIDAD A FIN DE EMPLEAR MÁS QUE MERAS DEFENSAS TECNOLÓGICAS. ESTUDIA LAS ÁREAS RELACIONADAS CON LA CREACIÓN DE SISTEMAS, LA DOCUMENTACIÓN DE LA RED, LAS COPIAS DE SEGURIDAD Y LA RESTAURACIÓN DE LOS DATOS EN EL ENTORNO.		
ENTORNO		**OPCIONES**
1	¿Es el HUACH el que gestiona el entorno o se contrata los servicios de un tercero?	La empresa gestiona el entorno **La empresa subcontrata la gestión**
1.1	¿Tiene la empresa acuerdos de servicios establecidos como parte de los contratos con los proveedores de servicios subcontratados?	**Sí** No
1.1.1	¿Se han incluido cláusulas específicas sobre seguridad en los acuerdos de servicios (SLA)?	Sí **No**
2	¿Utiliza la empresa hosts de gestión dedicados a la administración segura de los sistemas y dispositivos del entorno?	Sí **No** No lo sé
2.1	Seleccione los sistemas para los que existen host de gestión dedicados:	Dispositivos de red **Servidores**
3	¿Se utilizan cuentas de registro individuales para las actividades normales en contraposición con las actividades administrativas o de gestión?	**Sí** No No lo sé
4	¿Garantiza la empresa a los usuarios el acceso administrativo a sus estaciones de trabajo y equipos portátiles?	**Sí** No No lo sé
5	¿Se comprueba periódicamente el cortafuegos para garantizar que funciona según lo previsto?	**Sí** No No lo sé
6	¿El HUACH mantiene planes de recuperación ante desastres y de reanudación de negocio?	Sí **No** No lo sé
6.1	¿Se prueban estos planes de forma periódica?	Sí No No lo sé
DIRECTIVA DE SEGURIDAD		
7	¿Existe un modelo para asignar niveles de importancia a los componentes del entorno informático?	**Si** No No lo sé.
8	¿Existen directivas para la regulación del entorno informático?	**Si** No No lo sé.
8.1	¿Existe una directiva de seguridad de información para la regulación de la actividad relacionada con la seguridad en la empresa?	**Si** No No lo sé.
8.1.1	Indique quién desarrolló la directiva:	**Sólo el departamento de TI** Sólo el departamento de representantes comerciales El departamento de TI y de representantes comerciales en conjunto
8.2	¿Hay una directiva corporativa para el uso aceptable?	**Si** No No lo sé.
8.3	¿Hay directivas para la gestión de las cuentas de usuarios individuales?	**Si** No No lo sé.
8.3.1	Seleccione cuáles de las siguientes directivas se aplican a la gestión de las cuentas de usuarios individuales:	**Cuentas de usuarios individuales (no compartidas)** **Cuentas sin y con privilegios para dministradores** Hacer cumplir la calidad de las contraseñas **Cuando un empleado deja su trabajo, se desactivan sus cuentas**
9	¿Hay un proceso documentado para la creación de host?, Si la respuesta es afirmativa, ¿de qué tipo? (¿Para qué tipos de hosts hay un proceso de creación documentado?)	Dispositivos de infraestructura Servidores **Estaciones de trabajo y portátiles** Ninguno

10	¿Hay pautas documentadas que indiquen qué protocolos y servicios están permitidos en la red corporativa? Seleccione la opción adecuada:	Existen directivas y están documentadas **Existen directivas pero no están documentadas** No hay directivas
11	¿El HUACH dispone de un proceso formal bien documentado para la eliminación de datos en medios electrónicos y en formato impreso?	Si **No** No lo sé.
12	¿Su organización dispone de un esquema de clasificación de datos con directrices de protección de datos asociadas?	**Si** No No lo sé.
GESTIÓN DE ACTUALIZACIONES Y REVISIONES		
13	¿Hay un proceso de gestión para las configuraciones y los cambios?	**Si** No No lo sé.
13.1	¿Dispone la empresa de configuraciones documentadas a modo de referencia?	Si **No** No lo sé.
13.2	¿Prueba la empresa los cambios de configuración antes de aplicarlos a los sistemas de producción?	**Si** No No lo sé.
13.2.1	¿Se comprueba y se garantiza de forma centralizada la compatibilidad con las configuraciones (por ejemplo, mediante directivas de grupos de Active Directory)?	Si **No** No lo sé.
14	¿Existe un proceso establecido para las directivas de actualización y revisión?	**Si** No No lo sé.
14.1	Seleccione los componentes para los que existan estos procesos:	Sistemas operativos Aplicaciones **Tanto los sistemas operativos como las aplicaciones**
14.2	¿Prueba el HUACH las actualizaciones y revisiones antes de aplicarlas?	Si **No** No lo sé.
14.3	Indique cuáles de los siguientes elementos se utilizan para aplicar y gestionar las actualizaciones	**Actualización automática de Windows** Sitio Web de Windows Update Servicios de actualización de Windows Server (WSUS) Servidor para la gestión de sistemas (SMS) Otras soluciones de gestión de actualizaciones System Center Configuration Manager (SCCM)
14.3.1	¿En qué tipos de host se utiliza la gestión automática de actualizaciones?	**Estaciones de trabajo y portátiles** Servidores
15	¿Existe una directiva establecida por la que se regula la actualización de productos de detección basados en firmas?	**Antivirus** Sistema de detección de intrusiones (IDS) Ninguno
16	¿Hay diagramas lógicos y documentación de configuración precisa para la infraestructura de red y los host?	Si No No lo sé **Hay diagramas, pero han caducado**
17	¿Existen diagramas exactos de la arquitectura y del flujo de datos de las aplicaciones principales?	Si **No** No lo sé
17.1	Seleccione los tipos de aplicaciones de las que existen diagramas:	Sólo aplicaciones externas Sólo aplicaciones internas Tanto las aplicaciones internas como externas
COPIAS DE GESTIÓN Y RECUPERACIÓN		
18	¿Está activado en el entorno el registro de los eventos producidos en los host y los dispositivos?	Si No **No lo sé.**
18.1	¿Toma medidas la empresa para proteger la información incluida en los registros?	El sistema operativo y las aplicaciones están configuradas para no sobrescribir eventos. Los archivos de registro se rotan con frecuencia para asegurarse de que hay suficiente espacio disponible El acceso a los archivos de registro está restringido a las cuentas de tipo administrador Los registros se almacenan en un servidor central de registros

18.2	¿Revisa la empresa periódicamente los archivos de registro?	Si No No lo sé.
18.2.1	¿Con qué frecuencia se revisan los registros?	Diariamente Semanalmente Mensualmente Según sea necesario No lo sé
19	¿Se hacen copias de seguridad de todos los recursos críticos y confidenciales periódicamente?	**Si** No No lo sé.
19.1	¿Existen directivas y procedimientos para el almacenamiento y la gestión de los dispositivos de copias de seguridad?	**Si** No
19.1.1	¿Cuáles de las directivas y procedimientos siguientes se cumplen?	**Almacenamiento fuera de las instalaciones** Almacenamiento en armarios cerrados, a prueba de fuego. Acceso limitado a dispositivos de copias de seguridad. Rotación y duración de los dispositivos de copias de seguridad.
19.2	¿Existen directivas para la comprobación periódica de los procedimientos de copias de seguridad y restauración? Estas directivas, ¿están documentadas?	Si, y están documentados **Si, pero no están documentados** No No lo sé.

Ing. Milton López

Figura 29. Cuestionario de Operaciones

4.5. Personal

DIRECCIÓN ACADÉMICA
VICERRECTORADO ACADÉMICO

SGC

UNACH-RGF-01-04-02.10

Fecha: 28/10/2020
Persona entrevistada: Ing. Milton López
Cargo: Encargado de área de TIC's del Hospital General Universitario Andino de Chimborazo
A continuación, se muestran las diferentes preguntas planteadas y respondidas para la evaluación de Riesgo:

PERSONAL

Este apartado revisa los procesos de la empresa que regulan las directivas de seguridad corporativa, los procesos de recursos humanos, así como la formación y el grado de conocimiento de los empleados sobre la seguridad. También se centra en la seguridad en las operaciones diarias. Este apartado le ayuda a valorar como se mitigan los riesgos del área de personal.		
REQUISITOS Y EVALUACIONES		**OPCIONES**
1	¿Hay en su empresa individuos o grupos que sean responsables de la seguridad?	Si No No lo sé.
1.1	¿Tienen estos individuos o grupos experiencia en el tema de la seguridad?	Si No No lo sé.
1.2	¿Estos individuos o grupos se ocupan de establecer los requisitos de seguridad de las tecnologías nuevas y existentes?	Si No No lo sé.
1.3	¿En qué etapa del ciclo de vida de la tecnología suele participar este equipo o individuo encargado de la seguridad?	Planificación y diseño Implantación Pruebas Utilización
1.4	¿Existen responsables y roles definidos para cada individuo que participa en la seguridad de la información?	Si No No lo sé.
2	¿Realiza su empresa evaluaciones de la seguridad del entorno a través de terceros?	Si No No lo sé.
2.1	¿Con qué frecuencia se llevan a cabo estas evaluaciones?	Trimestralmente Semestralmente Anualmente Cada dos años o menos
2.2	Seleccione las áreas de análisis que comprenden estas evaluaciones	Infraestructura Aplicaciones Directiva Auditoría
3	¿Realiza su empresa evaluaciones de la seguridad del entorno de forma interna?	Si No No lo sé.
3.1	¿Con qué frecuencia se llevan a cabo estas evaluaciones?	Trimestralmente Semestralmente Anualmente Cada dos años o menos
3.2	Seleccione las áreas de análisis que comprenden estas evaluaciones	Infraestructura Aplicaciones Directiva Auditoría
DIRECTIVA Y PROCEDIMIENTOS		
4	¿Realiza la empresa comprobaciones del historial personal como parte del proceso de contratación?	Si No No lo sé.
4.1	Seleccione la opción más adecuada	Se hacen comprobaciones del historial personal de cada aspirante Se hacen comprobaciones del historial personal sólo de aspirantes a puestos críticos o confidenciales
5	¿Hay un proceso formal para la salida de la empresa de los empleados?	Si No No lo sé.
5.1	Seleccione las opciones para las que exista un proceso formal para la salida de la empresa de los empleados:	Salidas hostiles Salidas amatosas
6	¿Hay una directiva formal para las relaciones con terceros?	Si No No lo sé.

