



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Análisis de riesgo de las tecnologías de la
información del corporativo Equilibrio
Farmacéutico S.A. de C.V. basado en el
estándar 17799 y otros.

Informe Técnico de Residencias
Profesionales
Para Obtener el Título de

Ingeniero

Presenta(n):
Aldo Mota Zarate

Coacalco de Berriozábal, Febrero/2024

AGRADECIMIENTOS

A mis padres.

Por apoyarme incondicionalmente a lo largo de mi formación, por siempre darme todos los ánimos, además de estar siempre conmigo en los días y en las noches y ser mi principal motor de salir adelante e impulsar cada uno de mis sueños. A ellos principalmente les dedico este proyecto y todas mis metas.

A mi familia.

Por apoyarme, darme ánimos, por estar conmigo en momentos cuando los necesite.

A mi asesora.

Por ser una gran y excelente maestra, siendo mi guía y apoyo a lo largo de esta meta, por brindarme todos los conocimientos necesarios para poder realizar este proyecto, darme los ánimos para lograr concluir bien.

A mis mejores amigos.

Por compartir conmigo momentos especiales tanto académicos como personales, por darme alegría y consejos en situaciones difíciles, por estar conmigo en los momentos buenos y malos.

Al área de TI de EQF.

Por brindarme la oportunidad de realizar mis residencias profesionales, por darme gran parte de sus conocimientos y también ser guías tanto en mi proyecto como en la experiencia laboral que obtuve a lo largo de mis residencias profesionales.

RESUMEN

El presente proyecto sobre el análisis de riesgos de las tecnologías de la información de Equilibrio Farmacéutico en base al estándar ISO 17799 y otros, se estructura en diversos capítulos los cuales ayudan a tener una mejor comprensión de cómo se desarrollará dicho análisis, por lo que se explica a continuación cual es el contenido de cada uno de estos capítulos.

El siguiente análisis de riesgo, primeramente, aborda las generalidades del proyecto, esto con la intención de comprender el contexto de la empresa en el que será desarrollado, las problemáticas que se están presentando actualmente dentro del ámbito de seguridad informática en la empresa, además de conocer los objetivos que se alcanzaran al finalizar el proyecto y la justificación del porque se va a llevar a cabo este análisis de riesgo.

Como segunda parte, se encuentra el marco teórico el cual consta de tres partes, la primera trata sobre el estado del arte donde se busca dar un contexto sobre aquellos hechos más significativos que han ocurrido dentro del campo de la seguridad informática, esto es de gran ayuda para poder tomar decisiones informadas de una manera más fácil y así poder brindar la mejor solución a las diversas problemáticas que se presenten. Posteriormente, se tiene el marco conceptual en el cual se encontrará el significado de aquellos conceptos que puedan representar una dificultad para poder entender el contenido del proyecto. En seguida, se presenta el marco metodológico, dentro de este marco se aborda la estructura de cómo se llevará a cabo la implementación de este análisis de riesgos, además de una breve explicación de los estándares que se utilizaran a lo largo del desarrollo del proyecto.

Posteriormente, se realiza la tercera parte que consta del desarrollo del proyecto en el cual se abordan las técnicas y herramientas que se van a utilizar a lo largo del análisis, de igual manera se podrán encontrar cada uno de los formatos de las técnicas a utilizar y como se llevó a cabo la implementación de cada una de ellas, esto con el propósito de encontrar vulnerabilidades, amenazas y riesgos con los que se enfrenta actualmente EQF y en base a estos tres aspectos encontrar las mejores propuestas que puedan cubrir con la mayoría de las necesidades de la empresa.

Como cuarta parte del desarrollo de este proyecto se tienen los resultados, aquí es donde se muestra la implementación de las propuestas de solución que la empresa decide llevar a cabo de acuerdo a presupuestos y las necesidades que se tengan, con estos resultados se busca mejorar la seguridad de EQF.

Finalmente, se tiene la conclusión del proyecto, las competencias que se utilizaron durante el desarrollo del análisis de riesgos y las fuentes de información que se utilizaron en el marco teórico.

ÍNDICE DE CONTENIDOS

GENERALIDADES DEL PROYECTO	10
INTRODUCCIÓN	11
DESCRIPCIÓN DE LA EMPRESA	12
DESCRIPCIÓN DEL PUESTO O ÁREA DE TRABAJO.....	14
PROBLEMA A RESOLVER.....	15
OBJETIVOS	17
JUSTIFICACIÓN	19
MARCO TEÓRICO.....	21
ESTADO DEL ARTE.....	22
MARCO CONCEPTUAL	25
MARCO METODOLÓGICO	32
DESARROLLO	42
RESULTADOS.....	127
CONCLUSIONES	177
COMPETENCIAS DESARROLLADAS	178
FUENTES DE INFORMACIÓN	184
ANEXOS	187

ÍNDICE DE FIGURAS

Figura 1 Organigrama Equilibrio Farmacéutico.....	12
Figura 2 Grafica de Gantt de las actividades a desarrollar.....	39
Figura 3 Organigrama de Equilibrio Farmacéutico S.A. de C.V.	44
Figura 4 Organigrama del área de TI.....	47
Figura 5 Formato de análisis FODA.....	55
Figura 6 Formato para la matriz de riesgos.	56
Figura 7 FODA niveles de seguridad de software en Equilibrio Farmacéutico.	69
Figura 8 Análisis FODA de la protección del correo electrónico (Outlook).....	70
Figura 9 Análisis FODA de la protección del servicio en la nube (OneDrive).	71
Figura 10 Análisis FODA de la protección del chat TEAMS.....	72
Figura 11 Análisis FODA de las políticas de restricción de páginas web y plataformas de streaming.	73
Figura 12 Matriz de riesgos.....	86
Figura 13 Matriz de riesgos para evaluar.	98
Figura 14 Certificado TOP PRODUCT por AV-TEST.....	133
Figura 15 Certificación AAA de SE Labs como Enterprise Endpoint Security.....	134
Figura 16 Certificación Approved Business Security Product Award por AV Comparatives.	136
Figura 17 Cronograma de implementación de antivirus en dispositivos del corporativo.....	141
Figura 18 Cronograma de implementación del antivirus en dispositivos de sucursales.....	141
Figura 19 Interfaz para poder acceder a la consola de administración de Kaspersky.	143
Figura 20 Panel general de Kaspersky.....	143
Figura 21 Menú para ingresar a la descarga del agente de Kaspersky.	144
Figura 22 Paquetes de instalación (parte 1).	145
Figura 23 Paquetes de instalación (parte 2).	145
Figura 24 Propiedades del paquete independiente.....	146
Figura 25 Opciones del instalador del agente de Kaspersky (parte1).	146
Figura 26 Opciones del instalador del agente de Kaspersky (parte 2).	147
Figura 27 Archivo ejecutable del agente.	147
Figura 28 Comienzo de instalación del agente.	148
Figura 29 Proceso de instalación.....	148
Figura 30 Termina del proceso de instalación del agente de Kaspersky.....	149
Figura 31 Comprobación de la instalación del agente de Kaspersky.	149
Figura 32 Dispositivos no asignados a un grupo.	150
Figura 33 Asignación de grupo.	151
Figura 34 Dispositivos administrados dentro del grupo de EQF.	151
Figura 35 Búsqueda de dispositivos.	152
Figura 36 Propiedades del dispositivo seleccionado (parte 1).	152
Figura 37 Propiedades del dispositivo seleccionado (parte 2).	153
Figura 38 Dispositivos administrados (parte 1).	154
Figura 39 Dispositivos administrados (parte 2).	154
Figura 40 Propiedades del estado de protección de los dispositivos.....	155
Figura 41 Interfaz de las tareas de Kaspersky.	156

Figura 42 Asistente para crear una nueva tarea.	157
Figura 43 Tipos de tareas en Kaspersky.	157
Figura 44 Alcance de la tarea.	158
Figura 45 Especificaciones de la tarea.	158
Figura 46 Termino de la tarea creada.	159
Figura 47 Inicio de la tarea creada para la actualización de la base de datos de virus.	159
Figura 48 Estado de la tarea en ejecución.	160
Figura 49 Amenazas detectadas por componente.	161
Figura 50 Amenazas más frecuentes.	161
Figura 51 Top 10 de los dispositivos más infectados.	162
Figura 52 Directivas y perfiles.	165
Figura 53 Configuración general del aplicativo.	165
Figura 54 Configuración de la aplicación.	166
Figura 55 Opciones de controles de seguridad.	166
Figura 56 Habilitar control web.	167
Figura 57 Lista de reglas.	167
Figura 58 Creación y configuración de la nueva regla.	168
Figura 59 Personalización de mensaje de bloqueo.	168
Figura 60 Control de aplicaciones.	169
Figura 61 Habilitar control de aplicaciones.	169
Figura 62 Configuración de regla de bloqueo de aplicaciones.	170
Figura 63 Personalización de mensaje de bloqueo a aplicativos.	170
Figura 64 Control de aplicaciones.	171
Figura 65 Habilitar control de dispositivos.	171
Figura 66 Configuración de control de dispositivos.	172
Figura 67 Personalización de mensaje de bloqueo para los dispositivos.	172
Figura 68 Configuración de interfaz.	173
Figura 69 Interfaz simplificada del antivirus para el usuario.	174
Figura 70 Restricción de acceso a un sitio web no seguro.	175
Figura 71 Restricción de acceso a sitio web.	175
Figura 72 Evidencia de acceso a YouTube.	188
Figura 73 Interfaz para poder acceder a la consola de administración de Kaspersky.	192
Figura 74 Panel general de Kaspersky.	193
Figura 75 Menú para ingresar a la descarga del agente de Kaspersky.	194
Figura 76 Paquetes de instalación.	195
Figura 77 Propiedades del paquete independiente.	195
Figura 78 Opciones del instalador del agente de Kaspersky.	196
Figura 79 Archivo ejecutable del agente.	196
Figura 80 Comienzo de instalación del agente.	197
Figura 81 Proceso de instalación.	197
Figura 82 Termino del proceso de instalación del agente de Kaspersky.	198
Figura 83 Comprobación de la instalación del agente de Kaspersky.	198
Figura 84 Dispositivos no asignados a un grupo.	199
Figura 85 Asignación de grupo.	200

Figura 86 Dispositivos administrados dentro del grupo de EQF.	200
Figura 87 Búsqueda de dispositivos.	201
Figura 88 Dispositivos administrados.	202
Figura 89 Propiedades del estado de protección de los dispositivos.	202
Figura 90 Interfaz de las tareas de Kaspersky.	203
Figura 91 Asistente para crear una nueva tarea.	204
Figura 92 Tipos de tareas en Kaspersky.	205
Figura 93 Alcance de la tarea.	205
Figura 94 Especificaciones de la tarea.	206
Figura 95 Termina de la tarea creada.	206
Figura 96 Interfaz de las tareas de Kaspersky.	207
Figura 97 Inicio de la tarea creada para la actualización de la base de datos de virus.	208
Figura 98 Estado de la tarea en ejecución.	208
Figura 99 Directivas y perfiles	209
Figura 100 Configuración general del aplicativo.	210
Figura 101 Configuración de la aplicación.	210
Figura 102 Opciones de controles de seguridad.	211
Figura 103 Habilitar control web.	211
Figura 104 Lista de reglas.	211
Figura 105 Creación y configuración de la nueva regla.	212
Figura 106 Personalización de mensaje de bloqueo.	213
Figura 107 Directivas y perfiles	214
Figura 108 Configuración general del aplicativo.	214
Figura 109 Configuración de la aplicación.	215
Figura 110 Control de aplicaciones.	215
Figura 111 Habilitar control de aplicaciones.	216
Figura 112 Configuración de regla de bloqueo de aplicaciones.	216
Figura 113 Personalización de mensaje de bloqueo a aplicativos.	217
Figura 114 Directivas y perfiles	218
Figura 115 Configuración general del aplicativo.	218
Figura 116 Configuración de la aplicación.	219
Figura 117 Control de aplicaciones.	219
Figura 118 Habilitar control de dispositivos.	220
Figura 119 Configuración de control de dispositivos.	220
Figura 120 Personalización de mensaje de bloqueo para los dispositivos.	221
Figura 121 Configuración de interfaz.	221
Figura 122 Interfaz simplificada del antivirus para el usuario.	222

ÍNDICE DE TABLAS

Tabla 1 Cuadro Metodológico Integral para el Desarrollo del Proyecto.....	34
Tabla 2 Formato de encuesta de vulnerabilidades y amenazas.	55
Tabla 3 Primera parte del formato para la revisión de las actividades de control.	58
Tabla 4 Segunda parte del formato para la revisión de las actividades de control.	60
Tabla 5 Identificación de riesgos en base a vulnerabilidades y amenazas.	75
Tabla 6 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades.	77
Tabla 7 Cuestionario de nivel de impacto y probabilidad de amenazas.....	82
Tabla 8 Ejemplo del primer riesgo evaluado.....	85
Tabla 9 Nivel de prioridad de cada una de las vulnerabilidades evaluadas.....	86
Tabla 10 Nivel de prioridad de cada una de las amenazas evaluadas.	88
Tabla 11 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades.	89
Tabla 12 Cuestionario de nivel de impacto y probabilidad de amenazas.....	94
Tabla 13 Ejemplo del primer riesgo evaluado.....	97
Tabla 14 Nivel de prioridad de cada una de las vulnerabilidades evaluadas.....	99
Tabla 15 Nivel de prioridad de cada una de las amenazas evaluadas.	100
Tabla 16 Porcentaje de probabilidad de que ocurra una vulnerabilidad.....	103
Tabla 17 Porcentaje de probabilidad de que ocurra una amenaza.	105
Tabla 18 Valor Monetario Total Aproximando del Impacto de la Vulnerabilidad (pesos mexicanos).	106
Tabla 19 Valor Monetario Total Aproximando del Impacto de la Amenaza (pesos mexicanos).	107
Tabla 20 Valor Monetario Esperado de las Vulnerabilidades.....	108
Tabla 21 Valor Monetario Esperado de las Amenazas.	110
Tabla 22 Vulnerabilidades por orden de prioridad.	111
Tabla 23 Amenazas por orden de prioridad.....	112
Tabla 24 Primera parte de revisión del primer control de seguridad.	115
Tabla 25 Segunda parte de revisión del primer control de seguridad.	116
Tabla 26 Primera parte de revisión del segundo control de seguridad.....	116
Tabla 27 Segunda parte de revisión de seguridad control de seguridad.....	117
Tabla 28 Propuesta de solución del primer riesgo.	119
Tabla 29 Propuesta de solución del segundo y tercer riesgo.....	120
Tabla 30 Propuesta de solución del cuarto y quinto riesgo.....	122
Tabla 31 Propuesta de solución para el sexto riesgo.	123
Tabla 32 Propuesta de solución para el séptimo riesgo.	124
Tabla 33 Comparativa de precios de antivirus en su versión empresarial.....	129
Tabla 34 Comparativa de certificaciones entre Kaspersky y Panda en versiones empresariales.....	131
Tabla 35 Evaluación de las características más destacadas por SoftwareReviews.	132
Tabla 36 Calificación de pruebas realizadas por AV-Test.....	134
Tabla 37 Calificación de pruebas realizadas por SE Labs.	135
Tabla 38 Porcentaje de amenazas bloqueadas en pruebas realizadas por AV Comparatives.....	136
Tabla 39 Partner Oficiales de Kaspersky.....	137
Tabla 40 Comparativa de precios de partner de Kaspersky.	137
Tabla 41 Comparativa de precios de licenciamiento.	139

CAPÍTULO I

GENERALIDADES DEL PROYECTO

INTRODUCCIÓN

El presente proyecto aborda el tema de análisis de riesgo de las tecnologías de la información dentro de la empresa de Equilibrio Farmacéutico (EQF), en base al estándar ISO 17799 y otros, los cuales servirán como apoyo y guía para evaluar la situación actual en la que se encuentra la seguridad informática para la protección de la información, además de sus tecnologías de la información, con la finalidad de proponer e implementar mejoras las cuales brinden integridad, disponibilidad y confidencialidad de la información, incluyendo la protección tanto los dispositivos como de la red de comunicación de la empresa ante posibles ataques informáticos y/o filtración de algún tipo de virus

Actualmente, las PYMES son consideradas el foco principal para que suceda algún tipo de ciberataque y/o se llegue a propagar algún tipo de virus informático el cual llegue a provocar un daño bastante significativo para la empresa, es por ello que Equilibrio Farmacéutico al ser considerada como una PYME, resulta necesario implementar nuevos métodos y medidas de protección con el propósito de incrementar sus medidas y nivel de seguridad en sus tecnologías de la información, principalmente para salvaguardar su activo más importante dentro de la empresa que es la información.

DESCRIPCIÓN DE LA EMPRESA

Nombre, razón social

Equilibrio Farmacéutico S.A. de C.V.

Ubicación

Av. José López Portillo No. 53-A-Local-25, Villa de las Flores, San Francisco Coacalco, Estado de México

Organigrama

Ahora, se muestra una ilustración de cómo se encuentra actualmente el organigrama del corporativo Equilibrio Farmacéutico S.A. de C.V.

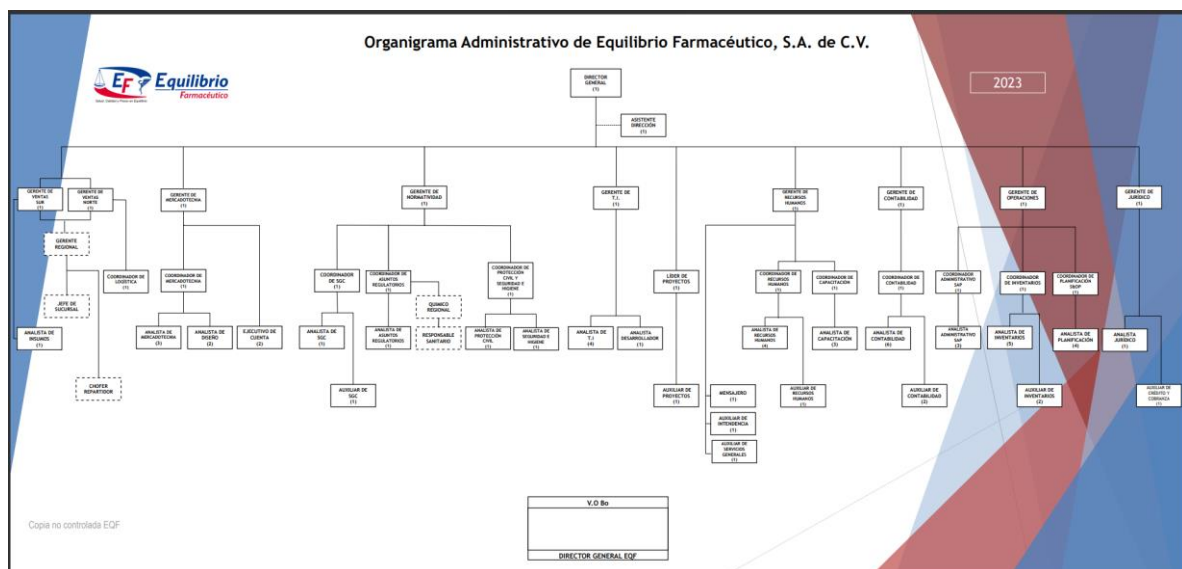


Figura 1 Organigrama Equilibrio Farmacéutico. [Equilibrio Farmacéutico, 2024]

Sector productivo de la empresa

Sector Terciario

Misión, Visión, Filosofía y/o Valores

Misión

Ofrecer al mercado mayorista y medio mayorista productos farmacéuticos de la más alta calidad a los precios más bajos, brindando siempre el mejor servicio.

Visión

Ser la empresa de comercialización farmacéutica mayorista más grande de México, siendo la mejor opción de compra por precio, variedad, calidad y servicio.

Valores

- Honestidad
- Servicio
- Responsabilidad
- Gratitude
- Respeto

Breve historia de la empresa.

Equilibrio farmacéutico es una empresa 100 mexicana que nace con el objetivo de ser la empresa de comercialización farmacéutica mayorista más grande de México. Gracias al innovador modelo de negocio que se implementa hoy día se visiona como líder en la venta al mayoreo de medicamento genérico. Hoy se tiene la capacidad de atender a más de 20 mil clientes a través de más de 80 sucursales ubicadas a lo largo y ancho del territorio nacional, trabajando de la mano con más de 150 laboratorios para ofrecer una extensa variedad de productos que hasta hoy suman más de 4000.

La calidad de los procesos y productos están garantizados debido a que funcionan y operan conforme a la Norma Oficial Mexicana. Son más de 10 años los que hacen de equilibrio farmacéutico una empresa sobresaliente en el manejo gestión y venta de medicamento genérico, la experiencia adquirida en todo este tiempo la ha consolidado como una empresa en constante crecimiento.

DESCRIPCIÓN DEL PUESTO O ÁREA DE TRABAJO

El puesto que se va a desempeñar a lo largo de las residencias profesionales es de Analista Temporal de TI, el cual se encuentra ubicado en el área de Tecnologías de la Información (TI) de Equilibrio Farmacéutico, desempeñando un papel clave en el soporte técnico tanto para el corporativo como para las sucursales. Este rol reportará directamente al Gerente de TI, bajo cuyas órdenes trabajará de manera estrecha con otros analistas del área de TI, estableciendo así una estructura jerárquica clara y fomentando la colaboración eficiente entre los miembros del equipo.

Las responsabilidades principales del Analista Temporal de TI abarcan el soporte técnico integral de los sistemas informáticos, garantizando su funcionamiento óptimo. Además, participará activamente en auditorías internas para evaluar y mejorar la seguridad, integridad y eficiencia de los sistemas de TI en toda la organización.

En cuanto a los objetivos, a corto plazo se espera que el Analista Temporal aplique sus conocimientos recién adquiridos durante la formación profesional para contribuir al equipo y adquirir experiencia práctica. A mediano plazo, se busca que este profesional innove procesos dentro del área de TI, aumentando así la eficiencia operativa y mejorando la calidad del servicio de soporte técnico. A largo plazo, se espera que el Analista Temporal de TI se desarrolle con mayor eficiencia en el campo, contribuyendo significativamente al crecimiento y la evolución de la infraestructura tecnológica de la empresa.

En términos de habilidades sociales y rasgos de personalidad, se valoran especialmente la comunicación efectiva, la capacidad de trabajo en equipo y la iniciativa. El Analista Temporal TI debe ser capaz de transmitir información técnica de manera clara y comprensible, colaborar efectivamente con otros miembros del equipo de TI y, sobre todo, demostrar proactividad al identificar oportunidades de mejora y presentar soluciones innovadoras para optimizar los procesos dentro del área de TI. Este puesto brinda una oportunidad única para el desarrollo profesional en un entorno dinámico, contribuyendo al éxito continuo de la empresa en el ámbito tecnológico.

PROBLEMA A RESOLVER

En la era digital actual, las empresas se enfrentan a una creciente dependencia de la tecnología de la información (TI) para llevar a cabo sus operaciones críticas y gestionar datos sensibles. Sin embargo, esta dependencia también conlleva un aumento en la exposición a amenazas cibernéticas que pueden tener un impacto devastador en la integridad, confidencialidad y disponibilidad de los sistemas y datos de la empresa. Las brechas de seguridad informática se han convertido en un desafío constante, y las empresas de todos los tamaños y sectores se ven afectadas por ataques cibernéticos cada vez más sofisticados.

En el entorno empresarial actual, la seguridad informática es fundamental para garantizar la protección de datos confidenciales y mantener la continuidad de las operaciones. La empresa "Equilibrio Farmacéutico" se enfrenta a desafíos significativos relacionados con la seguridad de la información en sus servicios, que pueden tener consecuencias graves si no se abordan de manera adecuada.

- **Falta de Administración de Cifrado de Discos:** La ausencia de una gestión adecuada de la encriptación de discos expone a la empresa a riesgos de pérdida de datos críticos. Sin una encriptación efectiva, los datos almacenados en dispositivos y servidores pueden ser vulnerables a accesos no autorizados y fugas de información.
- **Falta de Protección de en los aplicativos de Office 365:** La plataforma Office 365 se ha convertido en un objetivo común para ataques cibernéticos. La falta de protección adecuada puede dejar a "Equilibrio Farmacéutico" vulnerable a amenazas como el phishing, el malware y el robo de credenciales, lo que podría resultar en la pérdida de datos y la interrupción de las operaciones.
- **Falta de Análisis de Conexiones Cifradas:** La incapacidad para analizar adecuadamente las conexiones cifradas impide la detección de posibles amenazas y ataques cibernéticos que pueden ocultarse en el tráfico encriptado. Esto deja a la empresa expuesta a riesgos de malware y exfiltración de datos.
- **Falta de Monitoreo y Control de Sitios Web:** Sin una supervisión efectiva de los sitios web que se visitan desde la red de la empresa, existe el riesgo de acceder a sitios maliciosos o comprometidos. Esto puede dar lugar a la infección de sistemas y la exposición a amenazas de seguridad.

La falta de medidas de seguridad informática en estos aspectos puede tener consecuencias graves para "Equilibrio Farmacéutico". Estas consecuencias incluyen la pérdida de datos confidenciales de clientes y empleados, posibles sanciones legales y la pérdida de confianza de los clientes. Además, la interrupción de las operaciones debido a incidentes de seguridad puede resultar en pérdidas financieras significativas y daño a la reputación de la empresa.

Por lo tanto, es imperativo abordar estos problemas de seguridad informática y proponer medidas efectivas para mitigarlos. Este estudio busca analizar en detalle la situación de seguridad en "Equilibrio Farmacéutico" y recomendar soluciones específicas para fortalecer su postura de seguridad y evitar las potenciales consecuencias adversas de no hacerlo.

OBJETIVOS

Objetivo general

Realizar Análisis de riesgo de las tecnologías de la información del corporativo Equilibrio Farmacéutico S.A. de C.V. basado en el estándar ISO/IEC 17799 y otros.

Objetivos específicos

- Reconocer el entorno de Equilibrio Farmacéutico S.A. de C.V. y del área de TI, para obtener una comprensión completa de su contexto a evaluar.
 - Identificar la empresa para conocer su misión, visión, valores, sector, actividades y organigrama general.
 - Conocer el entorno del departamento de Tecnologías de la Información (TI) de la empresa, incluyendo sus actividades, objetivos y estructura organizativa.
- Analizar la información recopilada para identificar posibles vulnerabilidades y amenazas.
 - Crear formatos de encuesta, FODA y matriz de evaluación que ayudarán a recopilar datos importantes que influyen en la organización para tomar decisiones con respecto a la seguridad informática.
 - Aplicar una encuesta en el departamento de TI para detectar riesgos de seguridad informática.
 - Realizar diversos análisis FODA enfocados en el área de TI y sus servicios para evaluar la situación actual.
- Evaluar los riesgos identificados, teniendo en cuenta su nivel de impacto y probabilidad.
 - Crear una matriz de riesgos para los servicios de TI con el propósito de identificar, evaluar y priorizar riesgos que puedan afectar la prestación de estos servicios, y así asegurar su continuidad y calidad.
 - Evaluar cualitativamente los servicios de TI para el impacto y probabilidad de los escenarios de amenaza y vulnerabilidad.
 - Evaluar cuantitativamente los servicios de TI para medir otorgarle una clasificación y prioridad de atención.
 - Priorizar amenazas y vulnerabilidades en los servicios de TI.

- Revisar los controles de seguridad en el área de TI para entender su eficacia y su mejora.
- Proponer estrategias de seguridad según análisis y necesidades de la empresa.
 - Proponer estrategias de seguridad de acuerdo con las necesidades de la empresa.
- Implementar las medidas y/o estrategias de seguridad de acuerdo con las necesidades de la empresa.
 - Realizar un análisis general del antivirus y su funcionamiento, así como las ventajas del uso del antivirus Kaspersky en comparación con otros antivirus del mercado.
 - Hacer la planeación, justificación y negociación del uso del antivirus Kaspersky como nuevo método de protección de sistemas en la empresa.
 - Crear una estrategia y plan de implementación del software antivirus en los dispositivos de la corporativo y sucursales de EQF.
 - Instalar la versión empresarial del agente de Kaspersky en todos los equipos de cómputo de EQF con el propósito de asegurar su correcto funcionamiento.
 - Instalar el antivirus desde el servidor mediante una consola del mismo agente.
 - Dar seguimiento y programa de mantenimiento para validar que la actualización de la base de datos de virus se mantenga al día y en correcto funcionamiento.
 - Aplicar pruebas piloto conforme a las instalaciones del agente para verificar su correcto funcionamiento.
 - Utilizar las herramientas de control: monitoreo, políticas de restricciones, etc.
 - Instalar las políticas que brinda la herramienta conforme a las necesidades de la empresa.
 - Realizar pruebas conforme a las políticas de filtrado del agente para verificar el correcto funcionamiento.
 - Realizar la documentación respecto a la implementación del agente (antivirus) para posibles fallas de este y como resolver el conflicto.

JUSTIFICACIÓN

Dada la problemática anterior expuesta donde la empresa Equilibrio Farmacéutico S.A. de C.V. tiene problemas en la falta de administración de cifrado de discos debido a la ausencia de una gestión adecuada de la encriptación de discos lo cual expone a la empresa a riesgos de pérdida de datos críticos. Además, de una carencia de protección de los aplicativos de Office 365, ya que al no contar con una protección adecuada puede dejar a "Equilibrio Farmacéutico" vulnerable a amenazas como el phishing, el malware y el robo de credenciales, lo que podría resultar en la pérdida de datos y la interrupción de las operaciones. Por otra parte, la falta de análisis de conexiones cifradas impide la detección de posibles amenazas y ataques cibernéticos que pueden ocultarse en el tráfico encriptado. Así mismo, la ausencia de monitoreo y control de sitios web efectiva conlleva a la existencia de riesgos al acceder a sitios maliciosos o comprometidos. Esto puede dar lugar a la infección de sistemas y la exposición a amenazas de seguridad.

Por lo tanto, se requiere de una solución que permita beneficios en una correcta además de una buena administración de cifrado de discos para que los datos que se encuentren almacenados tanto en dispositivos como servidores no se encuentren vulnerables y de esta manera no se permita el ingreso no autorizado a la información. Por otro lado, al implementar una protección en los aplicativos de Office 365, de igual manera se asegura aquella información que se encuentre almacenada en la nube de cada una de las cuentas de los usuarios, además de la protección de dichos perfiles, así mismo, al tener un análisis en las conexiones cifradas brinda a Equilibrio Farmacéutico otro nivel de protección al momento de navegar en sitios web permitiendo una protección contra amenazas y control web, aunado a esto la implementación de un monitoreo y control de sitios web da una mayor seguridad y restricción a los usuarios que naveguen en internet, esto con la finalidad de no poner en riesgo los equipos con infecciones en el sistema y/o la exposición a amenazas de seguridad y por consiguiente afectar la producción de Equilibrio Farmacéutico.

Además de ventajas en los niveles de protección que se pueden brindar en los diferentes servicios con los que opera la empresa dando una mayor seguridad, de igual manera, implementar una protección de los aplicativos de Office 365 siendo una de las principales paqueterías que utiliza la empresa para sus operaciones, es esencial para

salvaguardar datos sensibles, prevenir amenazas y/o ataques cibernéticos como el phishing y el ransomware, cumplir con regulaciones de privacidad, garantizar la continuidad del negocio, y facilitar la recuperación de datos en caso de desastres. Las medidas de seguridad, como, el monitoreo continuo, control y análisis web, la protección contra la pérdida de datos y encriptación de discos, son cruciales para mantener la integridad y la disponibilidad de los recursos, además de proteger la empresa de costosos incidentes de seguridad.

CAPÍTULO II

MARCO TEÓRICO

ESTADO DEL ARTE

En la actualidad, la seguridad informática se ha convertido en un aspecto fundamental para las organizaciones de todo tipo, por ello la protección de los activos digitales y la gestión de riesgos cibernéticos son algunos de los puntos importantes para la continuidad y confiabilidad de las operaciones empresariales, así como salvaguardar la integridad de los datos.

En este contexto, el análisis de riesgo de las tecnologías de la información se perfila como una de las practicas imprescindibles, por lo que el estándar ISO/IEC 17799, junto con otros estándares y metodologías afines, se presentan como herramientas o guías fundamentales para abordar este desafío que enfrentan las organizaciones actualmente.

Según la revista Forbes México, del “2021 al 2022, México fue blanco del 66% de los ataques cibernéticos ocurridos en América Latina, provocando pérdidas de entre 3 mil y 5 mil millones de dólares por año, de acuerdo con la Asociación de Bancos de México” (Forbes México, 2023), esto da lugar a que las organizaciones pongan enfoque en la protección de sus activos de tecnologías de la información, buscando las mejores estrategias de protección contra amenazas y/o ataques cibernéticos.

Por otra parte, del mes de enero al mes de septiembre del año 2023 el Banco de México ha registrado cuatro ataques cibernéticos relevantes, los cuales han causado afectaciones hasta 67 millones 610 mil pesos. Según un reporte de El Financiero, en el primer caso de estos ataques se vulnero la información de los cajeros automáticos, el segundo caso, fue atacado un servicio de transferencias electrónicas a través de un malware, en el tercero también se vulneraron las transferencias electrónicas a través de un malware de tipo troyano y por ultimo “de la Sociedad Cooperativa de Ahorro y Préstamo se conoce que su banca por internet, sucursales, transferencias electrónicas y cajeros automáticos fueron alterados por un código malicioso de tipo ransomware” (El Financiero, 2023).

No obstante, de acuerdo con una encuesta realizada por Digital Trust Insights 2023, edición México, “revelaron que, en general, las empresas mexicanas se sienten más preparadas para afrontar y prevenir ataques cibernéticos” (PWC, 2023)³. Sin embargo, no solamente el equipo de ciberseguridad con el que cuenta una empresa debe de fortalecer sus

habilidades y estrategias para afrontar un ataque o amenaza, de igual manera se debe educar o informar a los usuarios con menos conocimientos acerca de este tema debido a que ellos principalmente son el blanco o la víctima más fácil para que los hackers puedan realizar un ciberataque con éxito.

Es por ello que actualmente se crean y desarrollan nuevas medidas así como estrategias de seguridad informática que permitan tener una protección contra cualquier tipo de amenaza, para que de esta manera las organizaciones no presenten afectaciones monetarias como las que se mencionaron anteriormente, por tal motivo Kaspersky que es una empresa de ciberseguridad privada más grande del mundo, brinda algunas sugerencias para prevenir ataques cibernéticos a nivel empresarial las cuales son: Educar al personal sobre la seguridad cibernética, cifrar y hacer copias de seguridad de los datos, realizar auditorías periódicas, tener en cuenta las brechas de datos internos, restringir los derechos de administrador, instalar un firewall, mantener el software, los dispositivos y los sistemas operativos actualizados, garantizar una directiva de contraseñas de mejores prácticas y por ultimo garantizar la protección de los endpoints (Kaspersky, 2023).

A medida que la tecnología avanza de igual manera se van presentando nuevas amenazas y en consecuencia nuevas formas de realizar ataques cibernéticos a diversas empresas, es por ello que en este año 2023 de acuerdo con el Tecnológico de Monterrey, las tendencias para confrontar estas problemáticas se centran principalmente en la Inteligencia Artificial y el aprendizaje automático, como bien se sabe actualmente la IA ha tomado más fuerza por lo que ha sido de gran ayuda para la ciberseguridad permitiendo la detección y respuesta temprana ante los ataques y/o amenazas cibernéticas, otra tendencia es la privacidad y protección de datos, hoy en día se cuentan con leyes nacionales e internacionales que brindan la protección de los datos que se encuentren almacenados en sitios web, redes sociales, aplicaciones entre otras tecnologías, siendo de gran ayuda para que las organizaciones implementen medidas más estrictas en salvaguardar la información de sus usuarios siendo este el activo más importante de todas las empresas, por último la seguridad en la nube es un tema el cual se le tiene que dar más enfoque debido a que actualmente la mayoría de las personas así como las empresas e instituciones, ya utilizan diversos servicios ligados a la nube por ende en un factor que puede ser crucial (Treviño, 2021).

Por todo lo mencionado anteriormente es muy importante que las organizaciones en México empiecen a tener medidas y estrategias de ciberseguridad en sus activos tecnológicos, además de fomentar una educación en sus empleados acerca de este tema, ya que estos principalmente son los responsables de permitir que un ataque pueda ser o no exitoso, además de estar siempre informado de aquellas nuevas amenazas y ataques que se vayan presentando para que el equipo de ciberseguridad pueda tomar las soluciones más adecuadas ante cualquier problemática que se presente.

MARCO CONCEPTUAL

Kernel

Es el corazón o núcleo de un sistema operativo el cual controla todas las funciones entre el hardware y el sistema operativo, además de gestionar los recursos de la forma más eficiente posible. “El Kernel siempre tiene la misma estructura y consta de varias capas:

- La capa más baja es la interfaz con el hardware (procesadores, memoria y dispositivos).
- Sobre ella se encuentra la gestión de la memoria, que distribuye la memoria RAM y la memoria virtual.
- La siguiente capa contiene el gestor de procesos, que se encarga de la gestión del tiempo y permite el multitasking.
- Posteriormente, el gestor de dispositivos (Device Management).
- La capa más alta es el sistema de archivos. Allí, se le asigna un espacio en la memoria principal (caché, RAM, etc.) o secundaria (disco duro, USB, etc.) a los procesos” (IONOS, 2021).

El Kernel cumple con cuatro tareas indispensables la primera de ellas es la gestión de la memoria o almacenamiento, donde administra cuanta memoria debe asignar para cada tipo de elemento y el lugar al cual será asignado dentro de la memoria. La segunda es la gestión de procesos, aquí se determina que procesos puede utilizar la Unidad Central de Procesamiento (CPU), cuando y durante cuánto tiempo. La tercera tarea consta de controlar los dispositivos en la cual se encarga de ser el intérprete entre el hardware y los procesos. Por último, recibe las llamadas al sistema además de proporcionar la seguridad.

Endpoint

Un Endpoint tiene dos tipos de significado uno más complejo que otro, el primero se entiende como Endpoint a cualquier dispositivo físico que tenga una conexión a internet ya sea un ordenador portátil, una computadora de escritorio, un smartphone o cualquier dispositivo de internet de las cosas (IoT). Por otro lado, un Endpoint puede ser una URL de

alguna API o un backend que se encargue de contestar alguna petición. “Los endpoints concretan los puntos a los que las APIs pueden acceder para conseguir recursos y ayudan a garantizar el funcionamiento correcto del software en el que se encuentran.” (Channel Partner, 2023).

Es importante aprender a diferenciar entre un antivirus, un firewall y un Endpoint, debido a que algunas empresas dedicadas a la ciberseguridad brindan servicios de antivirus agregando el nombre de endpoint, ejemplo de ello es Kaspersky que brinda un antivirus llamado “Endpoint Security”, sin embargo, el antivirus es el que brinda la protección a los Endpoints además de proteger todo el sistema de una red corporativa. Por otro lado, el firewall es otra medida de protección a los Endpoint ya que ayudan a filtrar el tráfico que puede resultar peligroso para una organización, además de que los Endpoint no solo se ocupan de filtrar la red, sino que también monitorean la seguridad de los dispositivos finales. (Acces Quality, 2020).

Ataque cibernético o ciberataque

Un ciberataque es un intento de malicioso por parte de un individuo o una organización para interrumpir las operaciones o el sistema de información comúnmente de otras organizaciones con la finalidad de obtener una recompensa monetaria hacia la parte que realizó este ataque. Por lo general, también se le conoce como ataque cibernético al robo, modificación, secuestro, exposición o destrucción de información que sea importante para una organización o individuo, que de igual manera el atacante busca obtener algún tipo de beneficio.

De acuerdo con Oracle, “las PYME se ven más afectadas por los ciberataques que las grandes empresas porque son más vulnerables, especialmente las empresas de comercio electrónico que poseen datos sensibles” (Oracle España, s.f.)

Existen diversos tipos de ciberataques, entre los que más destacan actualmente son los siguientes:

- **Troyano de puerta trasera:** Este tipo de ataque crea una vulnerabilidad en el sistema de la víctima, lo que permite al atacante obtener un control remoto y casi total. Los atacantes pueden usar el troyano para otros delitos cibernéticos.
- **Denegación de servicios (DoS):** Los ataques DoS y de denegación de servicio distribuida (DDoS) inundan los recursos de un sistema, impidiendo las respuestas a las solicitudes de servicio, provocando la reducción de la capacidad del sistema para funcionar.
- **Inyección de SQL:** Este tipo de ataque incorpora código malicioso en aplicaciones vulnerables, lo que genera resultados de consultas en la base de datos de backend y ejecuta comandos o acciones similares que el usuario no solicitó. (IBM, s.f.)

Malware

Se entiende como malware a todo tipo de código malicioso capaz de poder dañar, infectar o acceder a un dispositivo, sistema o red de comunicación. Este tipo de códigos son utilizados principalmente por los atacantes o también llamados hackers con la intención de poder extraer algún tipo de información o datos de los cuales puedan sacar algún beneficio el cual la mayoría de las veces es por una cantidad sumamente monetaria.

Según McAfee, “el malware ha encontrado varios métodos de ataque. Entre ellos se encuentran los archivos adjuntos al correo electrónico, los anuncios maliciosos en sitios populares, las instalaciones de software falso, las unidades USB infectadas, las aplicaciones infectadas, los correos electrónicos con phishing e incluso los mensajes de texto.” (McAfee, s.f.)

Hay que tomar en cuenta que un virus no es exactamente lo mismo que un malware, debido a que no todos los tipos de malware son virus. Por un lado, el malware es un código malicioso, mientras que un virus son solo un tipo de malware. En específico, los virus informáticos son código malicioso que se extiende por equipos y redes. (Avast, s.f.).

Ransomware

El ransomware es un tipo de malware de rescate o secuestro, el cual impide a los usuarios poder acceder a su equipo o a su información la cual tenga almacenada, esto de igual manera aplica para los servidores de las organizaciones los cuales son los principales objetivos de este tipo de ataques. La principal finalidad del ransomware es bloquear el acceso a los dispositivos y/o información y pedir una recompensa a cambio del acceso, dicha recompensa actualmente se pide en criptomonedas o tarjetas de crédito.

Hay diferentes tipos de ataques de ransomware uno de los más comunes son los correos electrónicos con phishing en el cual manipulan a los usuarios para que puedan descargar y ejecutar un archivo que contenga algún tipo de código malicioso, también los que aprovechan las vulnerabilidades del sistema operativo y del software para poder inyectar código malicioso en un dispositivo o red de comunicación, de igual manera existe el robo de credenciales en el cual se extraen los datos de dichas credenciales para que los atacantes puedan acceder a un dispositivo o cuenta de algún usuario y poder ejecutar directamente este tipo de malware. (IBM, s.f.).

Troyano

El virus troyano es un tipo de malware capaz de disfrazarse de un programa legítimo para que de esta manera pueda obtener el acceso dentro del sistema de los usuarios. Sin embargo, para que este tipo de virus pueda realizar su tarea con la que fue desarrollado es importante que el usuario descargue y ejecute un archivo el cual puede parecer legítimo, pero es todo lo contrario debido a que puede contener este tipo de malware. Como se mencionó anteriormente la forma más común de que un usuario se infecte de este tipo de virus es a través de un correo electrónico y posteriormente que descargue el archivo.