FORMACIÓN Y CONOCIMIENTO		
7	¿Hay un programa de divulgaciones de las medidas de seguridad en su empresa?	Si No No lo sé.
7.1	¿Cuál es el porcentaje de empleados que han participado en el programa de divulgación de las medidas de seguridad?	Menos del 25% Del 25 al 49% Del 50 al 75% Más del 75%
7.2	¿Cuáles de los siguientes temas se incluyen en los cursos de formación sobre la seguridad?	Directivas y controles de seguridad de la empresa Informes sobre actividades sospechosas Confidencialidad Seguridad del correo electrónico, incluyendo Spam y gestión de adjuntos. Seguridad de Internet, incluyendo navegación por la Web y descargas Seguridad informática, incluyendo el uso cortafuegos particulares y cifrado.
7.3	¿Con qué frecuencia se realizan estos cursos?	Trimestralmente Semestralmente Anualmente Cada dos años o menos
8	¿Se ofrece a los empleados formación relacionada con el cargo que desempeñan en la empresa?	Si No No lo sé.
8.1	Seleccione las opciones que correspondan en la siguiente lista:	Seguridad de las operaciones Seguridad de la infraestructura Seguridad de las aplicaciones Preparación para incidentes y reacción

Ing. Milton López

Figura 30. Cuestionario de Personal

Anexo E: Guía de actividades prioritarias

Guía de actividades prioritarias para soluciones de seguridad en el “Hospital General Universitario Andino de Chimborazo”

Universidad Nacional de Chimborazo

Realizado por: Gabriela Ortega Siguencia

Riobamba – Ecuador

2020

Índice

1. Introducción

El crecimiento constante de las tecnologías de la información y comunicación alrededor de todo el mundo, es algo indiscutible. Ahora bien, esto se ha convirtiendo en una gran ventaja y, a su vez, una desventaja. Por un lado, las TIC, han ayudado al desarrollo y crecimiento de la sociedad, y lamentablemente, por otro lado, estas se han visto como objeto de ataques, con fines ajenos a los objetivos de las organizaciones. Realmente no existe un sistema 100% seguro, ni ninguna empresa tiene tampoco 0% de riesgo, pero existen una serie de medidas o controles que ayudan a gestionar estos riesgos, para mitigar la probabilidad que ocurra un ataque.

Para proceder a la creación de estos controles o medidas es importante haber realizado previamente un análisis de la situación actual en la empresa en la que se quiere aplicar estas medidas, en este caso: el Hospital General Universitario Andino de Chimborazo (HGUACH). Tras la evaluación de riesgos realizada en el proyecto "Evaluación de Riesgos en el ambiente informático del Hospital General Universitario Andino de Chimborazo con la herramienta MSAT", se procedió a la elaboración de esta "Guía de actividades prioritarias para soluciones de seguridad en el Hospital General Universitario Andino de Chimborazo"

La presente guía tiene como finalidad, presentar el resultado de las actividades prioritarias a tomar en cuenta, para mejorar la seguridad en el HGUACH, siendo así, el resultado de la realización de una Evaluación de Riesgos realizada con la herramienta MSAT.

Esta guía ha sido construida bajo la referencia de los proyectos "Guía de controles de ciberseguridad para la protección integral de la PYME" (Olivan, 2017) y el proyecto "Propuesta de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynet Virtuales" (Palmay, 2017). También se han tomado en cuenta ciertos parámetros de la norma ISO/IEC 27001.2005, donde se propone la utilización del modelo de W. Edward Deming (Planificar-Hacer-Verificar-Actuar) (Guevara, 2014). Dicho modelo es para la implementación de un modelo de Gestión de

la Seguridad de la Información. Cabe mencionar que esta guía tiene un alcance limitado al tratarse del resultado de una evaluación de riesgos, se han tomado en consideración las dos primeras etapas del modelo anteriormente nombrado para su creación.

2. Objetivo de la guía

El objetivo principal de esta guía es dar a conocer al personal de TI, una serie de actividades prioritarias para el mejoramiento de la seguridad en el ámbito informático del HGUACH. Por otro lado, este documento puede servir como soporte para la adquisición de nuevos productos y/o servicios de seguridad y en fomentar una cultura de seguridad dentro del entorno organizacional del HGUACH.

3. Alcance de la guía

La presente guía de actividades prioritarias para soluciones de seguridad está creada a partir de un análisis de riesgos realizada por el autor mediante la herramienta MSAT que abarca los aspectos de infraestructura, operaciones, aplicaciones y personal. El alcance de esta investigación se enfoca en dar a conocer las actividades prioritarias recomendadas para mitigar los riesgos y mejorar la seguridad del HGUACH.

4. Usuarios a los que va dirigida la guía

La guía es de utilidad únicamente para el personal del departamento de tecnologías de la información, que cuente con un conocimiento de tipo medio-avanzado.

También cabe mencionar, que la guía no es aplicable a otras organizaciones que no sean el HGUACH, por lo que se trata del resultado de un estudio realizado únicamente a esta organización.

5. Normativas, guías y estándares

La normativa aplicada para la enumeración de las actividades prioritarias es la utilizada por la herramienta con la que se llevó a cabo la evaluación de riesgos (MSAT).

5.1 NIST-800.x (Instituto Nacional de Estándares y Tecnología)

NIST es un Instituto creado para promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que

mejoren la estabilidad económica y la calidad de vida (Carvajal , 2015). La normativa NIST 800, hace su enfoque en dar métodos viables y rentables, mediante la descripción de políticas, procedimientos y pautas de seguridad informática, siendo su objetivo principal la optimización de la seguridad de los sistemas y redes de TI (Rouse, 2006).

5.2 ISO/IEC 17799

Es una norma internacional que proporciona un marco para el establecimiento de diferentes métodos de evaluación de riesgos; políticas, controles y contramedidas.

La norma ISO/IEC 17799, establece diez dominios, que dan cumplimiento, casi en su totalidad, la Gestión de la Seguridad de la Información, estos dominios comprenden: las Políticas de seguridad, los aspectos organizativos, la clasificación y control de activos, seguridad ligada al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos, desarrollo y mantenimiento de sistemas, gestión de continuidad del negocio, y finalmente, el cumplimiento o conformidad de la legislación. De los diez dominios que muestran la estructura de la norma ISO/IEC 17799, se derivan 36 objetivos de control y 127 controles que comprenden prácticas, procedimientos o mecanismos que reducen el nivel de riesgo (Quintana et al., 2016). En la actualidad se encuentra con el nombre ISO/IEC 27002.

5.3 Trustworthy Computing Group de Microsoft (TwC)

TwC es una iniciativa de Microsoft lanzada en 2002 y anunciada por Bill Gates. El grupo TwC implementa los principios de seguridad y privacidad en los procesos de desarrollo de software y la cultura de la empresa (Microsoft, 2011). Es un grupo centralizado, que tiene como responsabilidad, simplificar la forma en la que se trabaja, aumentar la agilidad, impulsar una mayor rendición de cuentas y crear modelos de soporte que sean más magros y eficientes (Charney, 2014).

La iniciativa TwC, abarca conceptos como: confianza, estabilidad y seguridad en la plataforma (Aislamiento y flexibilidad; calidad; autenticación; autorización y control de accesos; orientación y formación) (UNIR, 2018).

6. Metodología Utilizada

6.1 Metodología para la obtención de las actividades prioritarias recomendadas

Es la utilizada por la herramienta MSAT, que consiste en la creación de un perfil de riesgos para la empresa (BRP) a través de la valoración del riesgo al que se está expuesto de acuerdo al modelo y sector empresarial. Tras el proceso anterior, se procede a la compilación de medidas de seguridad implantados con anterioridad, las cuales forman capas de defensa, cada capa contribuye a una estrategia combinada de defensa en profundidad (DiDI), medición de las defensas de seguridad utilizadas en el personal, procesos y tecnología para mitigar riesgos de una organización. Finalmente se realiza una comparación entre BRP y DiDI, para medir la distribución de riesgos a lo largo de las áreas de análisis (AoAs), dichas áreas son: infraestructura, aplicaciones, operaciones y personal (Microsoft, 2009). Finalmente, tras el proceso realizado anteriormente se elabora la presente guía.

7. Ámbito de aplicación

Las actividades prioritarias recomendadas para la aplicación en el HGUACH, son aplicables a las cuatro áreas que se detallan a continuación:

7.1 Infraestructura

Este componente del entorno del hospital comprende el funcionamiento de la red, los procesos comerciales (internos y externos) que debe favorecer, la construcción y utilización de los hosts, y la gestión y mantenimiento efectivos de la red. Una buena infraestructura, comprensible y que todos puedan seguir, favorece a la identificación de las áreas de riesgo e idealización de diferentes métodos para poner fin a las amenazas que se pudieran dar.

7.2 Aplicaciones

En el componente de aplicaciones se evalúan las tecnologías que se utilizan en el hospital para el aumento del índice de defensa en profundidad (DiDI), desde un punto de vista orientado a la seguridad y disponibilidad.

7.3 Operaciones

Se valoran las prácticas de funcionamiento y las normas que utiliza el hospital para el aumento de las estrategias orientadas a la defensa en profundidad. Analiza las áreas relacionadas con la creación de sistemas, documentación de la red, copias de seguridad y restauración de datos en el ambiente.