Ejemplo de ello, es cuando “un usuario puede recibir un correo electrónico de alguien que conoce, con un archivo adjunto que también parece legítimo. Sin embargo, el adjunto contiene código malicioso que ejecuta e instala el troyano en el dispositivo. El usuario a menudo no sabrá que se produjo un hecho desafortunado, ya que puede que su computadora siga funcionando normalmente, sin signos de infección.” (Fortinet, s.f.).

Phishing

Es una técnica que consiste en enviar un correo electrónico el cual puede parecer legítimo ya que este puede contener algún logotipo de una empresa o algún tipo de información que suplante la identidad de alguna organización o persona, además de ello suelen tener errores gramaticales, incluso transmiten un mensaje de urgencia o miedo para que el destinatario tome la máxima atención a dicho correo.

Este tipo de correos electrónicos suelen venir acompañados de un enlace a un sitio web el cual le va a pedir al usuario que ingrese sus datos principalmente es información de cuentas bancarias como su número de tarjeta de crédito, DNI, la contraseña de acceso a la banca online, etc. Además de ello, algunos correos de este tipo pueden contener archivos adjuntos los cuales suelen venir acompañados de códigos maliciosos dando lugar a algún tipo de ciberataque.

Sandboxing

El Sandboxing es un entorno de pruebas aislado dentro del sistema para poder ejecutar algún tipo de código el cual no esté del todo perfeccionado y así este pueda realizar diversas acciones o tareas las cuales puedan hacer algún tipo de daño en el hardware, por lo tanto, la finalidad del Sandboxing es proteger el hardware al igual que el sistema operativo de algún código erróneo o malware.

Por ejemplo, “imagina que estás abriendo un programa o ejecutando una unidad externa en un entorno de espacio aislado. Si este programa ya está infectado, el malware, como un virus, puede propagarse al resto de tu computadora. Sin embargo, esto no sucederá si utilizamos la técnica del Sandboxing” (gtd Perú, s.f.). Por lo tanto, si se detecta alguna amenaza que se esté ejecutando en este entorno aislado solamente habrá afectaciones ahí y el sistema operativo real al igual que el hardware no presentara ningún tipo de afectación. Es por ello que el Sandboxing se presenta como una medida de seguridad preventiva ante un ataque de un virus.

Firewall

Los firewalls son programas (software) o dispositivos (hardware) que se encargan de filtrar, examinar y controlar el tráfico generado en la red, comúnmente los firewalls son la primera medida de seguridad empleada para evitar algún ataque cibernético que se pueda presentar y de esta manera se pueda obtener una conexión a una red de forma segura.

Como se mencionó, existen dos tipos de firewall los de software y los de hardware. “El enrutador (a veces denominado "módem") que lleva internet de su proveedor de Internet a su casa u oficina suele ser un firewall de hardware. Y su equipo, ya sea que esté ejecutando Windows o macOS, lo más probable es que tenga un firewall de software ejecutándose.” (Microsoft, s.f.). Sin embargo, los firewalls de hardware solo protegen los dispositivos que se encuentren cerca de este, por lo que si un usuario se conecta a una red pública su dispositivo quedara desprotegido, de lo contrario deberá de tener un firewall de software para que pueda brindarle la protección cuando se realice la conexión a una red pública.

Cifrado de discos duros

Es cifrado de discos duros es una medida de protección para la información que este almacenada dentro de ellos. El cifrado de discos es un proceso el cual se realiza mediante algoritmos matemáticos el cual modifica la información de tal manera que una persona que acceda a ella de forma no autorizada no la pueda leer debido a que esta se encontrara de una manera no legible. Por lo tanto, el usuario deberá de proporcionar una contraseña o huella digital para poder descifrar la información o para poder tener acceso a ella.

Existen diversos softwares que ayudan a poder realizar este proceso de cifrado de discos duros, de igual manera algunos de ellos brindan la administración de dicho cifrado. Por ejemplo, en el sistema operativo de Windows se cuenta con un cifrado de unidad BitLocker la cual es una característica diseñada para proteger los datos proporcionando cifrado para volúmenes completos (Microsoft, 2023).

Conexiones Cifradas

Una conexión cifrada, es una conexión que tiene protección durante la transferencia de datos o información entre un dispositivo y un servidor a través de internet a algún medio de comunicación, garantizando que la información este protegida en dado caso que sea interceptada por algún atacante.

Actualmente se cuenta con un certificado SLL (Secure Sockets Layer), que es “una tecnología de encriptación que crea una conexión segura entre el servidor de una web y el navegador del usuario que visita la página. Esta conexión cifrada permite que la información que se transmite entre ambos esté protegida en todo momento” (Kallos, 2018).

MARCO METODOLÓGICO

En este apartado se abordan los estándares (Normas ISO) a utilizar durante el desarrollo del proyecto además de las actividades que se van a realizar, mencionando las herramientas que se van a utilizar, las técnicas que se implementan y el objetivo que se busca obtener para cada una de estas actividades, además de ello se presenta una gráfica de Gantt donde se muestran los tiempos de desarrollo para cada una de las actividades.

ISO/IEC 17799

La norma ISO/IEC 17799, es una estándar internacional que aborda los requisitos necesarios para poder llevar a cabo la implementación de un buen Sistema de Gestión de Seguridad de la Información (SGSI), lo cual ayuda a mantener a salvo la información además de los dispositivos que la almacenan, ante cualquier amenaza ya sea de manera física o lógica, de igual manera ayuda a las organizaciones a implementar medidas de seguridad las cuales son muy importantes en la actualidad.

Esta norma va orientada a tres principales principios para la seguridad de la información los cuales son:

- **Confidencialidad:** lo cual indica que solo el personal autorizado puede acceder a la información la cual le corresponde.
- **Integridad:** esto asegura y garantiza que la información no sea alterada, eliminada o destruida por personas no autorizadas o que sean externas de la organización.
- **Disponibilidad:** en donde se asegura que aquellos usuarios que sean autorizados puedan acceder a la información en el momento que ellos decidan y la requieran.

“La ISO 17799 no es una norma tecnológica, ha sido redactada de forma flexible independiente de cualquier solución de seguridad específica y proporciona buenas prácticas neutrales con respecto a la tecnología y a las soluciones disponibles en el mercado. Estas características posibilitan su implantación en todo tipo de organizaciones, sin importar su tamaño o sector de negocio” (Richard, 2016).

ISO/IEC 27001

La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual puede ser aplicado para las PYMES y grandes empresas. Una de las principales características y la cual añade un gran valor de seguridad para las empresas, es que se puede tener una certificación de dicha norma o estándar. Al igual que la norma ISO/IEC 17799, esta ISO también busca preservar los tres principales servicios para la seguridad de la información que es la confidencialidad, integridad y disponibilidad.

Este estándar brinda controles de seguridad “los cuales se dividen ahora en cuatro grandes grupos:

- Controles organizacionales, con 37 controles enfocados en la seguridad administrativa y las políticas de seguridad de la información.
- Controles de personas, que agrupa a 8 controles orientados a la protección de la Seguridad de la Información en lo que respecta capital humano de la organización.
- Controles físicos, con 14 controles orientados a la instalación e infraestructura IT de la empresa.
- Controles tecnológicos, con 34 controles enfocados en aspectos como autenticación, cifrado y otras materias tecnológicas no relacionadas con las instalaciones físicas o la infraestructura.” (ISO Tools Excellence, s.f.)

Cuadro Metodológico Integral para el Desarrollo del Proyecto

El cuadro metodológico integral que se presenta a continuación aborda cada una de las actividades a desarrollar a lo largo del proyecto, además de indicar las técnicas y herramientas que se van a utilizar para poder realizar cada una de estas actividades, y finalmente la meta que se va a obtener al culminar con dicha actividad.

Tabla 1 Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Elaboración propia].

Actividades	Técnicas	Herramientas	Metas
1.1 Identificar la empresa para conocer su misión, visión, valores, sector, actividades y organigrama general.	Investigación del contexto de la empresa. Recopilación de información.	Internet. Procesador de textos (Word).	Conocer el entorno de la empresa Equilibrio Farmacéutico S.A. de C.V.
1.2 Conocer el entorno del departamento de Tecnologías de la Información (TI) de la empresa, incluyendo sus actividades, objetivos y estructura organizativa.	Investigación del contexto del área de TI dentro de la empresa. Recopilación de información.	Entrevista. Procesador de textos (Word).	Entender el papel que juega el área de TI dentro de la organización.
2.1 Crear formatos de encuesta, FODA y matriz de evaluación que ayudarán a recopilar datos importantes que influyen en la organización para tomar decisiones con respecto a la seguridad informática.	Investigar elaboración de formatos. Elaborar formato de encuesta Elaborar formatos FODA's Elaborar formatos de matriz de evaluación	Procesador de textos (Word).	Obtener los formatos adecuados que serán aplicados a los datos que se recopilarán posteriormente.
2.2 Aplicar una encuesta en el departamento de TI para detectar riesgos de seguridad informática.	Aplicar encuesta al área de TI	Plataforma para aplicar encuestas (Google Forms)	Obtener información que sea interés para realizar un posterior análisis.

Tabla 1 Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Elaboración propia].

Actividades	Técnicas	Herramientas	Metas
2.3 Realizar diversos análisis FODA enfocados en el área de TI y sus servicios para evaluar la situación actual.	Aplicar e identificar la información recabada en las encuestas.	Procesador de textos (Word).	Analizar la información recabada en las encuestas y clasificarla de acuerdo con los FODA's para identificar las oportunidades de seguridad en el negocio.
3.1 Crear una matriz de riesgos para los servicios de TI con el propósito de identificar, evaluar y priorizar riesgos que puedan afectar la prestación de estos servicios, y así asegurar su continuidad y calidad.	Investigar cómo realizar una matriz de riesgo. Aplicar el formato de la matriz de riesgo.	ISO 27001:2005. Procesador de textos (Word).	Identificar, evaluar y priorizar los riesgos que puedan afectar a los servicios utilizados en la organización.
3.2 Evaluar cualitativamente los servicios de TI para el impacto y probabilidad de los escenarios de amenaza y vulnerabilidad.	Realizar una evaluación a los servicios de TI.	ISO/IEC 17799. ISO 27001:2005. Procesador de textos (Word).	Obtener un análisis del impacto y probabilidad de las amenazas y vulnerabilidades en un punto de vista cualitativo.
3.3 Evaluar cuantitativamente los servicios de TI para medir otorgarle una clasificación y prioridad de atención.	Realizar una evaluación a los servicios de TI.	ISO/IEC 17799. ISO 27001:2005. Procesador de textos (Word).	Clasificar los servicios de TI para priorizar la atención en base a un punto de vista cuantitativo.
3.4 Priorizar amenazas y vulnerabilidades en los servicios de TI.	Definir las vulnerabilidades y amenazas.	Procesador de textos (Word).	Priorizar y atender problemáticas de amenazas y vulnerabilidades en los servicios de TI.

Tabla 1 Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Elaboración propia].

Actividades	Técnicas	Herramientas	Metas
3.5 Revisar los controles de seguridad en el área de TI para entender su eficacia y su mejora.	Investigar los controles de seguridad. Realizar pruebas de testeo para verificar su funcionamiento.	Antivirus instalados.	Verificar que las medidas de seguridad implementadas en la organización funcionen de manera correcta o de lo contrario implementar otras estrategias de seguridad.
4.1 Proponer estrategias de seguridad de acuerdo con las necesidades de la empresa.	Investigar posibles medidas de seguridad dentro de las normas. Realizar propuestas de seguridad en base a las necesidades de la empresa.	ISO/IEC 17799. ISO 27001:2005. Procesador de textos (Word).	Realizar propuestas para implementar nuevas medidas de seguridad de acuerdo con las necesidades de la empresa y fundamentadas con las normas ISO 17799 y otros.
5.1 Realizar un análisis general del antivirus y su funcionamiento, así como las ventajas del uso del antivirus Kaspersky en comparación con otros antivirus del mercado.	Investigación acerca de antivirus. Recopilación bibliográfica	Procesador de textos (Word). Internet.	Identificar las principales ventajas de seguridad que brinda Kaspersky a comparación de otros antivirus mediante una recopilación de información,
5.2 Hacer la planeación, justificación y negociación del uso del antivirus Kaspersky como nuevo método de protección de sistemas en la empresa.	Planeación. Justificación. Negociación.	Entrevista. Procesador de textos (Word)	Realizar una negociación en la organización para la implementación del nuevo Antivirus como principal protección de seguridad.
5.3 Crear una estrategia y plan de implementación del software antivirus en los dispositivos de EQF.	Estrategias y plan de implementación.	Entrevista. Procesador de textos (Word).	Obtener estrategias y un plan de implementación de software Kaspersky en dispositivos de EQF.

Tabla 1 Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Elaboración propia].

Actividades	Técnicas	Herramientas	Metas
5.4 Instalar la versión empresarial del agente de Kaspersky en todos los equipos de cómputo de EQF con el propósito de asegurar su correcto funcionamiento.	Instalar el software de Kaspersky.	Software de Kaspersky.	Instalar el agente de Kaspersky en los dispositivos de EQF.
5.5 Instalar el antivirus desde el servidor mediante una consola del mismo agente.	Instalar el software de Kaspersky.	Software de Kaspersky. TeamViewer.	Instalar el agente de Kaspersky en los dispositivos restantes de EQF de manera remota a través de TeamViewer.
5.6 Dar seguimiento y programa de mantenimiento para validar que la actualización de la base de datos de virus se mantenga al día y en correcto funcionamiento.	Observación. Validación.	Antivirus de Kaspersky	Validar que la base de datos de virus en Kaspersky este actualizada en base a los ataques y/o virus, además de verificar que funcione correctamente.
5.7 Aplicar pruebas piloto conforme a las instalaciones del agente para verificar su correcto funcionamiento.	Observación Validación Pruebas	Antivirus de Kaspersky	Aplicar pruebas de seguridad para validar que el antivirus funcione de manera correcta.
5.8 Utilizar las herramientas de control: monitoreo, políticas de restricciones, etc.	Investigación Recopilación bibliográfica Utilizar herramientas de control.	Herramientas del antivirus Kaspersky	Implementar un control de monitoreo, políticas de restricciones, entre otras medidas de control, de acuerdo a una previa investigación del uso de las herramientas de control que brinda Kaspersky.

Tabla 1 Cuadro Metodológico Integral para el Desarrollo del Proyecto. [Elaboración propia].

Actividades	Técnicas	Herramientas	Metas
5.9 Instalar las políticas que brinda la herramienta conforme a las necesidades de la empresa.	Investigación. Recopilación de información. Implementar políticas de restricciones.	Entrevista. Antivirus de Kaspersky.	Conocer las restricciones de navegación de internet para implementar políticas de restricción en base a las necesidades de la empresa.
5.10 Realizar pruebas conforme a las políticas de filtrado del agente para verificar el correcto funcionamiento.	Pruebas de funcionamiento.	Antivirus de Kaspersky.	Validar que las pruebas de restricción implementadas funcionen de manera correcta.
5.11 Realizar la documentación respecto a la implementación del agente (antivirus) para posibles fallas de este y como resolver el conflicto.	Recopilación de información. Realizar documentación del proyecto.	Procesador de textos (Word).	Obtener la documentación de la implementación del proyecto.

Gráfica de Gantt

A continuación, se presenta una gráfica de Gantt la cual contiene cada una de las actividades que se van a realizar a lo largo del proyecto, además de ello se presentan los tiempos que van a abarcar cada una de dichas actividades para su elaboración. Cada periodo de tiempo se establece de acuerdo al nivel de complejidad de cada una de las actividades.

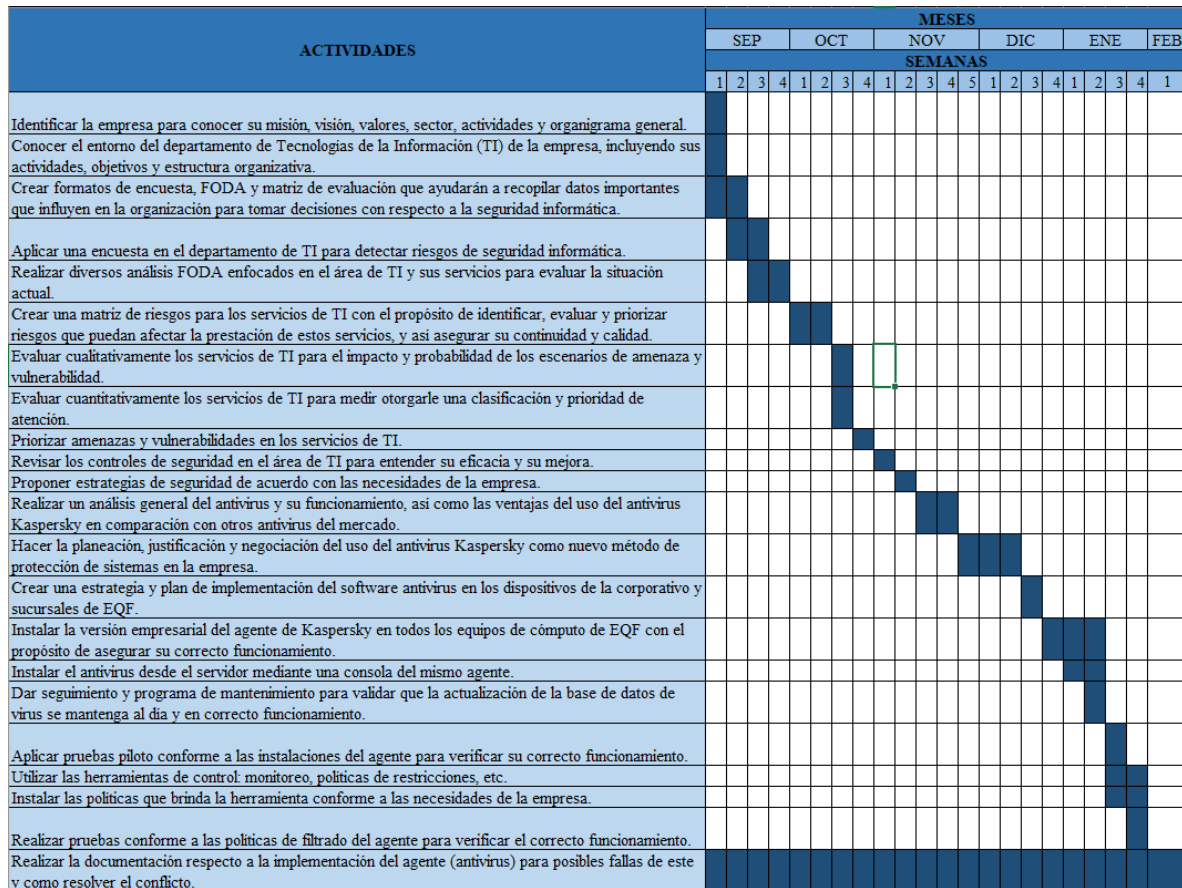


Figura 2 Gráfica de Gantt de las actividades a desarrollar. [Elaboración propia]

Para el desarrollo del presente proyecto se toman en cuenta varios aspectos que se consideran importantes entre ellos se debe de contar con una población que será de gran ayuda para aplicar algunas técnicas de estudio como las encuestas, además de una población se debe tomar una muestra de esta misma para poder realizar algún tipo de análisis de la información recabada en estudios que sean aplicados, para ello se puede tomar como muestra el total de la población o algún porcentaje de esta. Posteriormente, se menciona cuáles son los tipos de instrumentos que se van a utilizar a lo largo del proyecto para recabar información que sea de gran relevancia para así poder hacer la parte del análisis de datos el cual se va a

realizar con la ayuda de diversas técnicas, herramientas e incluso los mismos estándares (Normas ISO) que serán de gran importancia para dar la mejor solución a las problemáticas encontradas.

Población

La población principalmente se centra en los empleados del área de TI, que cuenta con un total de 6 empleados distribuidos de la siguiente manera:

- 1 gerente de TI
- 4 analistas de TI
- 1 analista de Desarrollo

Muestra

Para realizar la recolección y análisis de los datos se utiliza a la población total, debido a que la cantidad es bastante considerable para hacer el manejo y/o manipulación de la información que se va a ver reflejada, además de que la población utilizada para realizar dicho análisis de cómo se encuentra la situación actual de la empresa es la más adecuada y la que puede brindar información más concisa.

Instrumentos de recolección de información

El instrumento principal que se utiliza en el desarrollo de este proyecto para hacer la recolección de información es una encuesta la cual va a contener las preguntas necesarias para obtener un mayor conocimiento acerca de las medidas y/o estrategias de la seguridad informática que se tiene en la organización, así como aquellas amenazas que se han presentado y la forma en la que han dado solución ante este tipo de problemas.

Análisis de Datos

Para realizar el análisis y tratamiento de la información recabada se utilizan diversos instrumentos como FODA's, matrices de riesgos, evaluaciones cualitativas y cuantitativas, cada uno de ellos ayuda a dar un enfoque distinto a la información para poder identificar los

puntos positivos y negativos que se tengan en la organización en cuanto a su seguridad informática.

Por otra parte, se toma como referencia algunos estándares como la ISO 17799 que es una guía para las buenas prácticas de la gestión de seguridad informática, debido a que contiene algunos consejos, así como recomendaciones que se pueden implementar para salvaguardar la información de la mejor manera, además de este estándar se pretende consultar otros de ellos enfocados a la gestión de la seguridad informática, dando así la mejor solución ante las problemáticas que se vean reflejadas en la protección de la información con la que cuenta la organización.

CAPÍTULO III

DESARROLLO

Objetivo 1. Reconocer el entorno de Equilibrio Farmacéutico S.A. de C.V. y del área de TI, para obtener una comprensión completa de su contexto a evaluar.

El objetivo se enfoca en la identificación y análisis del entorno de Equilibrio Farmacéutico S.A. de C.V., además de realizar un reconocimiento en el departamento de TI. Esta actividad va orientada a obtener una comprensión completa del contexto empresarial y tecnológico en el que opera la organización. Esto incluye conocer la misión, visión, valores y estructura organizacional tanto de la empresa como del área de TI, además de saber cuáles actividades se realizan por ambas partes.