7.4 Personal

Este componente verifica los procesos que se hacen cargo de la regulación de las directivas de seguridad a nivel corporativo, procesos de recursos humanos, formación y grado de conocimiento de los empleados en cuestiones de seguridad y operaciones diarias. Obteniendo como resultado una ayuda para la valoración de mitigación de riesgos del área de personal.

8. Guía de actividades prioritarias para Infraestructura

Infraestructura		
Defensa del perímetro	→	Cortafuegos, antivirus, acceso remoto, segmentación
Autenticación	→	Directivas de contraseñas
Gestión y control	→	Host de gestión, archivos de registro
Estación de trabajo	→	Configuración de creación

Defensa del perímetro	
Subcategoría	**Mejores prácticas recomendadas**
Reglas y filtros de cortafuegos	Los firewalls son un mecanismo de primera línea de defensa y se deben colocar en todas las ubicaciones de borde de red. Las reglas implementadas en los firewalls deben ser muy restrictivas y establecerse host a host y servicio a servicio. Al crear reglas de firewall y listas de control de acceso (ACL) de enrutador, céntrese primero en la protección de los dispositivos de control y de la red frente a ataques. El firewall debe estar establecido con una posición de denegación predeterminada, permitiendo únicamente el tráfico necesario. • Aplique el flujo de datos utilizando las ACL de red y las reglas de firewall. • Pruebe las reglas de firewall y ACL de enrutador para determinar si las reglas. • Existentes contribuyen a ataques de denegación de servicio (DoS). • Implemente una o más DMZ como parte de una implementación de firewall. • Sistemática y formal. • Coloque ahí todos los servidores accesibles a través de Internet. Restrinja la conectividad hacia las DMZ y desde ellas.

	Resultados	Actividad
Reglas y filtros de cortafuegos	El resultado muestra que el cortafuegos se comprueba regularmente para asegurar que funciona correctamente.	Continuar realizando pruebas periódicas al cortafuegos. Asegurar que la funcionalidad responde según lo previsto, no únicamente desde el tráfico externo, y compruebe que el cortafuegos también está respondiendo al tráfico interno.
	El resultado muestra que no ha instalado cortafuegos en todas las oficinas.	Poner en práctica inmediatamente cortafuegos u otros controles de acceso de nivel de red en todas las ubicaciones de oficinas, realizar pruebas con frecuencia y verifique que todos los cortafuegos funcionan correctamente.
	Los resultados muestran que, aunque ha dado el primer paso para proteger el perímetro de la red con un cortafuegos, no ha creado ningún segmento DMZ para proteger los recursos corporativos a los que se puede acceder a través de Internet desde los dispositivos internos de la empresa.	Estudiar la utilización de un cortafuegos para separar los recursos accesibles por Internet, como servidores Web, de los recursos internos y corporativos. Poner en práctica reglas que controlen el acceso de entrada y salida. Plantear la utilización de filtros de salida para evitar conexiones innecesarias y limitar el acceso directo a los segmentos DMA por parte de los usuarios internos, ya que no es probable que éstos trabajen con los equipos hosts del DMZ con frecuencia. Limitar el acceso de la red central al segmento DMZ sólo a hosts específicos o a redes administrativas.

	Los resultados muestran que no utiliza software de cortafuegos basados en hosts para proteger los servidores.	Como una capa adicional de defensa, considerar instalar cortafuegos basados en host en todos los servidores y pensar también en emplear este software en todos los equipos de escritorio y portátiles en la empresa.
Subcategoría	**Mejores prácticas recomendadas**	
Antivirus	Implementar soluciones antivirus en todo el entorno en el nivel de servidor y de escritorio. Implementar soluciones antivirus especializadas para tareas específicas, como exploradores de servidores de archivos, herramientas de filtrado de contenido y exploradores de carga y descarga de datos. Configurar soluciones antivirus para buscar virus en el entorno tanto de entrada como de salida. Las soluciones antivirus se deben implementar primero en servidores de archivos críticos y, a continuación, en servidores de correo, bases de datos y web. La solución antivirus se debe incluir en el entorno de generación predeterminado para escritorios y portátiles. Si se hace uso de Microsoft Exchange, utilizar las capacidades de antivirus y filtrado de contenido adicionales en el nivel de buzón.	
	Resultados	**Actividad**
Antivirus – Equipos de escritorio	El resultado muestra que los equipos de escritorio utilizan soluciones antivirus.	Continuar con la práctica. Utilizar una directiva que requiera a los usuarios a actualizar las firmas de virus. Pensar en añadir el cliente antivirus al entorno predeterminado de creación de estaciones de trabajo.
Antivirus – Servidores	El resultado muestra que no se utilizan soluciones antivirus en el nivel de los servidores.	Considerar utilizar una solución antivirus en los servidores de archivos importantes y aplicar posteriormente a los servidores de correo, de bases de datos y de red.
Subcategoría	**Mejores prácticas recomendadas**	

Acceso remoto	Es importante seguir un proceso de creación de informes de incidentes y respuesta documentado para garantizar que todos los problemas e incidentes se revisan y se evalúan de forma coherente. Es importante que todos los usuarios comprendan su responsabilidad de notificar los problemas o incidentes de seguridad y que tengan un proceso definido claramente para notificar estos problemas.

	Resultados	**Actividad**
Acceso remoto	Los resultados muestran que existen empleados y/o socios que se conectan remotamente a la red interna, pero no utiliza ninguna tecnología VPN para permitirles un acceso seguro.	Utilizar VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH. Utilizar conectividad sitio-a-sitio basada en la tecnología IPSec. Configurar listas de acceso a redes y de usuario para limitar el acceso a los recursos corporativos necesarios.

Subcategoría	**Mejores prácticas recomendadas**
Segmentación	Utilizar segmentos para impedir el acceso a extranets específicas por parte de fabricantes, socios o clientes. Cada segmento externo de la red debe permitir que sólo se encamine determinado tráfico hacia los hosts y puertos concretos de aplicaciones que proporcionan servicios a los clientes. Asegurar la existencia de controles de red que permitan sólo el acceso necesario para cada conexión de terceros. Limitar el acceso de los servicios de red suministrados, así como el acceso entre los segmentos de red.

	Resultados	**Actividad**

Segmentación	El resultado muestra que los servicios ofrecidos en Internet se alojan en la red de su empresa.	Asegurar que los cortafuegos, la segmentación y los sistemas de detección de intrusiones permiten proteger la infraestructura de la empresa de los ataques desde Internet.
	Los resultados muestran que la red presenta un sólo segmento.	Utilizar segmentos para separar extranets específicas y el acceso de fabricantes, socios o clientes. Cada segmento externo de la red debe permitir que sólo el tráfico específico sea encaminado a hosts de aplicaciones específicos y a puertos utilizados para prestar servicios a los clientes. Asegurar que existan controles de red que permitan sólo el acceso necesario para cada conexión de terceros. Limitar el acceso a y de los servicios de red suministrados y entre los segmentos de red.
Subcategoría	**Mejores prácticas recomendadas**	
Inalámbrico	Las mejores prácticas para la implantación inalámbrica incluyen la garantía de que la red no hace público su SSID, que se usa el cifrado WPA y que la red no se considera fundamentalmente como de no confianza.	
	Resultados	**Actividad**
Inalámbrico	Los resultados muestran que existe la opción de conexión inalámbrica a su red	Para reducir los riesgos asociados a las redes inalámbricas, la implantación no debe incluir la difusión del SSID, pero sí el cifrado WPA, además de tratar la red como de no confianza.

	El resultado muestra que ha modificado el SSID predeterminado del punto de acceso.	El cambio del SSID predeterminado es el primer paso para asegurar su red inalámbrica. No obstante, es necesario combinarlo con otras prácticas para minimizar el riesgo. Estas prácticas incluyen la no difusión del SSID, el cifrado WPA y tratar la red como de no confianza.
	Los resultados muestran que no ha desactivado la difusión del SSID en el punto de acceso.	Considerar la deshabilitación de la difusión del SSID para dificultar a un usuario ocasional los intentos de conexión a su red inalámbrica.
	Los resultados muestran que no utiliza el cifrado WEP en el entorno inalámbrico.	Si actualmente no se usa ningún cifrado, considerar utilizar WPA para evitar que el tráfico de la red inalámbrica sea "detectado" y leído como texto sin formato.
	Los resultados muestran que utiliza el cifrado WPA en el entorno inalámbrico.	En la actualidad, WPA es el estándar de cifrado más seguro pero aún se puede descodificar. Considerar la utilización de un cifrado adicional (como VPN) para una mayor seguridad.
	Los resultados muestran que no utiliza la restricción por MAC en el entorno inalámbrico.	Considerar el uso de autenticación WPA además de los filtros MAC, con el fin de evitar que ordenadores no autorizados se conecten a la red.
	Los resultados muestran que la red inalámbrica se considera de no confianza.	Considerar migrar su red inalámbrica a un segmento de red de no confianza y exigir el uso de VPN o tecnologías similares para proteger mejor la integridad de los datos.
Autenticación		
Subcategoría	**Mejores prácticas recomendadas**	

Usuarios administrativos	Poner en práctica una directiva de contraseñas complejas para las cuentas administrativas con contraseñas que cumplan estas condiciones: + Alfanumérico + Mayúsculas y minúsculas + Contiene al menos un carácter especial + Contiene como mínimo 14 caracteres Para limitar más los riesgos de ataques a las contraseñas, poner en práctica los controles siguientes: + Caducidad de contraseñas + Bloqueo de la cuenta después de entre 7 y 10 intentos de registro fallidos + Registro del sistema Además de las contraseñas complejas, se puede recurrir a la autenticación multifactor. Utilizar controles avanzados de la gestión de cuentas y del registro de acceso a cuentas (no permita que se compartan cuentas).