Actividad 1.1. Identificar la empresa para conocer su misión, visión, valores, sector, actividades y organigrama general.

Descripción de la actividad

Para el desarrollo de esta actividad se realiza una investigación a través del portal de la Equilibrio Farmacéutico con el propósito de obtener una comprensión integral de su naturaleza y funcionamiento. Durante el proceso, se busca identificar su misión, visión y valores, que son los fundamentos que orientan su dirección estratégica y su propósito a largo plazo.

Además de investigar el sector en el que la empresa opera. Esto permite contextualizar su posición en el mercado y comprender las dinámicas que impactan su desempeño. También se aborda la estructura organizativa de la empresa mediante la elaboración de un organigrama general. Este organigrama proporciona una visión clara de la jerarquía y la distribución de responsabilidades en la organización.

Resultado de la actividad

Nombre, razón social: Equilibrio Farmacéutico S.A. de C.V.

Ubicación: Av. José López Portillo No. 53-A-Local-25, Villa de las Flores, San Francisco Coacalco, Estado de México

- A continuación, se muestra una ilustración de cómo se encuentra actualmente el organigrama de la organización.

- Gratitude
- Respeto

Breve historia de la empresa.

Equilibrio farmacéutico es una empresa 100 mexicana que nace con el objetivo de ser la empresa de comercialización farmacéutica mayorista más grande de México. Gracias al innovador modelo de negocio que se implementa hoy día se visiona como líder en la venta al mayoreo de medicamento genérico. Hoy se tiene la capacidad de atender a más de 20 mil clientes a través de más de 80 sucursales ubicadas a lo largo y ancho del territorio nacional, trabajando de la mano con más de 150 laboratorios para ofrecer una extensa variedad de productos que hasta hoy suman más de 4000.

La calidad de los procesos y productos están garantizados debido a que funcionan y operan conforme a la Norma Oficial Mexicana. Son más de 10 años los que hacen de equilibrio farmacéutico una empresa sobresaliente en el manejo gestión y venta de medicamento genérico, la experiencia adquirida en todo este tiempo la ha consolidado como una empresa en constante crecimiento.

Actividad 1.2. Conocer el entorno del departamento de Tecnologías de la Información (TI) de la empresa, incluyendo sus actividades, objetivos y estructura organizativa.

Descripción de la actividad.

Esta actividad implica conocer el departamento de Tecnologías de la Información (TI) de la empresa para obtener una comprensión completa de su entorno operativo. Por ello, se realiza una entrevista a un empleado de dicha área la cual abarca puntos como las actividades que realiza el departamento, sus objetivos específicos y su estructura organizativa.

Posteriormente, identificar las actividades clave de TI que respaldan las operaciones de la empresa. Estas actividades pueden incluir la gestión de infraestructura tecnológica, el soporte técnico, el desarrollo de software, la seguridad informática y otras funciones cruciales.

Resultado de la actividad.

El área de TI es un área dedicada a brindar apoyo y dar solución a los problemas existentes en las sucursales de Equilibrio Farmacéutico, especialmente en el área de Tecnología.

Ofrece un servicio enfocado a resolver problemas de nivel hardware y software que comprenden los principales aspectos básicos o de complejidad en reparación y mantenimiento de equipos informáticos.

Objetivo del área. El objetivo del área es mantener el control y la estabilidad de cada una de las sucursales de Equilibrio Farmacéutico para sus optimas funciones tanto en producción y ventas dando el soporte completo en lo tecnológico, seguridad y transferencia de información.

Actividades desarrolladas en el área de TI.

- Dar soporte técnico al corporativo y sucursales.
- Realizar mantenimiento a equipos de cómputo e infraestructura.
- Seguimiento de instalaciones y/o actualizaciones de software.
- Desarrollo de software.
- Seguimiento de sistemas y alarmas de seguridad.
- Monitoreo de cámaras de seguridad.

Organigrama.

La figura que se presenta en seguida muestra cómo se encuentra actualmente el organigrama del área de TI de Equilibrio Farmacéutico.



Figura 4 Organigrama del área de TI [Equilibrio Farmacéutico,2024]

Objetivo 2. Analizar la información recopilada para identificar posibles vulnerabilidades y amenazas.

El objetivo se enfoca en la fase de análisis de la información recopilada con el propósito de identificar aquellas posibles debilidades y amenazas que puedan poner en riesgo la seguridad de la información en la organización. Durante esta etapa se busca descubrir todas las amenazas, así como las vulnerabilidades con la ayuda de diversos instrumentos de recolección de datos, además de realizar un análisis de la información reflejada en dichos instrumentos, este análisis es esencial para implementar posteriormente medidas y/o estrategias de seguridad.

Actividad 2.1. Crear formatos de encuesta, FODA y matriz de evaluación que ayudarán a recopilar datos importantes que influyen en la organización para tomar decisiones con respecto a la seguridad informática.

Descripción de la actividad

En esta actividad se realizan tres formatos: Encuesta, análisis FODA y matrices de evaluación, estos formatos son esenciales para la recopilación de información de datos que

serán de suma importancia en el desarrollo del proyecto, buscando aquellas oportunidades y fortaleciendo las medidas de seguridad que ya se tengan implementadas.

La encuesta sirve como herramienta para obtener información acerca de los servicios y operaciones de la organización, así como de la seguridad que se tiene implementada. El análisis FODA es un recuadro el cual permite identificar aquellos factores internos y externos que pueden influir en la seguridad informática de la organización. Por ultimo las matrices de evaluación sirven para evaluar cuales riesgos resultan más significativos para la empresa y de esta manera determinar su nivel de prioridad.

Resultado de la actividad

Formato de encuesta.

Para desarrollar las preguntas de esta encuesta se consideran los siguientes temas a tratar en la seguridad informática de Equilibrio Farmacéutico: Protección de servicios, Softwares de protección, medidas de seguridad y ataques ocurridos en la empresa.

El propósito de la encuesta es recopilar información que sea de suma importancia para identificar las principales problemáticas y mejorar la seguridad de la información con la que actualmente se cuenta. A continuación, se muestran las preguntas para la aplicación de la encuesta en el área de TI.

Niveles de Seguridad en Software de Equilibrio Farmacéutico

Pregunta 1. ¿Tiene conocimientos de medidas de seguridad informática implementadas en la organización?

- a) SI
- b) NO

Pregunta 2. Si la respuesta anterior fue “SI”, ¿conoce cuáles son esas medidas de seguridad informática?

Respuestas: Abiertas

Pregunta 3. En base a la siguiente escala considera que la seguridad informática implementada es:

- a) Mala
- b) Regular
- c) Buena
- d) Excelente

Pregunta 4. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Abiertas

Pregunta 5. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) SI
- b) NO

Pregunta 6. Si la respuesta anterior fue “SI” ¿qué medida de seguridad recomienda?

Respuestas: Abiertas

Protección de las tecnologías utilizadas en Equilibrio Farmacéutico.

Pregunta 7. ¿Qué tipo de servicios son los que utiliza en Equilibrio Farmacéutico para desempeñar sus actividades?

- a) Paquetería Office 365
- b) Aplicación SAP
- c) Teams
- d) TeamViewer
- e) Legado
- f) Correo electrónico
- g) La nube
- h) Todos los anteriores.

Protección de correo electrónico (Outlook)

Pregunta 8. En cuanto al servicio de correo electrónico (Outlook), ¿cuentan con medidas de seguridad informática?

- a) SI
- b) NO

Pregunta 9. Si la respuesta anterior fue “SI”, ¿cuáles son esas medidas de seguridad informática?

Respuestas: Abiertas

Pregunta 10. En base a la siguiente escala considera que la seguridad informática implementada en los servicios es:

- a) Mala
- b) Regular
- c) Buena
- d) Excelente

Pregunta 11. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Abiertas

Pregunta 12. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) SI
- b) NO

Pregunta 13. Si la respuesta anterior fue SI ¿qué medida de seguridad recomienda?

Respuestas: Abiertas

Protección de servicio en la nube

Pregunta 14. En cuanto al servicio en la nube (OneDrive), ¿cuentan con medidas de seguridad informática?

- a) SI
- b) NO

Pregunta 15. Si la respuesta anterior fue “SI”, ¿cuáles son esas medidas de seguridad informática?

Respuestas: Abiertas

Pregunta 16. En base a la siguiente escala considera que la seguridad informática implementada en los servicios es:

- a) Mala
- b) Regular
- c) Buena
- d) Excelente

Pregunta 17. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Abiertas

Pregunta 18. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) SI
- b) NO

Pregunta 19. En caso de ser así, ¿qué medida de seguridad recomienda?

Respuestas: Abiertas

Protección de aplicativo Teams

Pregunta 20. En cuanto al aplicativo Teams, ¿cuentan con medidas de seguridad informática?

- a) SI
- b) NO

Pregunta 21. En caso de ser así, ¿cuáles son esas medidas de seguridad informática?

Respuestas: Abiertas

Pregunta 22. En base a la siguiente escala considera que la seguridad informática implementada en los servicios es:

- a) Mala
- b) Regular
- c) Buena
- d) Excelente

Pregunta 23. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Abiertas

Pregunta 24. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) SI
- b) NO

Pregunta 25. Si la respuesta anterior fue SI ¿qué medida de seguridad recomienda?

Respuestas: Abiertas

Políticas de restricción

Pregunta 26. ¿Existen políticas de uso de sitios web y/o plataformas de streaming (Spotify, Netflix, etc.)?

- a) SI
- b) NO

Pregunta 27. En caso de ser así, ¿Se cumplen adecuadamente estas reglas?

- a) Siempre
- b) Casi siempre
- c) A veces
- d) Rara vez
- e) Nunca

Pregunta 28. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Abiertas

Pregunta 29. ¿Recomienda que se implementa alguna otra política de restricción sobre el uso sitios web y/o plataformas de streaming (Spotify, Netflix, etc.)?

- a) SI
- b) NO

Pregunta 30. En caso de ser así, ¿qué políticas de restricción recomienda?

Respuestas: Abiertas

Software de protección utilizados en Equilibrio Farmacéutico.

Pregunta 31. ¿Tiene instalado un software de protección (antivirus) en los dispositivos de la empresa?

- a) SI
- b) NO

Pregunta 32. ¿Considera que el antivirus cubre todas las necesidades de la empresa?

- a) Totalmente
- b) Casi todas
- c) Algunas
- d) Ninguna

Pregunta 33. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Abiertas

Acontecimientos de ataques informáticos

Pregunta 34. ¿La empresa ha sido víctima de algún ataque informático?

- a) SI
- b) NO

Pregunta 35. En caso de ser así, ¿Qué tipo de ataque o ataques informáticos ocurrieron?

Respuestas: Abiertas

Pregunta 36. ¿Cómo enfrentaron ese tipo de ataques informáticos?

Respuestas: Abiertas

Pregunta 37. Actualmente, ¿cuentan con medidas o estrategias de seguridad informática para combatir ese tipo de ataques?

- a) SI

b) NO

Pregunta 38. En caso de ser así, ¿Qué tipo de medidas de seguridad se implementaron para enfrentar los ciberataques?

Respuestas: Abiertas

Pregunta 39. ¿Cómo considera que son actualmente esas medidas de seguridad implementadas?

- a) Excelente
- b) Buena
- c) Regular
- d) Mala

Pregunta 40. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Abiertas

Afectaciones en Equilibrio Farmacéutico

Pregunta 41. ¿La empresa sufrió algún tipo de afectación al ser víctima de ataques?

- a) SI
- b) NO

Pregunta 42. En caso de ser así, ¿de qué forma se vio afectada?

Respuestas: Abiertas

Pregunta 43. ¿Tuvo afectaciones económicas cuando sucedieron esos ataques informáticos?

- a) SI
- b) NO

Pregunta 44. ¿Cómo considera que fueron esas afectaciones económicas?

- a) No Hubo
- b) Pocas

- c) Significativas
- d) Altas
- e) Severas

Formato de análisis FODA

A continuación, se presenta el formato que se va a utilizar para realizar el análisis FODA, en dicho formato se cambia la versión de su contenido de acuerdo con la información obtenida en la encuesta que será aplicada posteriormente.

FORTALEZAS	DEBILIDADES
OPORTUNIDADES	AMENAZAS

Figura 5 Formato de análisis FODA [Elaboración propia]

Formato de cuestionario de probabilidad e impacto

La tabla que se presenta a continuación sirve como encuesta la cual se va a realizar al área de TI, con la finalidad de poder identificar el nivel de impacto y que tan frecuente ocurre una vulnerabilidad o amenaza en base a su criterio, ya que posteriormente con los resultados obtenidos se evaluara el nivel de prioridad de cada una de estas vulnerabilidades y amenazas (Prado Oseguera, 2009).

Tabla 2 Formato de encuesta de vulnerabilidades y amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

	Descripción de vulnerabilidad o amenaza.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro

¿Con que frecuencia considera que ocurre este riesgo en la empresa?					
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					

Formato de matriz de riesgo

A continuación, se presenta una matriz de riesgo la cual será de gran ayuda para poder priorizar los riesgos en función de la probabilidad en que ocurra el riesgo y el impacto que puede tener de que ocurra, para ello se considera una escala numérica del 1 al 5, donde el 1 es el nivel más bajo y el 5 es el nivel demasiado alto. Además de ello tiene una escala de colores para que de esta manera sea más fácil identificar los riesgos visualmente, para esta escala se considera el color verde como un nivel de riesgo bajo y el color vino como un nivel de riesgo demasiado alto.

		IMPACTO				
		¿Qué tantos daños causarían si ocurriera el riesgo?				
PROBABILIDAD	¿Qué tanta probabilidad hay de que el riesgo ocurra?	Insignificante 1	Menor 2	Significativo 3	Mayor 4	Severo 5
	Seguro 5	Medio 5	Alto 10	Muy alto 15	Demasiado alto 20	Demasiado alto 20
	Casi seguro 4	Bajo 4	Medio 8	Alto 12	Muy alto 16	Demasiado alto 20
	Moderado 3	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
	Poco probable 2	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
	Raro 1	Muy bajo 1	Muy bajo 2	Bajo 3	Bajo 4	Medio 5

Figura 6 Formato para la matriz de riesgos. [Elaboración propia]

Formato para revisar los controles de seguridad en EQF.

Para poder revisar los controles e identificar si estos son los adecuados para cumplir con su objetivo de control o la necesidad que tenga la empresa, se va a dividir en dos partes esta revisión, donde en la primera se abordaran los conceptos sobre la actividad de control y en la segunda parte se realizará la evaluación de dicha actividad de control para saber si realmente cumple con su objetivo.

La primera parte se divide en seis columnas donde se habla acerca de la actividad de control a evaluar, su estructura consta de la siguiente manera:

- **Objetivo de control:** En esta parte se aborda el objetivo o meta que debe tener la actividad de control el cual debe de ir de la mano con los objetivos que se tienen en la empresa.
- **Descripción del riesgo:** En este apartado se habla sobre el o los riesgos que se tienen en la actividad de control los cuales impiden llegar a cumplir el objetivo o meta.
- **Actividades de control:** “Son las políticas, procedimientos, prácticas y estructuras diseñadas para proporcionar una garantía de que los objetivos del negocio se alcanzarán y que los eventos no deseados serán prevenidos o detectados” (Prado Oseguera, 2009).
- **Descripción de la actividad de control:** Como su nombre lo indica, en esta parte se tiene que dar una descripción de la actividad de control dentro de la organización.
- **Periodicidad de la actividad de control:** Aquí se indica con qué frecuencia es aplicada la actividad de control, por lo que puede ser de forma diaria, quincenal, mensual, bimestral, anual, etc.
- **Clasificación de la actividad de control:** Para la clasificación se utilizarán solamente dos parámetros, el primero de ellos es el “Automático”, donde la actividad de control es realizada por aplicativos o softwares los cuales son capaces de hacer dicha actividad de control con una configuración establecida, y el segundo parámetro es el “Manual”, donde las actividades de control son realizadas por los empleados los cuales tengan la responsabilidad de llevar a cabo el cumplimiento de estas actividades de control.

Tabla 3 Primera parte del formato para la revisión de las actividades de control [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

Objetivo de control	Descripción del riesgo	Actividades de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control

Para esta segunda parte de la revisión de la actividad de control, se comienza a realizar la evaluación o monitoreo del control, por lo que esta segunda parte se divide en cinco apartados que son los que se mencionan a continuación:

- Descripción del plan de prueba: Esta parte trata sobre el procedimiento que se va a llevar a cabo para revisar que la actividad de control se esté realizando correctamente.
- Método y cantidad de selección de partidas: Aquí se indica la forma en que se realizó la selección de muestra o partida, la cual puede ser al azar, en donde se selecciona una muestra total al azar como el nombre lo indica; casual, donde se puede seleccionar de forma manual un número total de la muestra; y de forma sistemática donde se considera un intervalo fijo del número total de la población, estas formas de selección ayudan a verificar que se esté realizando la actividad de control en un intervalo de tiempo.
- Resultado de la prueba: En esta parte se hace la descripción de los resultados obtenidos de la prueba que se realizó mediante el método que se eligió.
- Conclusión sobre la efectividad: Aquí se indica el grado de efectividad del cumplimiento que tiene la actividad de control para cumplir con su objetivo. Para ello se utilizará una escala evaluativa en base el modelo COBIT el cual indica el nivel de madurez de acuerdo con un rango de parámetros los cuales se abordan a continuación:
 - Nivel 0 (Inexistente): Falta de un proceso reconocible en donde la empresa no ha reconocido que existe un problema a resolver.
 - Nivel 1 (Inicial): Existe evidencia de que la organización ha reconocido las problemáticas y que tienen que ser resueltas. Sin embargo, no hay procesos

estandarizados, pero existen métodos ad hoc que tienen que ser aplicados de forma individual o caso por caso.

- Nivel 2 (Repetible): Se han desarrollado los procesos a tal grado en que diversas personas procedimientos similares realizando la misma tarea. Sin embargo, no existe una capacitación o comunicación formal de los procedimientos estándar dejando la responsabilidad a la persona. Se tiene un alto grado de confianza en la persona causando la alta probabilidad de que haya errores.
 - Nivel 3 (Definida): Los procedimientos se han estandarizado y documentado, y comunicado a través de capacitaciones. Sin embargo, es poco probable que se detecten desviaciones debido a que se ha dejado en manos de la persona el seguimiento de estos procesos. Dichos procedimientos no son sofisticados, no obstante, son la formalización de la practicas existentes.
 - Nivel 4 (Administrada): Existe la posibilidad de monitorear y medir el cumplimiento de los procesos, además de actuar en donde los procesos no funcionan efectivamente. Se utilizan la automatización y herramienta de forma limitada.
 - Nivel 5 (Optimizada): Los procesos se encuentran refinados hasta un nivel de mejores prácticas, basados en resultados de mejora continua y diseño de madurez con otras organizaciones. TI se utiliza de forma integrada automatizando el flujo de trabajo, brindando herramientas que mejoran la calidad y efectividad, haciendo que la empresa se adapte con rapidez.
(ISACA, s.f.)
- Referencia de la evidencia: En esta última parte se mencionan las evidencias obtenidas durante la prueba las cuales validan el porqué de los resultados obtenidos durante la evaluación.

Tabla 4 Segunda parte del formato para la revisión de las actividades de control [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

Descripción del plan de prueba	Método y cantidad de selección de partidas	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia

De esta manera se pueda llevar a cabo la revisión o evaluación de cada una de las actividades de control con las que cuenta actualmente EQF, para que así se pueda obtener un mejor contexto del estado en el que se encuentran dichas actividades.

Actividad 2.2 Aplicar una encuesta en el departamento de TI para detectar riesgos de seguridad informática.

Descripción de la actividad

En esta actividad se debe de aplicar una encuesta con el formato que se realizó en la actividad anterior, dicha encuesta se aplica a los 6 trabajadores del área de TI con la finalidad de recopilar información acerca del estado de las medidas de seguridad con las que se cuentan en la empresa para la protección de la información almacenada de manera local en los dispositivos y la información que es compartida a través de tecnologías como la nube, correo electrónico y aplicaciones de la paquetería de Office 365.

Resultado de la actividad

Niveles de Seguridad en Software de Equilibrio Farmacéutico

Pregunta 1. ¿Tiene conocimientos de medidas de seguridad informática implementadas en la organización?

- a) **SI**
- b) NO

Pregunta 2. Si la respuesta anterior fue “SI”, ¿conoce cuáles son esas medidas de seguridad informática?

Respuesta: Se tiene un antivirus llamado Panda en su versión empresarial, también se cuenta con una protección de correo electrónico, además de restricción del uso de aplicaciones.

Pregunta 3. En base a la siguiente escala considera que la seguridad informática implementada es:

- a) Mala
- b) **Regular**
- c) Buena
- d) Excelente

Pregunta 4. En base a la respuesta anterior ¿por qué considera que es así?

Respuesta: Las medidas con las que se cuentan, en algunos casos no se cumplen totalmente como el control de acceso a sitios web, de igual manera se pudo infiltrar un tipo de virus a los equipos de las sucursales y del corporativo.

Pregunta 5. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) **SI**
- b) NO

Pregunta 6. Si la respuesta anterior fue “SI” ¿qué medida de seguridad recomienda?

Respuesta: Protección en la información que se encuentre almacenada en los dispositivos, más protección en los servicios que se usan diariamente, más políticas de restricción de uso de aplicaciones y en el acceso a sitios y/o plataformas de streaming.

Protección de las tecnologías utilizadas en Equilibrio Farmacéutico.

Pregunta 7. ¿Qué tipo de tecnologías son las que utiliza en Equilibrio Farmacéutico para desempeñar sus actividades?