	Resultados	**Actividad**
Usuarios administrativos	Los resultados muestran que se utilizan inicios de sesión distintos para la administración de seguridad de los sistemas y de los dispositivos del entorno.	Continuar exigiendo cuentas separadas para las actividades administrativas o de gestión y asegúrese de que las credenciales administrativas se modifican con frecuencia.
	Los resultados muestran que los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo.	Considerar eliminar el acceso administrativo de usuarios, para limitar la posibilidad de modificar la creación segura.

Subcategoría	Mejores prácticas recomendadas
Usuarios internos	Para las cuentas de usuario, Implementar una directiva que requiera el uso de contraseñas complejas que cumplan los siguientes criterios: * Caracteres alfanuméricos * Uso de mayúsculas y minúsculas * Al menos un carácter especial * Longitud mínima de 8 caracteres Para limitar aún más el riesgo de un ataque a contraseñas, implementar los siguientes controles: * Caducidad de contraseña * Bloqueo de cuenta tras al menos 10 intentos de inicio de sesión erróneos * Registro del sistema Además de contraseñas complejas, considere la posibilidad de implementar una autenticación de varias fases. Implemente controles avanzados para la gestión de cuentas (no permita el uso compartido de cuentas) y para el registro de acceso a cuentas.

Subcategoría	Mejores prácticas recomendadas
Usuarios de acceso remoto	Implementar controles de contraseña complejos para todos los usuarios de acceso remoto, si se ha concedido este acceso mediante el uso de tecnologías de acceso telefónico o VPN. Una contraseña se considera compleja si cumple los siguientes criterios: * Caracteres alfanuméricos * Uso de mayúsculas y minúsculas * Al menos un carácter especial * Longitud mínima de 8 caracteres

	Implementar una fase adicional de autenticación para las cuentas a las que se ha concedido acceso remoto. Considerar también la posibilidad de implementar controles avanzados para la gestión de cuentas (no permita el uso compartido de cuentas) y para el registro de acceso a cuentas. En el caso del acceso remoto, resulta especialmente importante proteger el entorno mediante el uso de unas prácticas de gestión de cuentas segura, buenas prácticas de registro y capacidades de detección de incidentes. Para mitigar aún más los riesgos de ataques de fuerza bruta a contraseñas, considere la posibilidad de implementar los siguientes controles: * Caducidad de contraseña * Bloqueo de cuenta tras 7 a 10 intentos de inicio de sesión erróneos * Registro del sistema Los servicios de acceso remoto también deben tener en cuenta los sistemas que se utilizan para obtener acceso a redes o hosts. Considerar también la posibilidad de implementar controles para hosts a los que se les permite acceder a la red de forma remota.

	Resultados	**Actividad**
Usuarios de acceso remoto	Los resultados muestran que los empleados pueden conectarse a la red de forma remota.	Si aún no está hecho, estudiar la utilización de un sistema de autenticación multifactor de acceso remoto y limitar el acceso únicamente a aquellos empleados que tengan una necesidad empresarial de conectividad remota.
	Los resultados muestran que los contratistas no pueden conectarse a la red de forma remota.	Al no permitir el acceso remoto, reduce los riesgos globales. Sin embargo, si el acceso remoto se planea o se utiliza en el futuro, asegurar que lo hace conforme a la mejor práctica recomendada para minimizar así el riesgo asociado con esta forma de acceso.

	Los resultados muestran que terceros usuarios pueden conectarse a la red de forma remota.	Además de permitir el acceso remoto a los empleados según las mejores prácticas recomendadas, considerar limitar el acceso a terceros para que únicamente puedan acceder a los sistemas remotos necesarios. Por otro lado, plantear utilizar un punto de entrada separado para los terceros, con el fin de controlar y limitar su acceso con más facilidad.
Subcategoría	**Mejores prácticas recomendadas**	
Directivas de contraseñas	La utilización de contraseñas complejas es un elemento fundamental del índice de defensa en profundidad. Las contraseñas complejas deben tener de 8 a 14 caracteres e incluir caracteres alfanuméricos y especiales. Debe establecer una longitud mínima, un historial, un límite a la duración y una caducidad para reforzar la defensa. Generalmente, la caducidad de las contraseñas debe configurarse de esta forma: + Duración máxima de 90 días + Las cuentas nuevas deben cambiar la contraseña al inicio de la sesión + Un historial de 8 contraseñas (mínimo de 8 días) Además de las contraseñas complejas, la autenticación multifactor es muy importante, especialmente para las cuentas administrativas y de usuarios remotos. En todas las cuentas de usuario, se debe activar un proceso de bloqueo de cuenta tras 10 intentos de registro fallidos. Los controles para bloquear una cuenta pueden variar; algunos sencillamente se dedican a los ataques de fuerza bruta a las contraseñas y otros requieren que un administrador desbloquee la cuenta. Se considera una práctica aconsejable activar el bloqueo en las cuentas administrativas, al menos en lo que respecta al acceso a la red. De esta forma, la cuenta no se puede bloquear desde fuera de la consola,	

	solamente desde la red. Es posible que esta solución no sea adecuada para todas las empresas, particularmente para aquellas con ubicaciones remotas. En tales casos, lo más adecuado es que un administrador desbloquee la cuenta, de este modo se evita que los ataques pasen desapercibidos durante largo tiempo si no se dispone de otros medios para detectar fallos de autenticación. Cuando se pongan en práctica controles de bloqueo de cuenta, siga las normas siguientes: + Bloqueo después de entre 7 y 10 intentos de registro fallidos para las cuentas administrativas y de acceso remoto + Bloqueo después de 10 intentos de registro fallidos para las cuentas de usuario estándar + Requerir la intervención de un administrador para desbloquear las cuentas de acceso remoto y de administrador, y para reactivar automáticamente las cuentas de usuarios estándar al cabo de 5 minutos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las que se aplican a las cuentas normales. En sistemas Windows, debe establecer contraseñas de 14 caracteres alfanuméricos y especiales para las cuentas administrativas (y las cuentas de servicio).

	Resultados	**Actividad**
Directivas de contraseñas	Los resultados muestran que no existen controles formales para hacer cumplir las directivas de contraseñas en todas las cuentas.	Pensar en implantar el uso de contraseñas complejas para todas las cuentas como en la sección de mejores prácticas recomendadas. Pensar en implantar el uso de la caducidad de contraseñas como en la sección de mejores prácticas recomendadas.
Subcategoría	**Mejores prácticas recomendadas**	

Cuentas inactivas	Continuar supervisando y gestionando cuentas inactivas. Establecer un proceso para incluir un procedimiento de notificación inmediata a todos los administradores del sistema para el personal que ya no está en la organización con el objeto de garantizar que sus cuentas se deshabiliten inmediatamente, especialmente sus cuentas de acceso remoto. Considerar la posibilidad de implementar un proceso para revisar las cuentas actuales del personal que se transfiere a otro departamento dentro de la organización. Revisar este elemento abierto con el personal de TI o un socio de seguridad. Escribir la respuesta más apropiada a esta pregunta en MSAT para obtener más información. Visitar habitualmente los sitios de los fabricantes para obtener actualizaciones de las firmas de virus y descárguelas en un sitio aislado para probarlas en un entorno de laboratorio. Verificar que las actualizaciones no causen problemas con ningún sistema operativo ni aplicaciones antes de utilizarlas. Desactivar las funciones de actualización automática de las soluciones antivirus en todos los sistemas para evitar la utilización de archivos potencialmente peligrosos antes de su comprobación. Utilizar una consola central para las aplicaciones antivirus, esta consola proporcionará información acerca de los sistemas obsoletos o con funciones de software desactivadas. Para los usuarios remotos que no se conectan regularmente a la red corporativa, utilizar la función de actualización automática. Las cuentas del personal que ya no está en la organización se deben deshabilitar a tiempo para garantizar que los usuarios eliminados u otros usuarios no puedan utilizar la cuenta para obtener acceso no autorizado. Si los administradores de sistemas no tienen información sobre los cambios del estado de un usuario debido a su transferencia, no cambiarán o quitarán los accesos al sistema o físicos. Esto puede dar lugar a un acceso no autorizado o excesivo por parte de los usuarios transferidos.

	Resultados	Actividad
Cuentas inactivas	El resultado muestra que la organización dispone de un proceso formal para revisar cuentas de usuarios inactivas.	Continuar supervisando y gestionando cuentas inactivas.
	El resultado muestra que existen directivas para las actualizaciones de firmas de virus en el entorno.	Visitar con regularidad los sitios de fabricantes y otros proveedores de soluciones de seguridad para buscar avisos de ataques recientes y brotes de virus. Realizar auditorías regularmente para comprobar que los usuarios remotos actualizan sus sistemas. Trabajar conforme a las mejores prácticas recomendadas.
	El resultado muestra que la organización no dispone de un proceso formal para revisar cuentas de usuarios inactivas.	Establecer un proceso para incluir un procedimiento de notificación inmediata a todos los administradores del sistema para el personal que ya no está en la organización con el objeto de garantizar que sus cuentas se deshabiliten inmediatamente, especialmente sus cuentas de acceso remoto. Considerar la posibilidad de implementar un proceso para revisar las cuentas actuales del personal que se transfiere a otro departamento dentro de la organización.
Gestión y control		
Subcategoría	**Mejores prácticas recomendadas**	
Creación segura	Continuar aplicando y siguiendo procedimientos de creación de informes y respuesta ante incidentes formales. Establecer procedimientos para la creación de informes de incidentes y sus respuestas, problemas o preocupaciones sobre seguridad. Designar un equipo de respuesta de emergencia que incluya representantes de	

	varias disciplinas, incluidas tecnología, recursos humanos y legal para responder a todos los incidentes y problemas de seguridad. Considerar la posibilidad de implementar un programa completo de respuesta a incidentes que incluya equipos de respuesta a incidentes, gestión de contención, correlación y análisis de eventos, y procedimientos de repuesta a incidentes. Revisar este elemento abierto con su personal de TI o un socio de seguridad. Escribir la respuesta más apropiada a esta pregunta en MSAT para obtener más información. Los planes de recuperación ante desastres y de reanudación de negocio deben estar bien documentados y actualizados para asegurar la recuperación en un período de tiempo aceptable. Los planes (incluida la restauración a partir de copias de seguridad para aplicaciones) se deben probar periódicamente para validar el grado de corrección e integridad. Los planes de continuidad de negocio se deben centrar en todo el entorno: físico, tecnológico y personal. Es importante seguir un proceso de creación de informes de incidentes y respuesta documentado para garantizar que todos los problemas e incidentes se revisan y se evalúan de forma coherente. Es importante que todos los usuarios comprendan su responsabilidad de notificar los problemas o incidentes de seguridad y que tengan un proceso definido claramente para notificar estos problemas.

	Resultados	**Actividad**
Creación segura	Los resultados muestran que no se han instalado cortafuegos particulares en todas las estaciones de trabajo del entorno.	Aplicar una directiva que solicite una revisión periódica de las configuraciones predeterminadas de los cortafuegos para tener en cuenta los cambios en las aplicaciones o los servicios utilizados.

El resultado muestra que los procesos de creación de los dispositivos de infraestructura están documentados.	Implantar un proceso de creación documentado para los dispositivos de infraestructura y asegurar que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Los resultados muestran que no hay software de acceso remoto del lado del cliente instalado en las estaciones de trabajo que se conectan remotamente a la red corporativa.	Considerar utilizar software de acceso remoto en todas las estaciones individuales, si se necesita conectividad remota. Configurar el software de cliente para seguir la directiva de servidores de acceso remoto.
Los resultados muestran que los procesos de creación de los servidores están documentados.	Implantar un proceso de creación documentado para los servidores y asegurar que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Los resultados muestran que no utiliza ningún software de cifrado de discos en el entorno.	Pensar en utilizar software de cifrado de discos con el fin de no poner en peligro la confidencialidad de los datos en caso de robo del equipo.
Los resultados muestran que los procesos de creación de las estaciones de trabajo y los portátiles están documentados.	Continuar usando un proceso de creación documentado para las estaciones de trabajo y los portátiles, y asegúrese de que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Los resultados muestran que no utiliza ningún software de control/gestión remota en el entorno.	Continuar con la práctica de no utilizar software de gestión/control remoto.

	Los resultados muestran que utiliza un protector de pantalla protegido por contraseña en el entorno.	Continuar con la práctica de exigir a todos los usuarios que tengan un protector de pantalla protegido por contraseña con un tiempo de espera breve.
	Los resultados muestran que no se utilizan módems en el entorno.	Continuar la deshabilitación del acceso por módem y marcación telefónica para reducir el riesgo de que se pueda acceder directamente a los equipos mediante marcación.

Subcategoría	**Mejores prácticas recomendadas**
Seguridad física	Continuar implementando controles de acceso de seguridad física. Establezca controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considerar la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumentar la concienciación del personal sobre las directivas de control de acceso del personal y fomentar la duda ante personas desconocidas. Todos los equipos informáticos se deben proteger contra robos. Los servidores y los equipos de red deben asegurarse en ubicaciones cerradas con acceso controlado. El acceso físico se debe controlar estrictamente, evitando que las personas no autorizadas accedan a edificios, datos confidenciales y sistemas. Con este acceso, pueden alterar las configuraciones del sistema, introducir vulnerabilidades en la red o incluso destruir o robar equipos.

	Resultados	**Actividad**
Seguridad física	Los resultados muestran se han instaurado controles de seguridad física para proteger los activos de la empresa.	Continuar utilizando los controles físicos y considere su uso en todos los equipos informáticos en caso de que aún no se haya realizado.

	Los resultados muestran que se ha instalado un sistema de alarma para detectar e informar de intrusiones.	Continuar utilizando el sistema de alarma y compruébelo con frecuencia (junto con la alarma de su empresa) para garantizar que está funcionando correctamente.
	El resultado muestra que (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada) no están implementados.	Establecer controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considerar la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumentar la concienciación del personal sobre las directivas de control de acceso del personal y fomentar la duda ante personas desconocidas.
	Los resultados muestran que los equipos de la red se hallan en una habitación cerrada con acceso restringido.	Continuar con la práctica de proteger equipo de red en una habitación cerrada y asegurar que únicamente acceden los que deben hacerlo por alguna actividad relacionada con la empresa.
	El resultado muestra que todo o parte de lo siguiente está implementado. (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada)	Continuar implementando controles de acceso de seguridad física.
	Los resultados muestran que los equipos de la red se encuentran además en un armario cerrado.	Si el equipo de red se encuentra en un armario cerrado, la protección contra la manipulación no autorizada es adicional. Asegurar que el acceso a las llaves y combinaciones se limita a aquéllos que únicamente lo necesitan por alguna actividad relacionada con la empresa.

	El resultado muestra que (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada) no están implementados.	Establecer controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considerar la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumentar la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas.
	Los resultados muestran que los servidores se hallan en una habitación cerrada con acceso restringido.	Continuar la práctica de asegurar los servidores en una habitación cerrada y asegúrese de que únicamente acceden los que deben hacerlo por alguna actividad relacionada con la empresa.
	El resultado muestra que (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles) no están implementados.	Establecer controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considerar la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumentar la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas. Seguridad física Sus respuestas indican que los servidores no se encuentran en un armario cerrado.
	Los resultados muestran que los servidores no se encuentran en un armario cerrado.	Si los servidores se encuentran en un armario cerrado, la protección contra la manipulación no autorizada es adicional. Si es posible, considerar migrar los servidores a recintos que se puedan cerrar con llave.

	Los resultados muestran que las estaciones de trabajo no están protegidas con cables de seguridad.	Para evitar robos, considerar asegurar las estaciones de trabajo con cables de seguridad.
	Los resultados muestran que los ordenadores portátiles no están protegidos con cables de seguridad.	Para evitar robos, considerar asegurar los portátiles mediante cables de seguridad.
	Los resultados muestran que los materiales impresos confidenciales se almacenan en armarios con llave.	Continuar la práctica de guardar los materiales impresos confidenciales en armarios cerrados. Además, los documentos confidenciales deben destruirse cuando no sean necesarios.

9. Guía de actividades prioritarias para Aplicaciones

Aplicaciones		
Utilización y uso	→	Mecanismos para mejorar la disponibilidad
Diseño y aplicaciones	→	Autenticación, control de acceso, gestión de actualizaciones, validación de datos de entrada y auditorías
Almacenamiento y comunicación de datos	→	Cifrado, transferencia de datos y acceso restrictivo

Implementación y uso		
	Resultados	**Actividad**
Equilibrio de carga	Los resultados muestran que no se utilizan equilibradores de carga en el entorno.	Pensar en utilizar equilibradores de carga de hardware en el primer nivel de los servidores Web para obtener una mayor disponibilidad. El equilibrador de carga muestra una sola dirección IP (virtual) al exterior que se asigna a todas las direcciones de cada servidor Web en el clúster.

Clústeres	Los resultados muestran que no se utiliza la agrupación en clústeres en el entorno.	Para asegurar una disponibilidad alta de las bases de datos críticas y de los archivos compartidos, pensar en utilizar mecanismos de clúster.
Aplicación y recuperación de datos	Los resultados muestran que su empresa no tiene ninguna línea de aplicaciones empresariales.	Al no tener ninguna aplicación de línea comercial de propósito crítico, se evita el riesgo de que tales sistemas fallen. Sin embargo, si se prevé utilizar alguna en el futuro, estas aplicaciones deberían evaluarse periódicamente para la seguridad, someterse a procesos regulares de copias de seguridad, documentarse a fondo y contar con planes de contingencia en caso de que se produzcan fallos.
	El resultado muestra que se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.	Poner en práctica una directiva de almacenamiento externo de los dispositivos de copias de seguridad y una directiva para las rotaciones frecuentes de estos dispositivos.

Subcategoría	**Mejores prácticas recomendadas**
Fabricante de software independiente (ISV)	Los fabricantes de software independiente (ISV) deben ofrecer revisiones y actualizaciones periódicas, en las que se explique su finalidad y las consecuencias derivadas de su uso en términos de funcionalidad, configuración y seguridad. El ISV debe identificar claramente cuáles son las actualizaciones más importantes para que se apliquen rápidamente. Asimismo, se debe describir los distintos mecanismos de seguridad de la aplicación y proporcionar la documentación más reciente. La empresa debe conocer las configuraciones necesarias para garantizar el nivel de seguridad más alto.

	Resultados	Actividad
Fabricante de software independiente (ISV)	Los resultados muestran que otros fabricantes han desarrollado una o más de las aplicaciones principales del entorno.	Asegurar que se podrá seguir disponiendo de servicio técnico y actualizaciones periódicas para los softwares clave de la empresa, o que el fabricante independiente de los mismos puede ofrecer el código de origen en caso de que ya no pueda prestar dicho servicio para la aplicación.
	El resultado muestra que los fabricantes independientes de software no suelen ofrecer revisiones ni actualizaciones de seguridad.	Intentar colaborar con el fabricante de aplicaciones para recibir actualizaciones y revisiones lo más frecuentemente posible. Cuando aparezca una actualización, pruébela completamente en el entorno de laboratorio antes de utilizarla. Intentar conseguir la documentación para reforzar la aplicación del ISV, si existe, y revisar las configuraciones de la aplicación.
Subcategoría	**Mejores prácticas recomendadas**	
Desarrollado internamente	El equipo de desarrollo interno debe proporcionar las actualizaciones y revisiones e indicar cuál es la finalidad de la actualización y las consecuencias derivadas de su uso en términos de funcionalidad, configuración y seguridad. El equipo de desarrollo interno debe identificar claramente cuáles son las actualizaciones más importantes para que la empresa pueda instalarlas rápidamente. El equipo de desarrollo debe describir los distintos mecanismos de seguridad de la aplicación y proporcionar la documentación más actualizada. La empresa debe conocer las configuraciones necesarias para garantizar el nivel de seguridad más alto.	