- a) **Paquetería Office 365**
- b) Aplicación SAP
- c) **Teams**
- d) **TeamViewer**

- e) Legado
- f) **Correo electrónico**
- g) **La nube**
- h) Todos los anteriores.

Protección de correo electrónico (Outlook)

Pregunta 8. En cuanto al servicio de correo electrónico (Outlook), ¿cuentan con medidas de seguridad informática?

- a) **SI**
- b) NO

Pregunta 9. Si la respuesta anterior fue “SI”, ¿cuáles son esas medidas de seguridad informática?

Respuesta: Protección contra ataques de virus y correos de tipo spam.

Pregunta 10. En base a la siguiente escala considera que la seguridad informática implementada en los servicios es:

- a) Mala
- b) **Regular**
- c) Buena
- d) Excelente

Pregunta 11. En base a la respuesta anterior ¿por qué considera que es así?

Respuesta: Porque se llegó a infiltrar un correo de spam el cual contenía un virus que afectó una cuenta de un usuario y además de ello empezó a mandar correos de forma masiva a los demás usuarios de las sucursales y corporativo.

Pregunta 12. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) **SI**
- b) NO

Pregunta 13. En caso de ser así, ¿qué medida de seguridad recomienda?

Respuesta: Protección para ataques de phishing o correos que contengan enlaces que seas maliciosos para que los dispositivos estén protegidos en caso de que un usuario caiga en ese tipo de ataques como el anteriormente sucedido.

Protección de servicio en la nube

Pregunta 14. En cuanto al servicio en la nube (OneDrive), ¿cuentan con medidas de seguridad informática?

- a) **SI**
- b) NO

Pregunta 15. Si la respuesta anterior fue “SI”, ¿cuáles son esas medidas de seguridad informática?

Respuesta: Detección y protección de virus que proporciona el antivirus.

Pregunta 16. En base a la siguiente escala considera que la seguridad informática implementada en los servicios es:

- a) Mala
- b) **Regular**
- c) Buena
- d) Excelente

Pregunta 17. En base a la respuesta anterior ¿por qué considera que es así?

Respuestas: Es regular debido a que, si detecta y protege de algunos virus, pero hubo una ocasión en la que se llegó a filtrar un archivo que contenía un virus de tipo troyano.

Pregunta 18. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) **SI**
- b) NO

Pregunta 19. En caso de ser así, ¿qué medida de seguridad recomienda?

Respuesta: Algún tipo de protección que analice si un archivo que este almacenado o que se llegue a compartir en la nube contine algún tipo de virus y pueda ponerlo en cuarentena.

Protección de aplicativo Teams

Pregunta 20. En cuanto al aplicativo Teams, ¿cuentan con medidas de seguridad informática?

- a) **SI**
- b) NO

Pregunta 21. Si la respuesta anterior fue “SI”, ¿cuáles son esas medidas de seguridad informática?

Respuesta: Protección de detección de virus al momento de descargar algún archivo.

Pregunta 22. En base a la siguiente escala considera que la seguridad informática implementada en Teams es:

- a) Mala
- b) **Regular**
- c) Buena
- d) Excelente

Pregunta 23. En base a la respuesta anterior ¿por qué considera que es así?

Respuesta: Porque algunas veces se llegan a infiltrar virus que no son detectados a tiempo ocasionando afectaciones en la producción o en la realización de actividades del usuario.

Pregunta 24. ¿Recomienda que se implementa alguna otra medida de seguridad?

- a) **SI**
- b) NO

Pregunta 25. En caso de ser así, ¿qué medida de seguridad recomienda?

Respuesta: Detección y protección de virus o algún tipo de ataque al momento de enviar y compartir archivos a través de este medio ya que es el que más se ocupa en la empresa.

Políticas de restricción de páginas web y/o plataformas de streaming

Pregunta 26. ¿Existen políticas de uso de sitios web y/o plataformas de streaming (Spotify, Netflix, etc.)?

- a) **SI**
- b) NO

Pregunta 27. En caso de ser así, ¿Se cumplen adecuadamente estas reglas?

- a) Siempre
- b) Casi siempre
- c) **A veces**
- d) Rara vez
- e) Nunca

Pregunta 28. En base a la respuesta anterior ¿por qué considera que es así?

Respuesta: Porque hay usuarios que tienen abiertas plataformas de streaming como Spotify para escuchar música o hay sitios web que no son del todo seguros en los que los usuarios ingresan para buscar algún tipo de información.

Pregunta 29. ¿Recomienda que se implementa alguna otra política de restricción sobre el uso sitios web y/o plataformas de streaming (Spotify, Netflix, etc.)?

- a) **SI**
- b) NO

Pregunta 30. En caso de ser así, ¿qué políticas de restricción recomienda?

Respuesta: Políticas que nieguen el acceso a sitios web que no son seguros o políticas que ayuden a controlar más el acceso a plataformas de streaming o cualquier otro sitio web.

Software de protección utilizados en Equilibrio Farmacéutico.

Pregunta 31. ¿Tiene instalado un software de protección (antivirus) en los dispositivos de la empresa?

- a) **SI**
- b) NO

Pregunta 32. ¿Considera que el antivirus cubre todas las necesidades de la empresa?

- a) Totalmente
- b) **Casi todas**
- c) Algunas
- d) Ninguna

Pregunta 33. En base a la respuesta anterior, ¿por qué considera que es así?

Respuesta: Porque hace falta más protección en los servicios que se utilizan a diario y que estas medidas de protección no dependan tanto del usuario para que se cumplan, además de implementar un tipo de protección en la información que se encuentre almacenada en los dispositivos de manera local.

Acontecimientos de ataques informáticos

Pregunta 34. ¿La empresa ha sido víctima de algún ataque informático?

- a) **SI**
- b) NO

Pregunta 35. En caso de ser así, ¿Qué tipo de ataque o ataques informáticos ocurrieron?

Respuesta: El ataque ocurrido fue un correo de spam el cual llegó a un usuario en donde este al ingresar al correo tenía un enlace, por lo que el usuario al ingresar al enlace le pedía datos bancarios mediante un formulario, pero al momento de que el usuario realizaba el formulario se enviaron correos masivos de spam suplantando la identidad del correo del usuario que fue víctima, además de ello se descargó un archivo el cual contenía un virus troyano.

Pregunta 36. ¿Cómo enfrentaron ese tipo de ataques informáticos?

Respuesta: Se bloqueo inmediatamente la cuenta de correo de ese usuario y se realizaron llamadas para informar a los demás usuarios que eliminaran el correo que se envió de tipo spam.

Pregunta 37. Actualmente, ¿cuentan con medidas o estrategias de seguridad informática para combatir ese tipo de ataques?

- a) **SI**
- b) NO

Pregunta 38. En caso de ser así, ¿Qué tipo de medidas de seguridad se implementaron para enfrentar los ciberataques?

Respuesta: Las medidas con las que cuenta el mismo antivirus, además se informó a los demás usuarios que hacer ante un ataque así y como identificarlo.

Pregunta 39. ¿Cómo considera que son actualmente esas medidas de seguridad implementadas?

- a) Excelente
- b) Buena
- c) Regular
- d) Mala

Pregunta 40. En base a la respuesta anterior, ¿por qué considera que es así?

Respuesta: Porque en parte siguen dependiendo del usuario para que estas medidas de seguridad sean efectivas, lo cual ocasiona que la empresa vuelva a ser víctima de algún tipo de virus o ataque informático.

Afectaciones en Equilibrio Farmacéutico

Pregunta 41. ¿La empresa sufrió algún tipo de afectación al ser víctima de ataques?

- a) **SI**
- b) NO

Pregunta 42. En caso de ser así, ¿de qué forma se vio afectada?

Respuesta: Se infectó un equipo de un virus, otros usuarios se vieron afectados de igual manera por el ataque del correo spam.

Pregunta 43. ¿Tuvo afectaciones económicas cuando sucedieron esos ataques informáticos?

- a) SI
- b) **NO**

Pregunta 44. ¿Cómo considera que fueron esas afectaciones económicas?

- a) **No hubo**
- b) Pocas
- c) Significativas
- d) Altas
- e) Severas

Actividad 2.3 Realizar diversos análisis FODA enfocados en el área de TI y sus servicios para evaluar la situación actual.

Descripción de la actividad

Para esta actividad se deben de realizar diversos análisis FODA enfocados en cada una de las principales tecnologías de Equilibrio Farmacéutico que se utilizan a diario para el desarrollo de las actividades, dichos FODA's tienen como objetivo evaluar la situación actual de las medidas de seguridad implementadas en la organización. Por lo tanto, para hacer dicho análisis FODA se contemplarán las respuestas de la encuesta de la actividad anterior.

Resultado de la actividad

FODA de los niveles de seguridad de software en Equilibrio Farmacéutico.

En este FODA se evalúa el estado actual en el que se encuentran los niveles de seguridad de software de Equilibrio Farmacéutico, con la finalidad de encontrar las mejores medidas de seguridad ante las amenazas que se puedan presentar.

FORTALEZAS	DEBILIDADES
• La empresa cuenta con un antivirus en su versión empresarial para la protección de los dispositivos. • Se cuenta con detección y protección de virus para el correo electrónico. • Políticas de restricción para el uso de aplicaciones las cuales no estén autorizadas por la organización. • Tienen niveles de acceso a los equipos de cómputo para que cualquier usuario no pueda instalar software sin autorización.	• En algunos dispositivos se encuentra almacenada la información de manera local sin ningún tipo de protección. • Parte de las medidas de seguridad dependen mucho del usuario para que estas cumplan adecuadamente con sus funciones. • Existe poco control y monitoreo del área de TI hacia los usuarios para que estos no hagan mal uso de aplicaciones. • El antivirus no cubre con todas las necesidades de protección de la empresa.
OPORTUNIDADES	AMENAZAS
• Implementar un nuevo antivirus en su versión empresarial que cubra con la mayoría de las necesidades de protección de la empresa. • Crear medidas de seguridad para la información que se encuentre almacenada de forma local en los dispositivos. • Hacer una estrategia de monitoreo para el uso y/o instalación de aplicaciones en los dispositivos. • Buscar un antivirus en el que las medidas de protección no dependan tanto del usuario para que estas se cumplan con éxito.	• La descarga de archivos que contienen algún tipo de virus los cuales pueden infectar los equipos de cómputo. • Creación de nuevas formas de realizar ataques informáticos de las cuales no se tengan conocimiento para su protección. • Pérdida de información a causa de ataques informáticos. • Infiltración de algún tipo de malware dentro de la red del corporativo.

Figura 7 FODA niveles de seguridad de software en Equilibrio Farmacéutico. [Elaboración propia]

En base al análisis FODA anterior se puede deducir que la protección para la información y los dispositivos que se encuentran actualmente implementadas en Equilibrio Farmacéutico carecen de algunas medidas de seguridad para que la empresa a futuro no sea víctima de ataques informáticos o algún virus, por lo tanto es necesario implementar otro antivirus a nivel empresarial el cual pueda cubrir todas las necesidades o en un 90% de ellas, además de implementar nuevas formas de protección que pueda ofrecer el mismo antivirus o de lo contrario crear estas nuevas formas de protección para proponerlas y en dado caso poder implementarlas.

FODA de la protección del servicio de correo electrónico (Outlook)

En este análisis FODA se busca evaluar la situación en la que se encuentra actualmente la protección para el servicio de correo electrónico (Outlook), siendo este uno de los principales medios de comunicación para asuntos importantes dentro de Equilibrio Farmacéutico.

FORTALEZAS	DEBILIDADES
• La empresa cuenta con un antivirus en su versión empresarial para la protección contra ataques de virus. • Se cuenta con detección y protección de virus para el correo electrónico. • Se distribuye información sobre los ataques de phishing para concientizar a los usuarios acerca de este tipo de ciberataques mediante una infografía.	• Hay usuarios que hacen caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM. • La protección de correo electrónico con la que se cuenta actualmente no es suficiente para cubrir adecuadamente las necesidades de la empresa. • Aunque existe una protección para correo electrónico, dicha seguridad es de forma general y no es tan específica en este rubro. • No todos los equipos de cómputo cuentan con un antivirus actualizado.
OPORTUNIDADES	AMENAZAS
• Implementar un antivirus el cual contenga una característica para la protección del correo electrónico de Outlook. • Crear estrategias para tener actualizado el antivirus del corporativo. • Implementar una medida de protección contra correos electrónicos de tipo SPAM los cuales contengan enlaces que sean maliciosos. • Crear estrategias de concienciación del personal acerca de otros delitos informáticos. • Crear procesos sencillos para salvaguardar los servicios de correo electrónico y antivirus	• Correos electrónicos de tipo SPAM, los cuales tratan de engañar a los usuarios con algún tipo de promocional o con un asunto de emergencia. • Ataques de phishing los cuales van ligados a los correos electrónicos de tipo SPAM donde se busca que el usuario atienda este tipo de correos para que este ciberataque tenga éxito. • Ataques de spoofing, donde se suplanta la identidad de una persona o correo electrónico de una organización y manda correos masivos a los demás destinatarios haciendo parecer que viene de una fuente legítima.

Figura 8 Análisis FODA de la protección del correo electrónico (Outlook). [Elaboración propia]

Por lo mencionado anteriormente en el análisis FODA, la organización cuenta con ciertas medidas de seguridad para uno de sus principales medios de comunicación que es el correo electrónico, sin embargo no solamente es responsabilidad del área de TI implementar estas medidas de seguridad, también los usuarios que pertenecen a las demás áreas deben de tener conocimientos básicos acerca de estos ataques, esto con la finalidad de evitar que la empresa o algún usuario sea víctima de un ataque de phishing, que es el más común. Por otra parte, es importante buscar alguna estrategia y/o antivirus el cual brinde seguridad en este medio de comunicación específicamente y que no dependa tanto del usuario para que esta protección cumpla en todas las necesidades de la organización, además de que estas medidas de seguridad deben actuar antes de que el usuario sea víctima de algún tipo de ataque referente al correo electrónico.

FODA de la protección del servicio en la nube (OneDrive)

El análisis FODA que se presenta a continuación tiene la finalidad de evaluar cómo se encuentra actualmente las medidas de seguridad en cuanto al servicio de la nube que utiliza Equilibrio Farmacéutico.

FORTALEZAS	DEBILIDADES
- La empresa cuenta con un antivirus en su versión empresarial para la protección contra ataques de virus. - Se cuenta con detección y protección de virus que brinda el mismo antivirus. - Se cuenta con grupos de trabajo para que cualquier usuario no pueda acceder a archivos que no corresponden a su área. - Algunos archivos compartidos cuentan con permisos como solamente lectura, modificación o que no se puedan eliminar. - Las contraseñas de las cuentas de Microsoft se reestablecen cuando un empleado sale de la empresa para que este no pueda acceder de nuevo.	- No se cuenta con una medida de seguridad para el análisis de archivos que son subidos a la nube. - La protección del servicio de la nube es ausente para cubrir adecuadamente las necesidades de la empresa. - Aunque existe una protección contra virus, dicha seguridad es de forma general y no es tan específica en este rubro. - No todos los equipos de cómputo cuentan con un antivirus actualizado que permita la protección de este servicio. - No hay un análisis de virus para los archivos que son compartidos mediante SharePoint.
OPORTUNIDADES	AMENAZAS
- Implementar un antivirus el cual contenga una característica para la protección del servicio en la nube (OneDrive). - Crear estrategias para tener actualizado el antivirus del corporativo. - Implementar una medida de protección contra archivos que se encuentren en la nube y que puedan contener algún tipo de virus.	- Archivos que contengan algún tipo de virus que no sea detectado por el antivirus. - Que un virus se pueda infiltrar e infecte los equipos de cómputo o los llegue a dañar. - La pérdida de información que se encuentre en un documento infectado.

Figura 9 Análisis FODA de la protección del servicio en la nube (OneDrive). [Elaboración propia]

En base al análisis FODA que se realizó previamente se puede observar que, aunque la empresa cuenta con un antivirus el cual brinda la detección y protección de virus, es necesario buscar otras medidas de seguridad las cuales se enfoquen en la protección del servicio en la nube debido a que por este medio se comparten varios archivos los cuales contienen información muy importante para la organización, por lo tanto, no se puede permitir que alguno de estos archivos se llegue a infectar por algún tipo de virus o malware, de igual manera se debe de implementar un análisis de los archivos que son subidos a la nube para que no se llegue a infiltrar un virus o que se pueda realizar algún tipo de ataque informático.

FODA de la protección del chat TEAMS

El siguiente análisis FODA busca evaluar cual es la situación en la que se encuentran hoy en día las medidas de seguridad en cuanto al chat de TEAMS, siendo este otro de las principales aplicaciones de comunicación en Equilibrio Farmacéutico.

FORTALEZA	DEBILIDADES
- La empresa cuenta con un antivirus en su versión empresarial para la protección contra virus y ataques informáticos. - Se cuenta con detección y protección de virus que brinda el mismo antivirus.	- No se cuenta con una medida de seguridad para el análisis de archivos, imágenes y/o videos que son compartidos por los usuarios mediante el chat de Teams. - La protección de Teams es ausente para cubrir adecuadamente las necesidades de la empresa. - Aunque existe una protección contra virus, dicha seguridad es de forma general y no es tan específica en este rubro. - No todos los equipos de cómputo cuentan con un antivirus actualizado que permita la protección en el uso del aplicativo.
OPORTUNIDADES	AMENAZAS
- Implementar un antivirus el cual contenga una característica para la protección del aplicativo Teams. - Crear estrategias para tener actualizado el antivirus del corporativo. - Ejecutar medidas de protección para los archivos, imágenes y/o videos que son compartidos por usuarios a través del chat de Teams.	- Archivos que contengan algún tipo de virus que no sea detectado por el antivirus. - La posibilidad de que suceda un ciberataque al momento de compartir cualquier tipo de archivos. - La probabilidad de que un archivo contenga un virus el cual llegue a infectar los equipos de cómputo.

Figura 10 Análisis FODA de la protección del chat TEAMS. [Elaboración propia]

Como se puede observar en el análisis FODA la empresa cuenta con un antivirus el cual puede brindar la protección contra algunos virus y ataques informáticos, sin embargo, esto no es suficiente para que los usuarios que utilizan el aplicativo de Teams tengan la seguridad adecuada, por lo que es importante implementar más niveles de protección para este aplicativo debido a que este es otro de los medios que día con día se utiliza para compartir diferentes tipos de archivos como documentos, imágenes y videos.

FODA de las políticas de restricción de páginas web y plataformas de streaming

El siguiente análisis FODA tiene la finalidad de evaluar el estado actual de las políticas de restricción de uso de páginas web y/o plataformas de streaming, debido a que puede representar un problema grave si estas no se cumplen en su totalidad.

FORTALEZAS	DEBILIDADES
- Actualmente se cuenta con políticas de denegación de acceso para algunos sitios web que no son seguros. - Existen políticas de restricción para el uso de plataformas de streaming. - Hay bloqueo de sitios web de redes sociales	- Aunque existen políticas donde no se permite acceso a sitios web que no son seguros, hay sitios en donde sí se puede ingresar. - No todos los usuarios respetan estas políticas de restricción a sitios web y/o plataformas de streaming, ya que permiten el acceso en sus dispositivos. - Existe poco control sobre el acceso de los sitios web o plataformas en las que ingresan los usuarios. - Debido a que algunos usuarios no respetan las políticas existentes, se afecta el rendimiento del internet y por consecuencia la comunicación para realizar alguna actividad.
OPORTUNIDADES	AMENAZAS
- Implementar políticas de restricción de acceso a sitios web que no son seguros y plataformas de streaming, que no dependan tanto del usuario - Implementar una medida de seguridad que analice sitios web que sean seguros. - Crear una estrategia para tener un mejor control del acceso a los sitios web y el uso de plataformas de streaming.	- El acceso a sitios web que no son seguros. - Actualmente, existen sitios que aparentan ser seguros incluso teniendo el certificado HTTPS, pero estos sitios web son una suplantación del sitio oficial. - Robo de datos mediante sitios web que piden información personal y/o datos bancarios. - Descargas de archivos que estén infectados de virus, por medio de sitios web. - Ciberataques por medio de sitios web no seguros o aparentemente oficiales.

Figura 11 Análisis FODA de las políticas de restricción de páginas web y plataformas de streaming. [Elaboración propia]

Por lo mencionado anteriormente en el análisis FODA, se puede deducir que, aunque existen actualmente políticas de restricción de acceso a sitios web que no son seguros, sitios de redes sociales y plataformas de streaming (Spotify, Netflix, etc.), estas no se cumplen totalmente por parte de los usuarios ya que estos permiten el acceso en sus dispositivos, lo que puede provocar que se llegue a infiltrar algún tipo de virus o que se realice algún tipo de ataque informático. Por lo tanto, es importante implementar políticas y/o reglas de bloqueo de acceso las cuales no dependan del usuario para que estas se cumplan o no, de igual manera es importante implementar una medida de protección para que se analicen sitios web que aparentan ser seguros, debido a que hoy en día existe la posibilidad de que un sitio oficial sea suplantado por otro aun teniendo el certificado de HTTPS.

Objetivo 3. Evaluar los riesgos identificados, teniendo en cuenta su nivel de impacto y probabilidad.

Este objetivo se centra en evaluar los riesgos que se lograron identificar en base a su nivel de probabilidad e impacto, con la finalidad de tener una mayor comprensión de la exposición del cada uno de los riesgos y así poder priorizar aquellos que pueden generar un mayor impacto tanto en las operaciones de la empresa como a nivel económico. Además, dicho objetivo servirá para implementar nuevas estrategias de gestión de riesgos y medidas de seguridad en la empresa.

Actividad 3.1 Crear una matriz de riesgos para los servicios de TI con el propósito de identificar, evaluar y priorizar riesgos que puedan afectar la prestación de estos servicios, y así asegurar su continuidad y calidad.

Descripción de la actividad

Para el desarrollo de esta actividad se debe de realizar un recuadro el cual permita identificar los posibles escenarios de riesgo en base a las vulnerabilidades y amenazas que se detectaron en la actividad anterior, además de ello se debe de hacer un cuestionario el cual se va a aplicar al área de TI con la finalidad de identificar la probabilidad e impacto de las amenazas y/o riesgos que puedan ocurrir en las tecnologías con las que se cuentan, posteriormente en base al cuestionario se creara la matriz de riesgo para que de esta manera se pueda priorizar la atención a los diversos riesgos o problemas con los que se cuentan.

Resultado de la actividad

El recuadro que se presenta a continuación sirve de ayuda para identificar aquellos riesgos que puedan llegar a afectar a la empresa, además de las vulnerabilidades y amenazas que pueden ocasionar dicho riesgo.

Tabla 5 Identificación de riesgos en base a vulnerabilidades y amenazas [Elaboración propia].

VULNERABILIDAD	AMENAZA	RIESGO
V1. No contar con una protección para la información almacenada de manera local en los dispositivos. V2. Los archivos que se suben a la nube y que son compartidos mediante SharePoint no sean analizados en busca de virus. V4. Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	A1. Nuevas formas de realizar un ciberataque. A2. Creación de nuevos virus. A3. Robo o secuestro de información que sea de gran importancia para la empresa. A4. Pérdida de información que se encuentre en un archivo infectado. A5. Robo de información mediante sitios web que piden datos personales y/o bancarios.	R1. Bloquear el acceso a la información que sea de gran importancia para la empresa a causa de un ciberataque.
V1. Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente. V2. Parte de los usuarios hacen caso omiso a las recomendaciones por parte del área de TI para identificar correos de tipo SPAM. V4. Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	A1. Nuevas formas de realizar un ciberataque, además de creación de nuevos virus. A3. Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo. A4. Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia. A5. Ataques de tipo phishing al correo electrónico de los usuarios. A6. Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	R2. Daños en los servicios de la empresa a causa de ciberataque por el incumplimiento de políticas de restricción o mal uso de aplicativos por parte de los usuarios. R3. Daño de equipos de cómputo debido a la infección de algún tipo de virus.

Tabla 5 Identificación de riesgos en base a vulnerabilidades y amenazas [Elaboración propia].

VULNERABILIDAD	AMENAZA	RIESGO
V1. Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos. V3. Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.). V4. Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	A1. Suplantación de sitios web oficiales, incluso teniendo el certificado HTTPS. A2. Descarga de archivos infectados por medio de sitios web. A3. Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	R4. Afectación en el rendimiento de las operaciones y servicios de comunicación de la empresa, debido al mal uso de aplicativos y sitios web.
V1. Aunque existe un antivirus este no cubre con todas las necesidades de protección de la empresa. V2. La protección de correo electrónico no es suficiente para cubrir adecuadamente las necesidades de la empresa. V3. Los equipos de cómputo no tengan un antivirus actualizado.	A1. Nuevas formas de realizar un ciberataque, además de creación de nuevos virus. A3. Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo. A4. Ciberataques al servicio de correo electrónico como correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia. A5. Ciberataque por medio de sitios web no seguros o aparentemente oficiales. A6. Infiltración de algún tipo de malware dentro de la red del corporativo.	R5. La empresa sea víctima de un ciberataque debido a que las medidas de seguridad no cubren con todas las necesidades de la empresa. R6. Infiltración de un virus a algún equipo de cómputo por medio de la red de la empresa debido a que las medidas de seguridad no cubren con todas las necesidades.

Tabla 5 Identificación de riesgos en base a vulnerabilidades y amenazas [Elaboración propia].

VULNERABILIDAD	AMENAZA	RIESGO
V1. Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente. V2. Algunos usuarios hacen caso omiso a las recomendaciones por parte del área de TI para identificar correos de tipo SPAM. V3. La protección de correo electrónico no es suficiente para cubrir adecuadamente las necesidades de la empresa.	A1. Nuevas formas de realizar un ciberataque. A2. Robo o secuestro de información que sea de gran importancia para la empresa. A3. Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo. A4. Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia. A5. Ciberataques al servicio de correo electrónico.	R7. Afectaciones en el servicio de correo electrónico.

La tabla que se presenta a continuación representa un cuestionario que servirá para determinar el impacto y probabilidad de las vulnerabilidades y amenazas que se reflejaron en la actividad anterior, para ello se realizaran diversos cuestionamientos a los empleados del área de TI (6 empleados).

Tabla 6 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

	VULNERABILIDAD: No contar con una protección para la información almacenada de manera local en los dispositivos.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?	2	3	1		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4

Tabla 6 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
Ocurrencia					
¿Con que frecuencia considera que ocurre este riesgo en la empresa?		6			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				1	5
VULNERABILIDAD: Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
Ocurrencia					
¿Con que frecuencia considera que ocurre este riesgo en la empresa?		2	3	1	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			3	4	
VULNERABILIDAD: Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
Ocurrencia					
¿Con que frecuencia considera que sucede este riesgo en la empresa?		2	3	1	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			2	4	

Tabla 6 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Los equipos de cómputo no tengan un antivirus actualizado.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	4	2			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4
VULNERABILIDAD: Los archivos que se suben a la nube no sean analizados en busca de virus.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	4	2			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			6		
VULNERABILIDAD: Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	5	1			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4

Tabla 6 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	2	4			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			5	1	
VULNERABILIDAD: Se pueda ingresar a sitios web que no son seguros.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?			2	4	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				6	
VULNERABILIDAD: Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?				2	4

¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			1	5	
--	--	--	---	---	--

Tabla 6 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.					
Nivel de impacto Ocurrencia	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	1	2	3		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			1	3	2
VULNERABILIDAD: Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.					
Nivel de impacto Ocurrencia	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?			1	5	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 7 Cuestionario de nivel de impacto y probabilidad de amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

	AMENAZA: Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?			4	2	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4
	AMENAZA: Perdida de información a causa de ataques informáticos y/o virus.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	1	3	2		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				1	5
	AMENAZA: Infiltración de algún tipo de malware en la red del corporativo.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?		4	2		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				1	5

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 7 Cuestionario de nivel de impacto y probabilidad de amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

	AMENAZA: Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	4	2			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?	1	2	3		
	AMENAZA: Ataques de tipo phishing al correo electrónico de los usuarios.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	5	1			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			4	2	
	AMENAZA: Ataques de tipo spoofing al servicio de correo electrónico de la empresa.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	5	1			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?		1	2	3	

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 7 Cuestionario de nivel de impacto y probabilidad de amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

AMENAZA: Robo de información mediante sitios web que piden datos personales y/o bancarios.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?	5	1			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6
AMENAZA: Descarga de archivos infectados, por medio de sitios web.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?	2	3	1		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6
AMENAZA: Ciberataque por medio de sitios web no seguros o aparentemente oficiales.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?	6				
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6

De acuerdo con el cuestionario anterior, ahora se evaluará el nivel de prioridad de cada una de las vulnerabilidades y amenazas mencionadas para ello se utiliza una matriz de riesgo la cual contiene valores de acuerdo al nivel de impacto y probabilidad.

Primeramente, se toma como ejemplo la primera vulnerabilidad del cuestionario, como se puede observar la mayoría de las personas encuestadas considera que la vulnerabilidad es **poco probable** que suceda y que su nivel de impacto si sucede sería **severo**. Por lo tanto, se tienen los valores de **Poco probable y Severo**.

Tabla 8 Ejemplo del primer riesgo evaluado [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: No contar con una protección para la información almacenada de manera local en los dispositivos.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?	2	3	1		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4

Ahora se buscarán los valores obtenidos dentro de la matriz de riesgo para medir su nivel de prioridad de esta primera vulnerabilidad.

IMPACTO						
¿Qué tantos daños causarían si ocurriera el riesgo?						
PROBABILIDAD	¿Qué tanta probabilidad hay de	Insignificante	Menor	Significativo	Mayor	Severo
		1	2	3	4	5
	Seguro	Medio	Alto	Muy alto	Demasiado alto	Demasiado alto
	5	5	10	15	20	20
	Casi seguro	Bajo	Medio	Alto	Muy alto	Demasiado alto
	4	4	8	12	16	20

	Moderado 3	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
	Poco probable 2	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
	Raro 1	Muy bajo 1	Muy bajo 2	Bajo 3	Bajo 4	Medio 5

Figura 12 Matriz de riesgos. [Elaboración propia]

Tomando en cuenta la matriz de riesgo se puede observar que su valor de prioridad es de 10 y por lo tanto se considera que es una vulnerabilidad de nivel **Alto**. A continuación, se muestran dos tablas con el nivel de prioridad de cada una de las vulnerabilidades y amenazas tomando en cuenta su probabilidad e impacto.

Tabla 9 Nivel de prioridad de cada una de las vulnerabilidades evaluadas [Elaboración propia].

VULNERABILIDADES	PROBABILIDAD	IMPACTO	NIVEL DE PRIORIDAD
No contar con una protección para la información almacenada de manera local en los dispositivos.	Poco probable	Severo	ALTO
Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	Poco probable	Severo	ALTO
Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.	Moderado	Mayor	ALTO
Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.	Moderado	Mayor	ALTO

Tabla 9 Nivel de prioridad de cada una de las vulnerabilidades evaluadas [Elaboración propia].

VULNERABILIDADES	PROBABILIDAD	IMPACTO	NIVEL DE PRIORIDAD
Los equipos de cómputo no tengan un antivirus actualizado.	Raro	Severo	MEDIO
Los archivos que se suben a la nube no sean analizados en busca de virus.	Raro	Significativo	BAJO
Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.	Raro	Severo	MEDIO
Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	Poco probable	Significativo	MEDIO
Se pueda ingresar a sitios web que no son seguros.	Casi seguro	Mayor	MUY ALTO
Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	Casi seguro	Severo	DEMASIADO ALTO
Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.	Moderado	Mayor	ALTO
Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	Casi seguro	Severo	DEMASIADO ALTO

Tabla 10 Nivel de prioridad de cada una de las amenazas evaluadas [Elaboración propia].

AMENAZAS	PROBABILIDAD	IMPACTO	NIVEL DE PRIORIDAD
Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.	Moderado	Severo	MUY ALTO
Perdida de información a causa de ataques informáticos y/o virus.	Poco probable	Severo	ALTO
Infiltración de algún tipo de malware en la red del corporativo.	Poco probable	Severo	ALTO
Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.	Raro	Significativo	BAJO
Ataques de tipo phishing al correo electrónico de los usuarios.	Raro	Significativo	BAJO
Ataques de tipo spoofing al servicio de correo electrónico de la empresa.	Raro	Mayor	BAJO
Robo de información mediante sitios web que piden datos personales y/o bancarios.	Raro	Severo	MEDIO
Descarga de archivos infectados, por medio de sitios web.	Poco probable	Severo	ALTO
Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	Raro	Severo	MEDIO

Actividad 3.2. Evaluar cualitativamente los servicios de TI para el impacto y probabilidad de los escenarios de amenaza y vulnerabilidad.

Descripción de la actividad

Para esta actividad se tiene que realizar primeramente una encuesta la cual permita determinar el nivel de impacto y la frecuencia que sucede cada amenaza y vulnerabilidad, esto en base a la opinión de los 5 analistas y el gerente del área de TI. Posteriormente, con los resultados obtenidos en la encuesta se va a evaluar el nivel de riesgo de cada amenaza y vulnerabilidad con ayuda de la matriz de riesgo, para finalmente saber el nivel de prioridad que se le va a brindar a cada una de estas.

Resultado de la actividad

La tabla que se presenta a continuación representa una encuesta que servirá para determinar el impacto y probabilidad de las vulnerabilidades que se reflejaron en la actividad anterior, para ello se realizaron diversos cuestionamientos a los empleados del área de TI (6 empleados).

Tabla 11 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

	VULNERABILIDAD: No contar con una protección para la información almacenada de manera local en los dispositivos.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?	2	3	1		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4

Tabla 11 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.					
Nivel de impacto Ocurrencia	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?		6			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				1	5
VULNERABILIDAD: Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.					
Nivel de impacto Ocurrencia	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?		2	3	1	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			3	4	
VULNERABILIDAD: Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.					
Nivel de impacto Ocurrencia	Insignificante	Menor	Significativo	Mayor	Severo
	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?		2	3	1	

¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			2	4	
--	--	--	---	---	--

Tabla 11 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Los equipos de cómputo no tengan un antivirus actualizado.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	4	2			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4
VULNERABILIDAD: Los archivos que se suben a la nube no sean analizados en busca de virus.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	4	2			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			6		
VULNERABILIDAD: Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	5	1			

¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4
--	--	--	--	---	---

Tabla 11 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	2	4			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			5	1	
VULNERABILIDAD: Se pueda ingresar a sitios web que no son seguros.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?			2	4	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				6	

Tabla 11 Cuestionario de nivel de impacto y probabilidad de vulnerabilidades [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?				2	4
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			1	5	
VULNERABILIDAD: Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	1	2	3		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			1	3	2
VULNERABILIDAD: Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?			1	5	

¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6
--	--	--	--	--	---

La tabla que se presenta a continuación representa una encuesta que servirá para determinar el impacto y probabilidad de las amenazas que se reflejaron en la actividad anterior, para ello se realizaran diversos cuestionamientos a los empleados del área de TI (6 empleados).

Tabla 12 Cuestionario de nivel de impacto y probabilidad de amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

	AMENAZA: Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?			4	2	
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4
	AMENAZA: Pérdida de información a causa de ataques informáticos y/o virus.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	1	3	2		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				1	5

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 12 Cuestionario de nivel de impacto y probabilidad de amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

AMENAZA: Infiltración de algún tipo de malware en la red del corporativo.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?		4	2		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				1	5
AMENAZA: Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	4	2			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?	1	2	3		
AMENAZA: Ataques de tipo phishing al correo electrónico de los usuarios.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	5	1			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			4	2	

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 12 Cuestionario de nivel de impacto y probabilidad de amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

AMENAZA: Ataques de tipo spoofing al servicio de correo electrónico de la empresa.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que sucede este riesgo en la empresa?	5	1			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?		1	2	3	
AMENAZA: Robo de información mediante sitios web que piden datos personales y/o bancarios.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?	5	1			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6
AMENAZA: Descarga de archivos infectados, por medio de sitios web.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?	2	3	1		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6

Tabla 12 Cuestionario de nivel de impacto y probabilidad de amenazas [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

AMENAZA: Ciberataque por medio de sitios web no seguros o aparentemente oficiales.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que suceda este riesgo en la empresa?	6				
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					6

De acuerdo con el cuestionario anterior, ahora se evaluará el nivel de prioridad de cada una de las vulnerabilidades y amenazas mencionadas para ello se utiliza una matriz de riesgo la cual contiene valores de acuerdo con el nivel de impacto y probabilidad.

Primeramente, se toma como ejemplo la primera vulnerabilidad del cuestionario, como se puede observar la mayoría de las personas encuestadas considera que la vulnerabilidad es **poco probable** que suceda y que su nivel de impacto si sucede sería **severo**. Por lo tanto, se tienen los valores de **Poco probable y Severo**

Tabla 13 Ejemplo del primer riesgo evaluado [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

VULNERABILIDAD: No contar con una protección para la información almacenada de manera local en los dispositivos.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Ocurrencia	Raro	Poco probable	Moderado	Casi seguro	Seguro
¿Con que frecuencia considera que ocurre este riesgo en la empresa?	2	3	1		

¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				2	4
--	--	--	--	---	---

Ahora se buscarán los valores obtenidos dentro de la matriz de riesgo para medir su nivel de prioridad de esta primera vulnerabilidad.

		IMPACTO				
		¿Qué tantos daños causarían si ocurriera el riesgo?				
PROBABILIDAD	¿Qué tanta probabilidad hay de que el riesgo ocurra?	Insignificante 1	Menor 2	Significativo 3	Mayor 4	Severo 5
	Seguro 5	Medio 5	Alto 10	Muy alto 15	Demasiado alto 20	Demasiado alto 20
	Casi seguro 4	Bajo 4	Medio 8	Alto 12	Muy alto 16	Demasiado alto 20
	Moderado 3	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
	Poco probable 2	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
	Raro 1	Muy bajo 1	Muy bajo 2	Bajo 3	Bajo 4	Medio 5

Figura 13 Matriz de riesgos para evaluar. [Elaboración propia]

Tomando en cuenta la matriz de riesgo se puede observar que su valor de prioridad es de 10 y por lo tanto se considera que es una vulnerabilidad de nivel **Alto**. A continuación, se muestran dos tablas con el nivel de prioridad de cada una de las vulnerabilidades y amenazas tomando en cuenta su probabilidad e impacto.

Tabla 14 Nivel de prioridad de cada una de las vulnerabilidades evaluadas [Elaboración propia].

VULNERABILIDADES	PROBABILIDAD	IMPACTO	NIVEL DE PRIORIDAD
Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	Casi seguro	Severo	DEMASIADO ALTO
Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	Casi seguro	Severo	DEMASIADO ALTO
Se pueda ingresar a sitios web que no son seguros.	Casi seguro	Mayor	MUY ALTO
No contar con una protección para la información almacenada de manera local en los dispositivos.	Poco probable	Severo	ALTO
Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	Poco probable	Severo	ALTO
Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.	Moderado	Mayor	ALTO
Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.	Moderado	Mayor	ALTO

Tabla 14 Nivel de prioridad de cada una de las vulnerabilidades evaluadas [Elaboración propia].

VULNERABILIDADES	PROBABILIDAD	IMPACTO	NIVEL DE PRIORIDAD
Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.	Moderado	Mayor	ALTO
Los equipos de cómputo no tengan un antivirus actualizado.	Raro	Severo	MEDIO
Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.	Raro	Severo	MEDIO
Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	Poco probable	Significativo	MEDIO
Los archivos que se suben a la nube no sean analizados en busca de virus.	Raro	Significativo	BAJO

Tabla 15 Nivel de prioridad de cada una de las amenazas evaluadas [Elaboración propia].

AMENAZAS	PROBABILIDAD	IMPACTO	NIVEL DE PRIORIDAD
Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.	Moderado	Severo	MUY ALTO
Perdida de información a causa de ataques informáticos y/o virus.	Poco probable	Severo	ALTO

Infiltración de algún tipo de malware en la red del corporativo.	Poco probable	Severo	ALTO
Descarga de archivos infectados, por medio de sitios web.	Poco probable	Severo	ALTO
Robo de información mediante sitios web que piden datos personales y/o bancarios.	Raro	Severo	MEDIO
Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	Raro	Severo	MEDIO
Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.	Raro	Significativo	BAJO
Ataques de tipo phishing al correo electrónico de los usuarios.	Raro	Significativo	BAJO
Ataques de tipo spoofing al servicio de correo electrónico de la empresa.	Raro	Mayor	BAJO

Actividad 3.3. Evaluar cuantitativamente los servicios de TI para medir otorgarle una clasificación y prioridad de atención.

Descripción de la actividad

En esta actividad se van a evaluar las amenazas y vulnerabilidades, en base a un aspecto cuantitativo el cual arrojará valores monetarios aproximados de pérdidas en caso de que ocurra un riesgo, para ello se utilizara una metodología llamada Valor Monetario Esperado (EMV), el cual “consiste en multiplicar el impacto financiero potencial de un riesgo (es decir, cuánto podría costar o beneficiar al proyecto si el riesgo ocurre) por la probabilidad de que ese riesgo realmente suceda” (Dharma Consulting, 2023).

Resultado de la actividad

Para realizar la evaluación cuantitativa de las amenazas y vulnerabilidades, primeramente, se debe de obtener el porcentaje de probabilidad de que estas sucedan, para ello se tomará la opinión de los 5 analistas y el gerente del área de TI de la encuesta de la actividad anterior, ósea que los 6 empleados en total representan un 100% de probabilidad de que un riesgo se produzca. Posteriormente, se debe de investigar con el gerente de TI el valor aproximado de que una amenaza o vulnerabilidad se produzca.

Como primer ejemplo se tiene la siguiente vulnerabilidad:

Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).

En base a la encuesta de la evaluación cualitativa se tiene que 4 empleados del área de TI consideran que es seguro que se produzca esta vulnerabilidad, por lo que se tiene que calcular el porcentaje que esto representa.

Se tiene la siguiente formula:

$$EEC * 100 / TE = \% EEC$$

Donde:

TE = Total de empleados

100 = 100% total de empleados

EEC = Empleados de la Evaluación Cualitativa

%EEC = Porcentaje de Empleados de la Evaluación Cualitativa

Ahora se realiza la operación con sus valores correspondientes:

$$4 * 100 / 6 = 66.67\%$$

Por lo tanto, el resultado de la operación (66.67%) representa el porcentaje de probabilidad de que se produzca la vulnerabilidad. En seguida se tiene que investigar el valor monetario aproximado del impacto que tendría esa vulnerabilidad.

Por ejemplo, si la vulnerabilidad sigue ocurriendo representaría pérdidas de aproximadamente \$20,000.00. Por lo tanto, ya se tienen todos los valores para calcular el Valor Monetario Esperado.

En seguida se tiene que calcular el valor monetario aproximado de la vulnerabilidad para ello se tiene la siguiente formula:

$$PR * CI = EMV$$

Donde:

PR = Probabilidad en centésimas de que se produzca la amenaza o vulnerabilidad.

CI = Coste del Impacto

EMV = Valor Monetario Esperado

Ahora se realizará la operación con sus valores correspondientes:

$$0.67 * 20,000.00 = 13,400.00$$

Por lo tanto, considerando la vulnerabilidad de que los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.). es de un 66.67% y puede representar pérdidas totales de \$20,000.00 si sigue ocurriendo, su valor aproximado esperado de pérdidas en base al porcentaje de probabilidad es de **13,400.00**.

A continuación, se muestran dos tablas con la representación en porcentaje de los empleados del área de TI que dijeron que una amenaza o vulnerabilidad podría ocurrir.