	Considerar la posibilidad de contratar servicios independientes para revisar la arquitectura y utilización de la aplicación y para identificar los problemas de seguridad que pudieran existir.

	Resultados	Actividad
Desarrollado internamente	Los resultados muestran que la empresa no utiliza macros personalizadas en las aplicaciones ofimáticas.	No continuar utilizando macros de Office personalizadas, ya que es necesario que las configuraciones de seguridad de Office se reclasifiquen a un nivel inferior, por lo que las aplicaciones ofimáticas quedan expuestas a documentos peligrosos.

Subcategoría	Mejores prácticas recomendadas
Vulnerabilidades	Se deben identificar y corregir todas las vulnerabilidades de seguridad conocidas. Visitar los sitios de los fabricantes y otros proveedores de soluciones de seguridad para buscar información sobre nuevas vulnerabilidades, así como las actualizaciones disponibles. Si no existen actualizaciones disponibles para vulnerabilidades de seguridad conocidas, intentar averiguar cuándo podrá disponer de una y desarrollar un plan de seguridad provisional. También se puede contratar servicios independientes para revisar regularmente el diseño de seguridad de la aplicación. Una evaluación realizada por terceros podría descubrir otros problemas que exijan mecanismos de seguridad adicionales.

	Resultados	Actividad
Vulnerabilidades	Los resultados muestran que no hay procedimientos que aborden los aspectos vulnerables de la seguridad conocidos.	Colaborar con el fabricante de la aplicación (fabricante independiente de software o equipo de desarrollo interno) para crear un plan contra las vulnerabilidades de seguridad. Si existe una actualización, probarla completamente en el entorno de laboratorio antes de utilizarla.

		Además, debe probar cada aplicación después de aplicar la actualización para identificar conflictos propios a esa aplicación que existan.

Diseño de aplicaciones	
Subcategoría	**Mejores prácticas recomendadas**
Autenticación	La aplicación debe utilizar un mecanismo de autenticación cuya eficacia sea proporcional a las necesidades de seguridad de los datos o de su funcionalidad. Las aplicaciones que dependen de contraseñas deben requerir contraseñas complejas que incluyan diversos caracteres (alfabéticos, numéricos, y símbolos), una longitud mínima, un historial, un límite de duración, una pre-caducidad y una comprobación en el diccionario. La aplicación debe archivar los intentos de registro fallidos, pero no la contraseña. Cada componente que concede acceso a datos o a funciones debe requerir una autenticación correcta. Se debe proteger el acceso administrativo a los sistemas con los tipos de autenticación más sólidos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las de las cuentas normales. Además de usar contraseñas sólidas con directivas de contraseñas, considerar la autenticación multifactor para una mayor seguridad.
Subcategoría	**Mejores prácticas recomendadas**
Directivas de contraseñas	La utilización de contraseñas sólidas es un elemento fundamental del índice de la defensa en profundidad. Estas contraseñas deben tener entre 8 y 14 caracteres e incluir caracteres alfanuméricos y especiales. Se debe establecer una longitud mínima, un historial, un límite a la duración y una

	caducidad para reforzar la defensa. Generalmente, la caducidad de las contraseñas debe configurarse de esta forma: + Duración máxima de 90 días + Las cuentas nuevas deben cambiar la contraseña al inicio de la sesión + Un historial de 8 contraseñas (mínimo de 8 días) Se debe proteger el acceso administrativo a los sistemas con los tipos de autenticación más sólidos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las que se emplean para cuentas normales, si las cuentas normales requieren contraseñas con 8 caracteres, las cuentas administrativas deben requerir contraseñas de 14 caracteres. Activar una práctica de bloqueo de la cuenta tras 10 intentos fallidos en todas las cuentas de usuario. Los controles para bloquear una cuenta pueden variar, algunos simplemente consisten en bloquear ataques de fuerza bruta a contraseñas y otros requieren que un administrador desbloquee la cuenta. Cuando se pongan en práctica controles de bloqueo de cuenta, siga las normas siguientes: + Bloqueo después de 10 intentos de registro fallidos para las cuentas de usuario + Requerir la intervención de un administrador para desbloquear las cuentas de aplicaciones importantes y reactivar automáticamente las cuentas de usuarios normales al cabo de 5 minutos + 30 minutos para almacenar en caché los fallos de cuentas de usuarios normales
Resultados	**Actividad**

Autorización y control de acceso	El resultado muestra que las aplicaciones principales limitan el acceso a datos y funciones confidenciales según los privilegios de la cuenta.	Pensar en probar exclusivamente las aplicaciones principales que procesen datos confidenciales y las interfaces disponibles para los usuarios por Internet. Incluir pruebas tipo "caja negra" e "informadas" de la aplicación y comprobar la asignación de mayores privilegios.
Subcategoría	**Mejores prácticas recomendadas**	
Registro	Se debe activar archivos de registro en todas las aplicaciones del entorno. Los datos de archivos de registro son importantes para los análisis de incidentes, tendencias y auditorías. La aplicación debe registrar los intentos de autenticación que tienen éxito y los fallidos, además de los cambios de datos de la aplicación, incluidas las cuentas de usuarios, los errores graves de la aplicación y los accesos correctos y fallidos a los recursos. Cuando se escriban datos en los archivos de registro, la aplicación deberá evitar los de carácter confidencial.	
	Resultados	**Actividad**
Registro	Los resultados muestran que hay varios eventos registrados por las aplicaciones del entorno. Las aplicaciones deben registrar todos los eventos según las prácticas recomendadas.	Para facilitar la gestión y el análisis de los archivos de registro, se pueden integrar en un mecanismo de registro central. Este mecanismo guarda estos archivos según la directiva corporativa de retención de datos.
	Los resultados muestran que no se registran los intentos fallidos de autenticación.	Considerar realizar registros de intentos de autenticación fallidos con el fin de poder detectar ataques de fuerza bruta.

	Los resultados muestran que se registran los intentos de autenticación correctos.	Continuar realizando registros de autenticaciones correctos.
	Los resultados muestran que no se registran los errores de las aplicaciones.	Considerar realizar registros de errores de la aplicación con el fin de poder resolver problemas y detectar todos los caballos troyanos o códigos peligrosos.
	Los resultados muestran que no se registran los accesos denegados a los recursos.	Considerar realizar registros de acceso denegado a los recursos para poder detectar intentos de asignación de mayores privilegios.
	Los resultados muestran que no se registran los accesos correctos a los recursos.	Considerar realizar registros de acceso correctos a los recursos, con el fin de localizar el comportamiento contraproducente después de que se haya producido.
	Los resultados muestran que se registran los cambios en los datos.	Continuar realizando registros de modificaciones en los datos
	Los resultados muestran que no se registran los cambios en las cuentas de usuario.	Considerar realizar registros de las modificaciones de las cuentas de usuarios para detectar asignaciones de mayores privilegios y creaciones de cuentas nuevas no autorizadas.
Subcategoría	**Mejores prácticas recomendadas**	
Validación de datos de entrada	La aplicación puede permitir la entrada de datos en distintos puntos a partir de fuentes externas, como, por ejemplo, usuarios, aplicaciones de cliente o bien alimentación de datos. Será necesario comprobar que los datos de entrada tengan una sintaxis y semántica correctas. Por otro lado, se comprobará si tales datos cumplen las	

	restricciones de los componentes subyacentes o dependientes, particularmente la longitud de cadenas y los juegos de caracteres. El servidor deberá validar los campos suministrados por el usuario.	
	Resultados	**Actividad**
Validación de datos de entrada	El resultado muestra que se validan los datos de entrada de todos los usuarios finales.	Seguir auditando cada aplicación para asegurarse de que se validan los datos de entrada de forma sistemática y apropiada. Las restricciones de validación de datos de entrada deben permitir datos con sintaxis y semántica correctas y no efectuar únicamente el análisis para la detección de caracteres no válidos.
	El resultado muestra que no se validan los datos de entrada de las aplicaciones de cliente.	Colaborar con el fabricante de la aplicación (fabricante independiente de software o equipo de desarrollo interno) para implantar mecanismos de validación de la entrada de datos. Las restricciones de validación de datos de entrada deben permitir datos con sintaxis y semántica correctas y no efectuar únicamente el análisis para la detección de caracteres no válidos.
	El resultado muestra que no se validan los datos de entrada que proceden de un feed de datos.	Colaborar con el fabricante de la aplicación (fabricante independiente de software o equipo de desarrollo interno) para implantar mecanismos de validación de la entrada de datos. Las restricciones de validación de datos de entrada deben permitir datos con sintaxis y semántica correctas y no efectuar únicamente el análisis para la detección de caracteres no válidos.
Subcategoría	**Mejores prácticas recomendadas**	

Metodología de desarrollo de seguridad de software	Continuar utilizando las metodologías de desarrollo de seguridad de software. Establecer el uso de metodologías de desarrollo de seguridad de software para aumentar la seguridad de las aplicaciones. Si se utilizan consultores o proveedores en alguna fase del ciclo de desarrollo, asegúrese de que tienen formación en la metodología de desarrollo de seguridad de software que la organización utilice o recomiende. Todo el personal de desarrollo de la organización debe recibir formación sobre la metodología de desarrollo de seguridad para software elegido por la organización. Esto incluye administradores de desarrollo, desarrolladores, evaluadores y personal de control de calidad. Con el panorama de evolución de amenazas de seguridad, es importante actualizar la formación sobre metodologías de desarrollo de seguridad de software y modelos de amenazas anualmente. Se le solicitará al personal de desarrollo que siga la formación sobre desarrollo de seguridad cada año. El uso de herramientas de prueba de software de seguridad mejora la capacidad del equipo para escribir código seguro con más eficacia. El resultado del uso de las herramientas de prueba se debe incorporar a la formación anual necesaria.

	Resultados	**Actividad**
Metodología de desarrollo de seguridad de software	El resultado muestra que la organización utiliza herramientas de pruebas de software de seguridad como parte del proceso de desarrollo de seguridad.	Ampliar el uso de las herramientas de prueba de software de seguridad como parte instrumental de todos los planes de desarrollo de seguridad.
	El resultado muestra que la organización no proporciona formación sobre metodologías de seguridad para software para el personal de desarrollo.	Establecer un programa de formación de metodologías de desarrollo de seguridad de software con el objeto de mejorar la capacidad del personal para desarrollar código seguro.

Almacenamiento y comunicaciones de datos	
Subcategoría	**Mejores prácticas recomendadas**
Cifrado	Los datos confidenciales deben cifrarse o codificarse mediante hash en la base de datos y en el sistema de archivos. La aplicación debe diferenciar entre los datos que podrían estar expuestos a la divulgación (es necesario cifrarlos), los datos que podrían llegar a manipularse (es necesario un valor de claves hash) y los datos que se pueden transformar (hash) sin ninguna pérdida de funcionalidad, como las contraseñas. Las claves para descifrar se guardarán en un lugar distinto a la información cifrada. Los datos confidenciales se deben cifrar antes de transmitirlos a otros componentes. Verifique que los componentes intermedios que controlan los datos en un formato de texto sin formato antes o después de la transmisión no representan una amenaza excesiva. La aplicación debe sacar partido de las funciones de autenticación disponibles con el mecanismo de transmisión segura. Algunos de los cifrados más habituales y fiables son: 3DES, AES, RSA, RC4 y Blowfish. Utilice claves de 128 bits (1024 bits para RSA) como mínimo.
Subcategoría	**Mejores prácticas recomendadas**
Cifrado - Algoritmo	La aplicación debe utilizar algoritmos de cifrado estándares del sector, con claves de tamaños adecuados y modelos de cifrado apropiados. Algunos de los cifrados más habituales y fiables son: 3DES, AES, RSA, RC4 y Blowfish. Se debe utilizar un tamaño de clave mínimo de 128 bits (para RSA, 1024 bits).

10. Guía de actividades prioritarias para Operaciones y Personal

Operaciones y Personal		
Requisitos y evaluaciones	→	Planificación, evaluaciones de terceros
Directiva y procedimientos	→	Directiva de RR.HH., relaciones con terceros
Formación y conocimiento	→	Divulgación de las medidas de seguridad

Requisitos y evaluaciones	
Subcategoría	**Mejores prácticas recomendadas**
Requisitos de seguridad	La empresa identifica a los individuos con experiencia en el tema de la seguridad para incluirlos en todas las reuniones y decisiones relacionadas. Además, señala qué debe protegerse, teniendo en cuenta el valor del recurso y el nivel de seguridad que se requiere. El análisis incluye todas las amenazas posibles. La estrategia que resulta equilibra los costes y los beneficios de las protecciones, y puede incluir como opciones el traslado o la aceptación de los riesgos. Los requisitos de seguridad, definidos por representantes comerciales y técnicos, se documentan y publican para que el conjunto del personal los pueda consultar y contrastar para diseños futuros. Las diferencias entre los tipos de aplicaciones y de datos pueden dar como resultado la existencia de requisitos diferentes.

	Resultados	**Actividad**
Requisitos de seguridad	Los resultados muestran que la empresa tiene un modelo para la asignación de niveles de gravedad a cada componente del entorno informático.	Continuar asignando niveles de importancia a los componentes y asegurar la actualización del modelo según se añada al equipo nuevo.
	El resultado muestra que existen equipos comerciales y de seguridad que trabajan definiendo requisitos de seguridad.	El equipo de seguridad debe tomar parte en todos los aspectos de los requisitos, diseño y utilización de tecnologías. Se deben documentar requisitos claros para las

		especificaciones de funcionamiento.
	Los resultados muestran que el equipo de seguridad no participa en la fase de planificación ni diseño del ciclo de vida de la tecnología.	El equipo de seguridad debe participar en todas las fases del ciclo de vida de la tecnología, para todos los proyectos.
	Los resultados muestran que el equipo de seguridad no participa en la fase de implantación del ciclo de vida de la tecnología.	El equipo de seguridad debe participar en todas las fases del ciclo de vida de la tecnología, para todos los proyectos.
	Los resultados muestran que el equipo de seguridad no participa en la fase de comprobación del ciclo de vida de la tecnología.	El equipo de seguridad debe participar en todas las fases del ciclo de vida de la tecnología, para todos los proyectos.
Subcategoría	**Mejores prácticas recomendadas**	
Evaluaciones de seguridad	Las evaluaciones por parte de terceros aportan una perspectiva objetiva muy valiosa para las medidas de seguridad de una empresa. Estas evaluaciones también podrían resultar beneficiosas para cumplir las estipulaciones normativas y los requisitos de los clientes, socios y fabricantes. Las evaluaciones deben incluir la infraestructura, las aplicaciones, las directivas y los procedimientos de auditoría. Estas evaluaciones no deben centrarse exclusivamente en la identificación de vulnerabilidades, sino también en señalar configuraciones que no sean seguras o privilegios de acceso innecesarios. Se deben revisar las directivas y los procedimientos de seguridad para descubrir si tienen lagunas.	
	Resultados	**Actividad**

Evaluaciones de seguridad	Los resultados muestran que las evaluaciones de la seguridad de la empresa las realiza personal interno.	El personal interno debe continuar realizando auditorías de seguridad frecuentes, pero debe aumentar estas auditorías con los datos de entrada de un tercero de confianza.
	Los resultados muestran que la evaluación se realiza trimestralmente.	Seguir la práctica de evaluaciones de seguridad de forma trimestral.
	El resultado muestra que no encarga a empresas independientes la evaluación de los medios de seguridad.	Empezar con autoevaluaciones de la infraestructura crítica de red y de las aplicaciones. Estudiar desarrollar un plan que solicite evaluaciones regulares realizadas por terceros para la infraestructura crítica de red y de las aplicaciones. Incluir los resultados de las evaluaciones en los proyectos de mejora.
Directiva y procedimientos		
Subcategoría	**Mejores prácticas recomendadas**	
Comprobaciones del historial personal	Se deben realizar comprobaciones del historial personal para descubrir cualquier problema posible, con objeto de reducir el riesgo al que se exponen la empresa y los empleados. Este proceso también permite localizar cualquier problema o laguna en el currículum del aspirante. El proceso de contratación de personal debe incluir una evaluación del historial laboral y cualquier antecedente penal del aspirante. Se deben evaluar las habilidades del aspirante comparándolas con las descripciones detalladas y los requisitos del puesto para detectar los puntos fuertes y débiles.	

	Resultados	Actividad
Comprobaciones del historial personal	El resultado muestra que se hacen comprobaciones del historial personal de todos los empleados. habilitados accesos administrativos a las estaciones de trabajo.	Asegurar que la comprobación del historial personal incluye una evaluación del historial laboral, la formación y los antecedentes penales del aspirante.
Subcategoría	**Mejores prácticas recomendadas**	
Directiva de recursos humanos	Los procedimientos formales para gestionar el caso de los empleados que dejan la empresa garantizan que se actúa debidamente cuando se rescinde un contrato de trabajo. Estos procedimientos deben existir para gestionar la situación de los empleados que dejan la empresa amistosamente y los que la dejan de forma hostil. Estos procedimientos deben incluir: + Notificación a todos los departamentos (Recursos humanos, TI, Seguridad física, Servicio de atención al cliente, Finanzas, etc.) + Acompañamiento del empleado al abandonar las instalaciones + Cancelación de todas las cuentas del usuario y de su acceso a la red + Recuperación de todos los bienes de la empresa (portátiles, PDA, dispositivos electrónicos, documentos confidenciales, etc.)	
	Resultados	**Actividad**
Directiva de recursos humanos	El resultado muestra que existe una directiva formal para los empleados que dejan la empresa de forma hostil.	Revisar a menudo el procedimiento para los empleados que dejan la empresa de forma hostil y complételo previa evaluación de ceses anteriores.
	El resultado muestra que no existe ninguna directiva para los empleados que dejan la empresa de forma amistosa.	Colaborar con el departamento de recursos humanos para desarrollar de inmediato un procedimiento para los empleados que dejan la empresa de forma amistosa.

Subcategoría	Mejores prácticas recomendadas
Relaciones con terceros	Con objeto de reducir el riesgo de revelación de datos, deben existir directivas y procedimientos formales enfocados a las relaciones con terceros. Así, se podrá detectar cualquier problema de seguridad y la responsabilidad de cada parte a la hora de solucionarlo. Estas directivas deben incluir: + El nivel de conectividad y acceso + La presentación y el tratamiento de los datos + Los roles y las responsabilidades (incluida la autoridad) de cada parte + La gestión de la relación: creación, mantenimiento y cese.

	Resultados	Actividad
Relaciones con terceros	Los resultados muestran que los acuerdos de nivel de servicio están incluidos en los contratos con el proveedor de los servicios subcontratados.	Continuar exigiendo acuerdos de nivel para los servicios específicos de seguridad subcontratados.
	Los resultados muestran que los sistemas se configuran por parte de los proveedores o distribuidores de hardware.	Para reducir los riesgos que implica la ejecución de los servicios predeterminados, el personal interno debería configurar los sistemas siguiendo una simulación de creación.
	Los resultados muestran que la empresa ha contratado los servicios de un tercero para la gestión del entorno informático.	Según las necesidades de la empresa, pueden ser soluciones viables tanto la gestión propia como la subcontratada. Si se subcontratan los servicios, los requisitos de seguridad deberían tratarse en el contrato y los acuerdos de nivel de servicio (SLA) deberían garantizar el cumplimiento de tales requisitos.