Tabla 16 Porcentaje de probabilidad de que ocurra una vulnerabilidad [Elaboración propia].

VULNERABILIDADES	TOTAL DE EMPLEADOS QUE CONSIDERAN QUE OCURRE ESTA VULNERABILIDAD	CALCULO DE OPERACIÓN	PORCENTAJE TOTAL
Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son	4	$4 * 100 / 6 = 67$	67%

seguros o plataformas de streaming (Spotify, Netflix, etc.).			
Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	5	$5 * 100 / 6 = 83$	83%
Se pueda ingresar a sitios web que no son seguros.	4	$4 * 100 / 6 = 67$	67%
No contar con una protección para la información almacenada de manera local en los dispositivos.	3	$3 * 100 / 6 = 50$	50%
Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	6	$6 * 100 / 6 = 100$	100%
Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.	3	$3 * 100 / 6 = 50$	50%
Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.	3	$3 * 100 / 6 = 50$	50%
Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.	3	$3 * 100 / 6 = 50$	50%
Los equipos de cómputo no tengan un antivirus actualizado.	4	$4 * 100 / 6 = 67$	67%
Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.	5	$5 * 100 / 6 = 83$	83%

Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	4	$4 * 100 / 6 = 67$	67%
Los archivos que se suben a la nube no sean analizados en busca de virus.	4	$4 * 100 / 6 = 67$	67%

Tabla 17 Porcentaje de probabilidad de que ocurra una amenaza [Elaboración propia].

AMENAZAS	TOTAL DE EMPLEADOS QUE CONSIDERAN QUE OCURRE ESTA VULNERABILIDAD	CALCULO DE OPERACIÓN	PORCENTAJE TOTAL
Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.	4	$4 * 100 / 6 = 67$	67%
Perdida de información a causa de ataques informáticos y/o virus.	3	$3 * 100 / 6 = 50$	50%
Infiltración de algún tipo de malware en la red del corporativo.	4	$4 * 100 / 6 = 67$	67%
Descarga de archivos infectados, por medio de sitios web.	3	$3 * 100 / 6 = 50$	50%
Robo de información mediante sitios web que piden datos personales y/o bancarios.	5	$5 * 100 / 6 = 83$	83%
Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	6	$6 * 100 / 6 = 100$	100%
Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.	4	$4 * 100 / 6 = 67$	67%
Ataques de tipo phishing al correo electrónico de los usuarios.	5	$5 * 100 / 6 = 83$	83%

Ataques de tipo spoofing al servicio de correo electrónico de la empresa.	5	$5 * 100 / 6 = 83$	83%
---	---	--------------------	------------

Ahora, se muestran las tablas de las vulnerabilidades y amenazas con el costo monetario total aproximado del impacto que causaría si alguna de estas sucede. El costo aproximado total se calculó en base a las tres sucursales top (Ecatepec, Iztapalapa 1 e Iztapalapa 2), las cuales suman unas ventas totales de entre \$900,000.00 a \$1,100,000.00 de pesos mexicanos al día, por lo que si sucede alguna de estas vulnerabilidades y amenazas serían las principales sucursales que reflejarían afectaciones muy significativas a Equilibrio Farmacéutico S.A de C.V.

Tabla 18 Valor Monetario Total Aproximando del Impacto de la Vulnerabilidad (pesos mexicanos) [Elaboración propia].

VULNERABILIDADES	VALOR MONETARIO TOTAL APROXIMANDO DEL IMPACTO DE LA VULNERABILIDAD (PESOS MEXICANOS)
Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	\$500,000.00
Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	\$900,000.00
Se pueda ingresar a sitios web que no son seguros.	\$600,000.00
No contar con una protección para la información almacenada de manera local en los dispositivos.	\$1,000,000.00
Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	\$1,000,000.00
Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.	\$300,000.00

Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.	\$700,000.00
Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.	\$800,000.00
Los equipos de cómputo no tengan un antivirus actualizado.	\$1,000,000.00
Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.	\$900,000.00
Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	\$400,000.00
Los archivos que se suben a la nube no sean analizados en busca de virus.	\$800,000.00

Tabla 19 Valor Monetario Total Aproximando del Impacto de la Amenaza (pesos mexicanos) [Elaboración propia].

AMENAZAS	VALOR MONETARIO TOTAL APROXIMANDO DEL IMPACTO DE LA VULNERABILIDAD (PESOS MEXICANOS)
Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.	\$700,000.00
Perdida de información a causa de ataques informáticos y/o virus.	\$1,000,000.00
Infiltración de algún tipo de malware en la red del corporativo.	\$900,000.00
Descarga de archivos infectados, por medio de sitios web.	\$500,000.00
Robo de información mediante sitios web que piden datos personales y/o bancarios.	\$900,000.00
Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	\$900,000.00

Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.	\$300,000.00
Ataques de tipo phishing al correo electrónico de los usuarios.	\$400,000.00
Ataques de tipo spoofing al servicio de correo electrónico de la empresa.	\$400,000.00

Ya que se tienen los valores del porcentaje que se produzca cada una de las vulnerabilidades y amenazas, además de su valor total aproximado, se prosigue a realizar el cálculo del Valor Monetario Esperado de cada una de estas. A continuación, se muestran dos tablas con el cálculo del EMV de las vulnerabilidades y amenazas.

Tabla 20 Valor Monetario Esperado de las Vulnerabilidades [Elaboración propia].

VULNERABILIDADES	% DE QUE SE PRODUZCA LA VULNERABILIDAD	VALOR MONETARIO TOTAL APROXIMADO	CALCULO DEL EMV	VALOR MONETARIO ESPERADO SI SUCEDE LA VULNERABILIDAD
Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	67%	\$500,000.00	$0.67 * 500,000$	\$335,000.00
Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	83%	\$900,000.00	$0.83 * 900,000$	\$738,000.00
Se pueda ingresar a sitios web que no son seguros.	67%	\$600,000.00	$0.67 * 600,000$	\$402,000.00
No contar con una protección para la información almacenada de manera local en los dispositivos.	50%	\$1,000,000.00	$0.50 * 1,000,000$	\$500,000.00

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 20 Valor Monetario Esperado de las Vulnerabilidades [Elaboración propia].

VULNERABILIDADES	% DE QUE SE PRODUZCA LA VULNERABILIDAD	VALOR MONETARIO TOTAL APROXIMADO	CALCULO DEL EMV	VALOR MONETARIO ESPERADO SI SUCEDE LA VULNERABILIDAD
Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	100%	\$1,000,000.00	$1.0 * 1,000,000$	\$1,000,000.00
Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.	50%	\$300,000.00	$0.50 * 300,000$	\$150,000.00
Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.	50%	\$700,000.00	$0.50 * 700,000$	\$350,000.00
Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.	50%	\$800,000.00	$0.50 * 800,000$	\$400,000.00
Los equipos de cómputo no tengan un antivirus actualizado.	67%	\$1,000,000.00	$0.67 * 1,000,000$	\$670,000.00
Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.	83%	\$900,000.00	$0.83 * 900,000$	\$747,000.00
Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	67%	\$400,000.00	$0.67 * 400,000$	\$268,000.00

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Los archivos que se suben a la nube no sean analizados en busca de virus.	67%	\$800,000.00	$0.67 * 800,000$	\$536,000.00
---	-----	--------------	------------------	---------------------

Tabla 21 Valor Monetario Esperado de las Amenazas [Elaboración propia].

AMENAZAS	% DE QUE SE PRODUZCA LA AMENAZA	VALOR MONETARIO TOTAL APROXIMADO	CALCULO DEL EMV	VALOR MONETARIO ESPERADO SI SUCEDE LA VULNERABILIDAD
Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.	67%	\$700,000.00	$0.67 * 700,000$	\$469,000.00
Perdida de información a causa de ataques informáticos y/o virus.	50%	\$1,000,000.00	$0.50 * 1,000,000$	\$500,000.00
Infiltración de algún tipo de malware en la red del corporativo.	67%	\$900,000.00	$0.67 * 900,000$	\$603,000.00
Descarga de archivos infectados, por medio de sitios web.	50%	\$500,000.00	$0.50 * 500,000$	\$250,000.00
Robo de información mediante sitios web que piden datos personales y/o bancarios.	83%	\$900,000.00	$0.83 * 900,000$	\$747,000.00
Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	100%	\$900,000.00	$1.0 * 900,000$	\$900,000.00
Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.	67%	\$300,000.00	$0.67 * 300,000$	\$201,000.00

Ataques de tipo phishing al correo electrónico de los usuarios.	83%	\$400,000.00	$0.83 * 400,000$	\$332,000.00
Ataques de tipo spoofing al servicio de correo electrónico de la empresa.	83%	\$400,000.00	$0.83 * 400,000$	\$332,000.00

Con esta evaluación cuantitativa se pueden priorizar las diferentes vulnerabilidades y amenazas en base a su Valor Monetario Esperado (EMV) del impacto que causaría si cada una o alguna de estas llegase a ocurrir en Equilibrio Farmacéutico. Sin embargo, para tener los costos más exactos de que se produzca una vulnerabilidad es necesario realizar todo el análisis de este monto monetario con un experto en el área.

Actividad 3.4. Priorizar amenazas y vulnerabilidades en los servicios de TI.

Descripción de la actividad.

Para el desarrollo de esta actividad se tienen que priorizar las diferentes amenazas y vulnerabilidades tomando como referencia las evaluaciones cualitativa y cuantitativa previamente realizadas, para así poder atenderlas por su nivel de prioridad.

Resultado de la actividad.

Las tablas que se presentan a continuación contienen las vulnerabilidades y amenazas de acuerdo con su nivel de prioridad en base a su evaluación cualitativa y cuantitativa.

Tabla 22 Vulnerabilidades por orden de prioridad [Elaboración propia].

NIVEL DE PRIORIDAD	VULNERABILIDAD	NIVEL DE IMPACTO CUALITATIVO	NIVEL DE IMPACTO CUANTITATIVO
1	Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	100%	\$1,000,000.00
2	Los archivos que son compartidos mediante SharePoint no sean analizados en busca de virus.	83%	\$747,000.00

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

3	Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	83%	\$738,000.00
4	Los equipos de cómputo no tengan un antivirus actualizado.	67%	\$670,000.00
5	Los archivos que se suben a la nube no sean analizados en busca de virus.	67%	\$536,000.00
6	No contar con una protección para la información almacenada de manera local en los dispositivos.	50%	\$500,000.00
7	Se pueda ingresar a sitios web que no son seguros.	67%	\$402,000.00
8	Hay poco control sobre los sitios web y/o plataformas de streaming a las que acceden los empleados de la empresa.	50%	\$400,000.00
9	Los usuarios hagan caso omiso a las recomendaciones por parte del área de TI para identificar un correo de tipo SPAM.	50%	\$350,000.00
10	Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	67%	\$335,000.00
11	Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	67%	\$268,000.00
12	Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.	50%	\$150,000.00

Tabla 23 Amenazas por orden de prioridad [Elaboración propia].

NIVEL DE PRIORIDAD	AMENAZA	NIVEL DE IMPACTO CUALITATIVO	NIVEL DE IMPACTO CUANTITATIVO
1	Ciberataque por medio de sitios web no seguros o aparentemente oficiales.	100%	\$900,000.00
2	Robo de información mediante sitios web que piden datos personales y/o bancarios.	83%	\$747,000.00

3	Ataques de tipo phishing al correo electrónico de los usuarios.	83%	\$332,000.00
4	Ataques de tipo spoofing al servicio de correo electrónico de la empresa.	83%	\$332,000.00
5	Infiltración de algún tipo de malware en la red del corporativo.	67%	\$603,000.00
6	Perdida de información a causa de ataques informáticos y/o virus.	50%	\$500,000.00
7	Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.	67%	\$469,000.00
8	Descarga de archivos infectados, por medio de sitios web.	50%	\$250,000.00
9	Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.	67%	\$201,000.00

Una vez teniendo la priorización de las vulnerabilidades y amenazas, se tienen que proponer diversas medidas de seguridad para solucionar cada una de estas.

Actividad 3.5. Revisar los controles de seguridad en el área de TI para entender su eficacia y su mejora.

Descripción de la actividad

Para esta actividad se deben de revisar los controles de seguridad con los que cuenta actualmente la empresa con la finalidad de verificar que realmente estén cumpliendo con su función o de lo contrario implementar una nueva medida de seguridad o aplicar una mejora a dichos controles.

Por otra parte, para realizar la conclusión sobre la efectividad de cada control a evaluar se va a utilizar la escala de madurez en base al modelo COBIT el cual se aborda a continuación:

- Nivel 0 (Inexistente): Falta de un proceso reconocible en donde la empresa no ha reconocido que existe un problema a resolver.
- Nivel 1 (Inicial): Existe evidencia de que la organización ha reconocido las problemáticas y que tienen que ser resueltas. Sin embargo, no hay procesos

estandarizados, pero existen métodos ad hoc que tienen que ser aplicados de forma individual o caso por caso.

- Nivel 2 (Repetible): Se han desarrollado los procesos a tal grado en que diversas personas procedimientos similares realizando la misma tarea. Sin embargo, no existe una capacitación o comunicación formal de los procedimientos estándar dejando la responsabilidad a la persona. Se tiene un alto grado de confianza en la persona causando la alta probabilidad de que haya errores.
- Nivel 3 (Definida): Los procedimientos se han estandarizado y documentado, y comunicado a través de capacitaciones. Sin embargo, es poco probable que se detecten desviaciones debido a que se ha dejado en manos de la persona el seguimiento de estos procesos. Dichos procedimientos no son sofisticados, no obstante, son la formalización de la practicas existentes.
- Nivel 4 (Administrada): Existe la posibilidad de monitorear y medir el cumplimiento de los procesos, además de actuar en donde los procesos no funcionan efectivamente. Se utilizan la automatización y herramienta de forma limitada.
- Nivel 5 (Optimizada): Los procesos se encuentran refinados hasta un nivel de mejores prácticas, basados en resultados de mejora continua y diseño de madurez con otras organizaciones. TI se utiliza de forma integrada automatizando el flujo de trabajo, brindando herramientas que mejoran la calidad y efectividad, haciendo que la empresa se adapte con rapidez.

Resultado de la actividad

A continuación, se presenta un formato la cual ayudara a poder revisar los controles de seguridad con los que cuenta actualmente la empresa y verificar que realmente estén cumpliendo con su objetivo de control. Primeramente, se revisará el control del antivirus de Panda en su versión empresarial siendo este su principal medida de protección para la empresa. Como primera parte de revisión se presenta una tabla la cual brinda un contexto sobre el control de seguridad a revisar.

Tabla 24 Primera parte de revisión del primer control de seguridad [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

Objetivo de control	Descripción del riesgo	Actividades de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control
Proteger los equipos y la red de la empresa ante un ciberataque o la infiltración de algún tipo de amenaza como virus, para salvaguardar la información que es encontrada almacenada ya sea de manera local o en la nube, además de no generar una interrupción en las actividades a causa del riesgo mencionado.	Infiltración de un virus a algún equipo de cómputo por medio de la red de la empresa debido a que las medidas de seguridad no cubren con todas las necesidades.	Tener un antivirus el cual tenga su base de datos de virus actualizada constantemente y verificar que cubra con las necesidades de protección de la empresa.	La empresa actualmente cuenta con un antivirus actualizado, sin embargo, este no cubre con todas las necesidades de seguridad y protección de la empresa.	Anual	Automático

Como segunda parte se muestra la siguiente tabla la cual ayuda a “determinar si las actividades de control operan de manera efectiva para prevenir errores”.

Tabla 25 Segunda parte de revisión del primer control de seguridad [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

Descripción del plan de prueba			Método y cantidad de selección de partidas	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia
Analizar	si	las características y/o funciones que brinda el antivirus con el que actualmente cuenta EQF cubre con las necesidades de la empresa.	Casual / 1	Se encontró que las características y funciones con las que cuenta el antivirus no son suficientes para cubrir las necesidades de protección de la empresa, como protección de correo electrónico, depende del usuario para que el antivirus cumpla con la protección deseada.	La efectividad tiene nivel de madurez de 3.	1. Investigación de características del antivirus Panda en su versión empresarial. Revisar actividad 5.1 para la evidencia. 2. Comparación de las características con las necesidades de protección que requiere la empresa. Revisar actividad 5.1 para la evidencia.

Ahora se revisará el segundo control de seguridad que son las reglas de restricción para el bloqueo de acceso a sitios web. Como primera parte de revisión se muestra una segunda tabla la cual brinda un contexto sobre el control de seguridad a revisar.

Tabla 26 Primera parte de revisión del segundo control de seguridad [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

Objetivo de control	Descripción del riesgo	Actividades de control	Descripción de la actividad de control	Periodicidad de la actividad de control	Clasificación de la actividad de control
Brindar seguridad al momento de que	Daños en los servicios de la	Establecer reglas de restricción de	La empresa cuenta con dichas reglas de	Anual	Manual

un usuario se encuentre navegando en internet, bloqueando aquellos sitios web que no sean seguros o plataformas de streaming que puedan afectar el servicio de internet además de las actividades que requieran este servicio.	empresa a causa de ciberataque por el incumplimiento de políticas de restricción o mal uso de aplicativos por parte de los usuarios.	acceso a sitios web que no son seguros y/o plataformas de streaming (Spotify, Netflix, entre otras).	restricción de acceso, mismas que se pueden establecer en el propio antivirus.		
--	--	--	--	--	--

Como segunda parte se muestra la siguiente tabla la cual ayuda a “determinar si las actividades de control operan de manera efectiva para prevenir errores”.

Tabla 27 Segunda parte de revisión de seguridad control de seguridad [Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de la información, 2009].

Descripción del plan de prueba	Método y cantidad de selección de partidas	Resultados de la prueba	Conclusión sobre efectividad	Referencia de la evidencia
Realizar una auditoria ingresando a equipos de cómputo al azar por medio del aplicativo TeamViewer y verificar si se tiene el acceso a sitios web no seguro, al igual que las	Casual / 250	Se logro observar que en algunos dispositivos se puede ingresar a los sitios web que no son seguros, al igual que páginas web como YouTube o plataformas de streaming las cuales utilizan	La efectividad tiene nivel de madurez de 2.	Se ingreso a varios equipos de cómputo por medio de TeamViewer y se navegó por sitios web no seguros y plataformas de streaming. Revisar en

plataformas de streaming, con la finalidad de revisar que las reglas de acceso efectivamente se estén cumpliendo.		más recursos del servicio de internet, lo que puede provocar afectaciones en el rendimiento de actividades.		el apartado de Anexos el anexo 1.
---	--	---	--	-----------------------------------

Como se puede observar en la revisión de los controles que se tienen actualmente en la empresa, estos no cumplen del todo con su objetivo de control o propósito, dado que en los resultados de las pruebas que se llevaron a cabo se llegó a la conclusión que los controles no son tan efectivos ya que no cumplían del todo con sus funciones y en algunos casos dependían mucho del usuario para que la protección tanto de los equipos como de la información se lograra con éxito.

Objetivo 4. Proponer estrategias de seguridad según análisis y necesidades de la empresa.

El objetivo se enfoca en realizar una estrategia de seguridad de la información y dispositivos de la empresa, en base a las necesidades que esta tenga. Para ello se busca implementar medidas de seguridad que abarquen las vulnerabilidades, además de mitigar y gestionar los riesgos evaluados anteriormente.

Actividad 4.1. Proponer estrategias de seguridad de acuerdo con las necesidades de la empresa.

Descripción de la actividad

Para esta actividad se deben de realizar las propuestas de medidas de seguridad de acuerdo con las necesidades de la empresa, tomando en cuenta la solución de los diversos riesgos, amenazas y vulnerabilidades que se reflejaron durante el análisis previo, además de ello se tomara como referencia las recomendaciones del estándar ISO 17799 y posteriores.

Resultado de la actividad

Primera propuesta de medida de seguridad.

A continuación, se presenta una tabla con la primera propuesta en base al primer riesgo que se tiene Equilibrio Farmacéutico, además de su posible solución ante este riesgo y finalmente la justificación del porque se tiene que dar de esa manera dicha solución.

Tabla 28 Propuesta de solución del primer riesgo [Elaboración propia].

RIESGO	
Bloquear el acceso a la información que sea de gran importancia para la empresa a causa de un ciberataque.	
VULNERABILIDAD	AMENAZAS
V1. No contar con una protección para la información almacenada de manera local en los dispositivos. V2. Los archivos que se suben a la nube y que son compartidos mediante SharePoint no sean analizados en busca de virus. V4. Los archivos, imágenes y/o videos que son compartidos por Teams no sean analizados en busca de malware.	A1. Nuevas formas de realizar un ciberataque. A2. Creación de nuevos virus. A3. Robo o secuestro de información que sea de gran importancia para la empresa. A4. Perdida de información que se encuentre en un archivo infectado.
PROPUESTA DE SOLUCIÓN	
Hacer una auditoria para saber que dispositivos tienen la información almacenada de manera local, posteriormente crear un plan para migrar la información que se encuentre localmente al servicio de la nube con el que se cuenta actualmente. Para aquellos dispositivos en los que no se cuente con dicho servicio de la nube, crear un proceso de respaldo de la información cada cierto tiempo y almacenar ese respaldo en otros medios y finalmente hacer un seguimiento para verificar que se estén realizando dichos respaldos de información. Implementar un antivirus que permita proteger de manera local la información. Implementar Defender para Office 365 en Microsoft Teams con el propósito de proteger la información, además de analizar los archivos que sean compartidos por medio de Teams.	
JUSTIFICACIÓN DE LA SOLUCIÓN	FUNDAMENTACIÓN TEORICA
Debido a que existen dispositivos en la empresa funcionando con discos duros mecánicos, estos se pueden dañar con más frecuencia, además de que no	En base a la ISO 17799 apartado 10.5 Respaldo o Back-Up, “Se debieran establecer los procedimientos de rutina para implementar la

son tan eficientes a diferencia de otros discos duros, representando un gran riesgo para la información que se encuentre almacenada localmente, por lo que resulta necesario establecer un respaldo en otros medios además de hacer un seguimiento de dichos respaldos para tener acceso a la información más reciente en caso de pérdida. Por otra parte, actualmente una de las mejores opciones para tener almacenada la información es mediante el servicio de la nube por lo que es necesario migrar los archivos que tengan mayor importancia a este servicio y de esta manera no haya pérdida de información en caso de que se llegara a dañar un disco duro. Finalmente, es necesario tener protección en los dispositivos y servicios para prevenir ataques informáticos y que puedan acceder a la información almacenada para darle un mal uso u obtener algún tipo de beneficio principalmente monetario.	política de respaldo acordada y la estrategia para tomar copias de respaldo de la data y practicar su restauración oportuna.” Además de ello se deben “proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios”
--	---

En seguida se muestra la segunda propuesta la cual cubre los siguientes dos riesgos los cuales van de la mano, por lo que la propuesta que se presenta dará la posible solución a estos dos riesgos.