	Los resultados muestran que no se han incluido condiciones específicas de seguridad en los SLA (Acuerdos de nivel de servicio).	Con el fin de tener un mecanismo para tratar y garantizar el cumplimiento de los requisitos de seguridad, deberían exigirse acuerdos de nivel de nivel para los servicios específicos de seguridad subcontratados.
	El resultado muestra que no existe ninguna directiva para las relaciones con terceros.	Se deben desarrollar directivas y procedimientos formales para los distintos tipos de relaciones con terceros con el acuerdo común de toda la empresa. Para ello, hacer partícipe a los diversos equipos empresariales. Si las directivas se elaboran correctamente, los riesgos a los que está expuesta la empresa se verán reducidos.
Formación y conocimiento		
Subcategoría	**Mejores prácticas recomendadas**	
Conocimiento de seguridad	Un programa formal de divulgación de las medidas de seguridad ayuda a los empleados a contribuir a la seguridad global de la empresa, puesto que se les mantiene informados acerca de los riesgos existentes. La mejor garantía de alerta ante problemas potenciales es formar debidamente al personal en materia de seguridad. Un programa de divulgación efectivo debe tener en cuenta todos los aspectos de la seguridad (aplicaciones, redes y soportes físicos) y ofrecer también pautas claras a los empleados en caso de que detecten un riesgo para la seguridad de cualquiera de estos elementos. Poner en práctica directivas para regular la utilización de los recursos corporativos por parte de los empleados. Los programas de divulgación deben formar parte del curso de orientación de empleados nuevos. Se debe proporcionar información	

	actualizada y cursos para asegurar que todos los empleados conozcan las prácticas y los riesgos más recientes. Se deben realizar comprobaciones periódicas para asegurarse de que los empleados han asimilado la información.

	Resultados	Actividad
Conocimiento de seguridad	Los resultados muestran que ha asignado a un individuo o grupo la seguridad de la empresa.	Continuar asegurándose que la empresa tenga una persona o equipo responsable de la seguridad y requiera que se consulte a este equipo antes de realizar cambios en el entorno informático.
	Los resultados muestran que el equipo de seguridad no participa en la definición de los requisitos para las nuevas tecnologías o para las ya existentes.	Exigir realizar consultas al equipo de seguridad antes de realizar cambios en el entorno informático. El equipo de seguridad debería participar en todas las reuniones, desde las primeras fases de planificación.
	El resultado muestra que no existe ningún programa de divulgación de las medidas de seguridad en la empresa.	Evaluar poner en práctica un programa formal de divulgación de seguridad para que los empleados conozcan los riesgos relacionados con los recursos de TI. Poner en práctica directivas que regulen la utilización de los recursos y las tecnologías corporativas por parte de los empleados e incluya un programa de divulgación de seguridad en el curso de orientación para nuevos empleados. La mejor garantía de alerta ante problemas potenciales es formar debidamente al personal en materia de seguridad.

Subcategoría	**Mejores prácticas recomendadas**

Formación sobre seguridad	Trabajar con propietarios de empresa para determinar el tiempo de inactividad de aplicaciones críticas. Basándose en esos resultados, aplique las medidas oportunas para satisfacer e incluso superar esos requisitos. La disponibilidad y el rendimiento de las aplicaciones basadas en web mejoran al implementar equilibrio de carga delante de los servidores web. Para equilibrar la carga del servidor, el equilibrio de carga distribuye las solicitudes entre los distintos nodos en el clúster del servidor con el objetivo de optimizar el rendimiento del sistema. Si se produce un error en un servidor web en el clúster del servidor, la solicitud se dirige a otro servidor para atender la solicitud, lo que proporciona una alta disponibilidad. Determinar el tiempo de inactividad aceptable para los usos compartidos de archivos y bases de datos de propietarios de empresa. Pruebe los mecanismos de conmutación por error para las aplicaciones y determine si la cantidad del tiempo de inactividad es aceptable.

	Resultados	**Actividad**
Formación sobre seguridad	El resultado muestra que la formación por temas se está ofreciendo actualmente a los empleados sobre la base de los cometidos que desempeñan en la empresa.	La formación basada en roles y el aprendizaje continuo garantizan que todos los empleados entiendan qué se espera de ellos y cómo deben satisfacer esas expectativas. Seguir ofreciendo formación en todos los niveles de la empresa y en todos los aspectos de seguridad que exigen el desempeño de los distintos cargos.
	Los resultados muestran que la formación de seguridad de aplicaciones no se ofrece a los empleados en función de su puesto en la empresa.	Todos los empleados de la empresa deberán recibir una formación por temas, adaptada a sus funciones. La formación deberá ser más detallada que la que se ofrezca a los empleados generales. También

		deberá actualizarse periódicamente.
	Los resultados muestran que la formación de preparación para incidentes y reacción no se ofrece a los empleados en función de su puesto en la empresa.	Todos los empleados de la empresa deberán recibir una formación por temas, adaptada a sus funciones. La formación deberá ser más detallada que la que se ofrezca a los empleados generales. También deberá actualizarse periódicamente.
	Los resultados muestran que la formación de seguridad de infraestructuras no se ofrece a los empleados en función de su puesto en la empresa.	Todos los empleados de la empresa deberán recibir una formación por temas, adaptada a sus funciones. La formación deberá ser más detallada que la que se ofrezca a los empleados generales. También deberá actualizarse periódicamente.

11. Trabajo futuro

Teniendo en cuenta que la normativa en cuestiones de seguridad, va cambiando constantemente a lo largo del tiempo, es importante realizar periódicamente nuevas evaluaciones de riesgos o procesos de auditoría. Por otro lado, cabe mencionar que según se vayan agregando nuevos componentes de seguridad en la organización, se deberá volver a evaluar la seguridad, para que la organización este actualizada.

12. Referencias

Carvajal , R. (2015). *Estudio de las normas españolas y estadounidenses de seguridad de la información.* Obtenido de Universidad de Valladolid : https://uvadoc.uva.es/handle/10324/13335

Charney, S. (22 de septiembre de 2014). *Microsoft*. Obtenido de Mirando hacia adelante: Computación confiable: https://www.microsoft.com/security/blog/2014/09/22/looking-forward-trustworthy-computing/

Guevara Díaz, M. L. (2014). *Desarrollo de una Guía para la implantación del modelo de Gestión de la Seguridad de la información en el Instituto Geográfico Militar*. Obtenido de ESPE: http://repositorio.espe.edu.ec:8080/bitstream/21000/10379/1/T-ESPE-048357.pdf

Microsoft. (2011). *Microsoft.* Obtenido de Informe del progreso del proceso SDL.

Microsoft. (11 de 10 de 2017). *Microsoft.* Obtenido de Herramienta de Evaluación de Seguridad de Microsoft (MSAT): https://docs.microsoft.com/es-es/security-updates/security/technetsecurityherramientadeevaluacindeseguridaddemicrosoftmsat#mainsection

Oliván Huerva, A. (2017). *Guía de controles de ciberseguridad para la protección integral de la PYME*. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73066/6/aolivan1TFM0118memoria.pdf

Palmay López, M. C. (2017). *Propuesta de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynet virtuales*. Obtenido de ESPOCH: http://dspace.espoch.edu.ec/bitstream/123456789/7818/1/20T00932.pdf

Quintana Sánchez, A. M., Quintana Romero, M. A., Ojeda Escobar, J. A., & Trujillo Calero, G. E. (2016). *Estándares Internacionales para el control en las ISO.* Quintanilla Romero, Marco Antonio. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiRz-jRucvsAhWitlkKHdxkCEcQFjALegQIBRAC&url=http%3A%2F%2Fwww.dsp

ace.uce.edu.ec%2Fbitstream%2F25000%2F14181%2F1%2FEstandares%2520internacionales%2520para%2520el%2520con

Rouse, M. (2006). *Whatls.* Obtenido de NIST 800 Series: https://whatis.techtarget.com/definition/NIST-800-Series

UNIR. (2018). *Metodologías de Desarrollo Web Seguro*. Obtenido de http://manosnegras.com/unir2018/wp-content/uploads/2017/11/T1.Metodolog%C3%ADas.pdf

13. ANEXOS

13.1Acrónimos

Acrónimo	Descripción
TIC	Tecnologías de la Información y Comunicación
HGUAC	Hospital General Universitario Andino de Chimborazo
TI	Tecnologías de la Información
MSAT	Microsoft Security Assessment Tool
NIST	Instituto Nacional de Estándares y Tecnología
ISO	Organización Internacional de Normalización o Estandarización
TwC	Trustworthy Computing
IEC	Comisión Electrónica Internacional
DiDI	Defense-in-Depth Index / Defensa en Profundidad
AoAs	Áreas de Análisis
BRP	Perfil de Riesgos de Negocio
ACL	Lista de Control de Acceso
DoS	Denegación de Servicio
DMZ	Zona Desmilitarizada
DMA	Acceso Directo a la Memoria
IPSec	Internet Protocol Security
SSL	Secure Socket Layer
SMS	Microsoft Systems Management Server
SSH	Secure Shell
VPN	Red Privada Virtual
SSID	Service Set Identifier
WPA	Acceso Wi-Fi Protegido
WSUS	Windows Server Update Services

MAC	Media Access Control
FTP	Protocolo de Trasnferencia de Archivos
ISV	Fabricante de Software Independiente
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest, Shamir y Adleman
RC4	Ron’s Code 4