Tabla 29 Propuesta de solución del segundo y tercer riesgo [Elaboración propia].

RIESGO	
Daños en los servicios de la empresa a causa de ciberataque por el incumplimiento de políticas de restricción o mal uso de aplicativos por parte de los usuarios. Daño de equipos de cómputo debido a la infección de algún tipo de virus.	
VULNERABILIDAD	AMENAZAS
V1. Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	A1. Nuevas formas de realizar un ciberataque, además de creación de nuevos virus.

V2. Parte de los usuarios hacen caso omiso a las recomendaciones por parte del área de TI para identificar correos de tipo SPAM. V4. Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	A3. Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo. A4. Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia. A5. Ataques de tipo phishing al correo electrónico de los usuarios. A6. Ciberataque por medio de sitios web no seguros o aparentemente oficiales.
---	--

PROPUESTA DE SOLUCIÓN

Crear un plan el cual informe de manera sencilla a los usuarios acerca de los ataques más comunes de los cuales pueden ser víctimas y cuáles serían las sanciones o consecuencias en caso de que algún ciberataque o infección de un virus suceda.

Crear una política la cual contenga sanciones para aquellos usuarios que hagan caso omiso a las medidas de seguridad implementadas.

JUSTIFICACIÓN DE LA SOLUCIÓN

De acuerdo con el análisis previo que se llevó a cabo se puede deducir que el desconocimiento acerca de la seguridad informática, así como posibles ataques o virus por parte de los usuarios puede poner en riesgo tanto la información de la empresa como los equipos de cómputo, por lo que es importante mantener informado a los usuarios cada cierto tiempo acerca de este tema, ya que no solamente basta con implementar varias medidas de seguridad por parte del área de TI, si no también es responsabilidad del usuario respetar las políticas de restricción así como recomendaciones que se lleguen ya que de lo contrario estarían poniendo en riesgo diversos activos entre ellos el más importante la información de la empresa

FUNDAMENTACIÓN TEORICA

De acuerdo con la ISO 17799 apartado 10.4 Protección contra el código maliciosos y móvil, se requiere tomar precauciones para la evitar y detectar la introducción de algún tipo de código malicioso, algún tipo de virus o un ciberataque. Además de ello los “usuarios debieran estar al tanto de peligros de códigos maliciosos, virus y/o ciberataques.

Por otro lado, en el apartado 10.4.1 Controles contra códigos maliciosos, se tiene que establecer una política prohibiendo el uso de software no autorizado.

A continuación, se presenta la tercera propuesta la cual va a solucionar el cuarto y quinto riesgo los cuales van enlazados.

Tabla 30 Propuesta de solución del cuarto y quinto riesgo [Elaboración propia].

RIESGO	
La empresa sea víctima de un ciberataque debido a que las medidas de seguridad no cubren con todas las necesidades de la empresa.	
Infiltración de un virus a algún equipo de cómputo por medio de la red de la empresa debido a que las medidas de seguridad no cubren con todas las necesidades.	
VULNERABILIDAD	AMENAZAS
V1. Aunque existe un antivirus este no cubre con todas las necesidades de protección de la empresa.	A1. Nuevas formas de realizar un ciberataque, además de creación de nuevos virus.
V2. La protección de correo electrónico no es suficiente para cubrir adecuadamente las necesidades de la empresa.	A3. Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.
V3. Los equipos de cómputo no tengan un antivirus actualizado.	A4. Ciberataques al servicio de correo electrónico como correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.
	A5. Ciberataque por medio de sitios web no seguros o aparentemente oficiales.
	A6. Infiltración de algún tipo de malware dentro de la red del corporativo.
PROPUESTA DE SOLUCIÓN	
Implementar un nuevo antivirus que pueda cubrir las necesidades de la empresa.	
Aplicar medidas de seguridad como respaldo de información, actualizar la base de datos de virus del antivirus para proteger los equipos de cómputo, la información y los servicios que son utilizados cotidianamente.	
JUSTIFICACIÓN DE LA SOLUCIÓN	FUNDAMENTACIÓN TEORICA
En base a las vulnerabilidades se puede observar que actualmente la empresa cuenta con un antivirus instalado en sus dispositivos, sin embargo, este no es suficiente para cubrir totalmente o la mayor parte	En base a la norma ISO 17799, apartado 10.4.1 Controles contra códigos maliciosos, indica que el uso de dos o más software para protección puede mejorar la efectividad de la protección contra

de sus necesidades, por ello es importante buscar otra alternativa de antivirus la cual sea la más adecuada, ya que esta es una de sus medidas principales de seguridad para sus dispositivos. Además de ello, es importante también proteger la información que se encuentre almacenada en diversos medios y de igual manera establecer seguridad en los servicios que son utilizados día con día como el correo electrónico, la nube, entre otros.	códigos maliciosos, virus o ciberataques. También el apartado 11.4 Control de acceso a la red, menciona que el acceso del usuario a la redes y servicios de las redes no debieran comprometer la seguridad de los servicios de la red.
--	--

A continuación, se muestra la siguiente tabla la cual contiene la propuesta la cual da solución al sexto riesgo con el que cuenta actualmente la empresa.

Tabla 31 Propuesta de solución para el sexto riesgo [Elaboración propia].

RIESGO	
Afectaciones en el servicio de correo electrónico.	
VULNERABILIDAD	AMENAZAS
V1. Algunas medidas de seguridad dependen del usuario para que estas se cumplan correctamente.	A1. Nuevas formas de realizar un ciberataque.
V2. Algunos usuarios hacen caso omiso a las recomendaciones por parte del área de TI para identificar correos de tipo SPAM.	A2. Robo o secuestro de información que sea de gran importancia para la empresa.
V3. La protección de correo electrónico no es suficiente para cubrir adecuadamente las necesidades de la empresa.	A3. Descarga de archivos que contienen algún tipo de virus e infecten el equipo de cómputo.
	A4. Que lleguen correos de tipo SPAM, ya sea con un mensaje promocional o un asunto de emergencia.
	A5. Ciberataques al servicio de correo electrónico.
PROPUESTA DE SOLUCIÓN	
Aplicar una autenticación multifactor para los servicios de Office 365.	
Implementar directivas anti-spam y anti-phishing la cual detecte correos de tipo SPAM antes de que un usuario los abra o interactúe con ellos.	
Informar a los usuarios sobre los posibles ataques que pueden ocurrir mediante el servicio de correo electrónico con la finalidad de que sepan cómo actuar ante ellos si llegase a suceder.	
JUSTIFICACIÓN DE LA SOLUCIÓN	FUNDAMENTACIÓN TEORICA

En la actualidad no solamente basta con tener un correo electrónico y una contraseña como medida de seguridad para ingresar a una cuenta, hoy en día la autenticación multifactor es otro nivel de seguridad que se le ha añadido al inicio de sesión de las cuentas, ejemplo de ello es Office 365 el cual brinda este nivel de seguridad al ingresar al correo electrónico de Outlook, la nube, entre otros servicios o aplicativos. Por otro lado, es indispensable mantener conscientes a los usuarios sobre los ataques más comunes que se pueden presentar en el servicio de correo electrónico, ya que este medio es utilizado en la empresa para informar sobre asuntos importantes o de mayor relevancia, por lo que se debe de proteger este servicio ante correos de tipo SPAM.	En base a la norma ISO 17799 apartado 10.8.4 Mensajes electrónicos se debe proteger adecuadamente la información involucrada en mensajes electrónicos. Aunado a esto en el apartado 11.4.2 Autenticación del usuario para las conexiones externas, indica que se deben de "utilizar métodos de autenticación apropiados para controlar el acceso de usuarios."
--	--

En seguida se presenta la última propuesta de seguridad la cual cubre el ultimo riesgo reflejado en el análisis previo.

Tabla 32 Propuesta de solución para el séptimo riesgo [Elaboración propia].

RIESGO	
Afectación en el rendimiento de las operaciones y servicios de comunicación de la empresa, debido al mal uso de aplicativos y sitios web.	
VULNERABILIDAD	AMENAZAS
V1. Hay poco control y monitoreo hacia los usuarios para que estos no hagan mal uso de los aplicativos.	A1. Suplantación de sitios web oficiales, incluso teniendo el certificado HTTPS.
V3. Los usuarios no respeten las políticas de restricción de acceso a sitios web que no son seguros o plataformas de streaming (Spotify, Netflix, etc.).	A2. Descarga de archivos infectados por medio de sitios web. A3. Ciberataque por medio de sitios web no seguros o aparentemente oficiales.

V4. Afectación en el rendimiento del internet y comunicación para realizar actividades, debido al incumplimiento de las políticas de restricción.	
PROPUESTA DE SOLUCIÓN	
Implementar una política de restricción a acceso a plataformas de streaming y sitios web que no sean seguros o utilicen muchos recursos de internet. Crear sanciones para aquellos usuarios que no respeten dichas políticas. Crear un plan de monitoreo para tener un mayor control sobre los usuarios acerca del uso de estas plataformas de streaming o sitios web que no sean autorizados.	
JUSTIFICACIÓN DE LA SOLUCIÓN	FUNDAMENTACIÓN TEORICA
Debido a que algunos usuarios no respetan del todo las políticas de restricción de uso de plataformas de streaming y acceso a sitios web no seguros o que utilizan muchos recursos de internet, resulta necesario realizar un plan de monitoreo, además de crear sanciones para tratar esta vulnerabilidad, ya que teniendo algún tipo de consecuencia sobre los usuarios estos respetaran más las políticas de restricción, esto con la finalidad de no tener afectaciones tanto en la comunicación como en las actividades que sean de importancia entre sucursales y corporativo.	De acuerdo con la ISO 17799 apartado 10.10.1 Registro de auditoría, se debe de producir y mantener registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un periodo. Además, en el apartado 11.4.1 Control de conexión a la red, se indica que “Los usuarios sólo debieran tener acceso a los servicios para los cuales hayan sido específicamente autorizados.”

De acuerdo con las necesidades de la empresa y las soluciones que se propusieron para tener una mejoría en la protección de sus activos de TI, se llevaran a cabo la implementación de las siguientes propuestas:

- Como medida de seguridad principal se va a realizar la instalación de un nuevo antivirus (Kaspersky EDR Optimum) para la protección de los equipos de cómputo y la información que se encuentre almacenada localmente y en diversos servicios como la nube.

- Implementar políticas de restricción de acceso a sitios web no seguros y plataformas de streaming (Spotify, Netflix, etc.).
- Realizar la documentación sobre el antivirus de acuerdo con las necesidades de la empresa para posibles fallas de este y como resolver el conflicto.

CAPÍTULO IV

RESULTADOS

Objetivo 5. Implementar las medidas y/o estrategias de seguridad de acuerdo con las necesidades de la empresa.

Este objetivo se enfoca principalmente en implementar las medidas de seguridad según las necesidades de la empresa, tomando en cuenta el análisis previo a los diversos riesgos, vulnerabilidades y amenazas con las que Equilibrio Farmacéutico se enfrenta actualmente y así poder brindar la mejor protección tanto para la información como para sus dispositivos.

Actividad 5.1. Realizar un análisis general del antivirus y su funcionamiento, así como las ventajas del uso del antivirus Kaspersky en comparación con otros antivirus del mercado.

Descripción de la actividad

Realizar una investigación en diversas fuentes de información acerca del funcionamiento examinando como detectan y combaten ciberataques, así como destacar las principales ventajas de Kaspersky en comparación con otros antivirus disponibles en el mercado dando enfoque principalmente en la diferenciación con el antivirus de Panda. Posteriormente se realiza un análisis con la información recopilada resaltando los puntos más importantes como sus características, certificaciones, protección contra virus y ciberataques, medidas de seguridad que brinda. Esto ayuda a respaldar la toma de decisiones sobre las medidas y estrategias de seguridad que serán implementadas en la organización.

Resultado de la actividad

Comparativa de precios de antivirus en su versión empresarial.

A continuación, se presenta una tabla con la comparativa de los precios de diferentes antivirus tomando en cuenta la versión empresarial de cada uno de ellos. Dichos precios se consultaron en sus sitios web oficiales, de igual manera la cotización que se refleja en dicha tabla se realizó en base un total de 100 dispositivos por una un año de licenciamiento de cada uno de los antivirus, esto debido a que si se requiere hacer una cotización mayor a 100 dispositivos de debe de contactar directamente con la empresa del antivirus o con un partner oficial.

Tabla 33 Comparativa de precios de antivirus en su versión empresarial [Elaboración propia].

Antivirus en su versión empresarial.	Precio de cotización (100 dispositivos por un año de licencia).
	\$200,000.00
	\$110,090.00
	\$77,300.00
	\$59,000.00
	\$49,700.00

Como se puede observar los antivirus que ofrecen un mejor precio son Kaspersky y Panda, por lo que se tomara en cuenta estas dos opciones para realizar una comparación en base a sus funciones y algunas certificaciones de organizaciones encargadas de realizar pruebas de seguridad a diversos antivirus.

Comparación entre Kaspersky y Panda de las principales medidas de seguridad.

Se realizó una investigación en la documentación oficial de las versiones empresariales de Kaspersky y Panda, para hacer una comparativa entre estos dos antivirus dando lugar a las principales características y protección de ataques que estos pueden brindar en base a las necesidades de la empresa.

Una de las principales ventajas y gran diferenciador entre Panda y Kaspersky es la protección de la paquetería de Office 365, brindando mayor seguridad en sus aplicativos como Microsoft Exchange Online, usuarios de OneDrive y sitios de SharePoint Online, incluidos los archivos cargados o enviados a través de Microsoft Teams.

Dando lugar a una mayor protección en los mensajes de correo electrónico entrantes y salientes ya que se analizan automáticamente en busca de virus, troyanos y otros tipos de malware y ransomware que se puedan transmitir mediante correo electrónico.

La segunda ventaja que se logró identificar es que Kaspersky a diferencia de Panda, puede detectar ataques de tipo Spoofing, este tipo de ataques se basa en enviar mensajes de correo electrónico mediante la suplantación de identidad en el que utiliza una dirección de correo electrónico de una persona o entidad confiable, por lo que el destinatario no se dará cuenta fácilmente que está siendo víctima de este tipo de amenazas.

Este tipo de ataques pueden ser muy peligrosos ya que como se mencionó, al enviarse un correo de una persona confiable el remitente no se dará cuenta de que ese correo tiene una suplantación de identidad y con ello puede dar lugar a que sucedan otro tipo de ataques como el phishing que uno de los más comunes o que se infecte de otro tipo de virus.

Otro gran diferenciador es la protección ante un ataque de Mailsploit, este tipo de ataque se caracteriza por quitar todas las protecciones anti-phishing con las que se cuentan, lo cual provoca que se puedan infiltrar otro tipo de ataques como el spoofing, el phishing o infectarse de algún tipo de virus. Debido a que Kaspersky cuenta con protección de Office 365, es necesario de igual manera, tener medidas de seguridad ante este tipo de ataques.

Estas tres medidas de seguridad que brinda Kaspersky se adaptan perfectamente a las necesidades de la empresa debido a que las principales aplicaciones y servicios que se utilizan a diario como lo es el servicio de correo electrónico Outlook, Microsoft Teams, entre otros pertenecen a la paquetería de Office 365, por lo tanto al tener diversas herramientas y/o funciones de protección dedicadas específicamente a esta paquetería brinda más confianza a la organización en cuanto a la seguridad de los usuarios y la información.

Comparativa de certificaciones de las empresas más reconocidas que realizan pruebas de seguridad a antivirus.

A continuación, se presenta una tabla con tres de las principales organizaciones encargadas de realizar diversas pruebas de seguridad a diferentes antivirus que se encuentran actualmente en el mercado, sin embargo, se hará la comparativa entre los antivirus de Kaspersky y Panda en su versión empresarial. Cabe mencionar que consulto la información

en el sitio oficial de las organizaciones certificadoras, además de considerar las pruebas realizadas en este año en curso (2023).

Tabla 34 Comparativa de certificaciones entre Kaspersky y Panda en versiones empresariales [Elaboración propia].

			Antivirus en su versión empresarial	
			 Panda	 Kaspersky
Empresa certificadora.		% de amenazas bloqueadas en base a las pruebas realizadas por la organización.	No aplica	100%
		Aprobación para obtener la certificación.	No aprobado	Aprobado
		% de amenazas bloqueadas en base a las pruebas realizadas por la organización.	No aplica	100%
		Aprobación para obtener la certificación.	No aprobado	Aprobado
		% de amenazas bloqueadas en base a las pruebas realizadas por la organización.	98.9%	100%
		Aprobación para obtener la certificación.	Aprobado	Aprobado

Principales características de Kaspersky en base a la empresa SoftwareReviews.

En la tabla que se presenta a continuación se muestran algunas características que más resaltan del antivirus Kaspersky, dichas características fueron sometidas a pruebas realizadas por la empresa SoftwareReviews en la que se obtuvieron ciertos porcentajes de evaluación de acuerdo con las pruebas realizadas.

Tabla 35 Evaluación de las características más destacadas por SoftwareReviews [Elaboración propia].

Tipo de prueba	Porcentaje obtenido en la evaluación de prueba.	Descripción de la prueba realizada.
Detección dinámica de malware	90%	Aplicación de heurísticas a los archivos para identificar similitudes con malware conocido y bloquearlo.
Detección y respuesta de endpoints	89%	Detección activa de amenazas que soluciona malware y actividades maliciosas conocidas y desconocidas, aprovechando técnicas de aprendizaje automático.
Recuperación y eliminación de ransomware	89%	Recuperación de archivos eliminados y/o cifrados por ransomware.
Monitoreo de Kernel	86%	Monitoreo de procesos, memoria y archivos del sistema a nivel de SO.
Funcionalidad NGFW (Firewall de siguiente generación) del host	86%	Denegación predeterminada/lista blanca basada en políticas y verificación y confianza de aplicaciones (VPN/virtualización).
Control de puertos y dispositivos	86%	Cifrado de USB y prevención de pérdida de datos de terminales.

Mecanismos de contención de aplicaciones	85%	Protección basada en la nube y sandboxing.
Portal de administración centralizada	85%	Administración de múltiples clientes, capacidad de instalación automática, políticas integrales para diferentes grupos.

Certificaciones más importantes obtenidas en Kaspersky

AV-Test

“Es el instituto de investigación independiente en materia de seguridad informática de Alemania. Una de las mayores colecciones de códigos maliciosos de todo el mundo, el departamento de investigación propio del instituto y la intensa colaboración con otras instituciones garantizan pruebas de una categoría reconocida internacionalmente.” (AV-Test, s.f.).

De acuerdo con una evaluación del producto e informe de certificación AV-TEST en los meses de julio a agosto del año 2023, Kaspersky pudo obtener la certificación como TOP PRODUCT, dicha certificación es un galardón para productos destacados a partir de una puntuación total de 17,5 puntos.



Figura 14 Certificado TOP PRODUCT por AV-TEST. [AV-Test, s.f.]

A continuación, se muestra una tabla la cual contiene información acerca del tipo de prueba realizada al antivirus de Kaspersky en su versión empresarial por parte de la organización AV-Test, además de una descripción de dicha prueba realizada y la calificación obtenida.

Tabla 36 Calificación de pruebas realizadas por AV-Test [Elaboración propia].

Tipo de prueba	Calificación	Descripción de la prueba
Protección	6.0/6.0	Protección contra infecciones maliciosas (tales como virus, gusanos o troyanos).
Rendimiento	6.0/6.0	La influencia media del producto de seguridad en la velocidad del ordenador en el uso diario.
Usabilidad	6.0/6.0	Como repercute el software de seguridad en la utilidad de todo el ordenador.

SE Labs

“Es una empresa que evalúa productos y servicios de seguridad. Tiene como objetivo mejorar la seguridad de la tecnología de la información mediante la evaluación de productos y servicios diseñados para detectar ataques, proteger contra intrusiones o ambos. Probamos una gama de soluciones que incluyen software de endpoint, dispositivos de red y servicios en la nube” (SE Labs, s.f.)

De acuerdo con una evaluación del producto Endpoint Security (EPS): Enterprise 2023 Q3 realizada entre los meses de julio a septiembre del presente año 2023 Kaspersky pudo obtener la certificación AAA de SE Labs como Enterprise Endpoint Security.



Figura 15 Certificación AAA de SE Labs como Enterprise Endpoint Security [SE Labs, s.f.]

En la tabla que se muestra a continuación, contiene información acerca del tipo de prueba realizada al antivirus de Kaspersky en su versión empresarial por parte de la empresa SE Labs, al igual que la descripción de dicha prueba realizada y la calificación obtenida.

Tabla 37 Calificación de pruebas realizadas por SE Labs [SE Labs, s.f.].

Porcentaje de la exactitud de protección	Tipo de ataque		Puntuación general
	Tipo de amenaza	Puntuación	
100%	Ataques generales	75	100
La precisión de la protección representa la capacidad del producto para detectar y detener amenazas en esta prueba.	Ataques dirigidos	25	

AV Comparatives

“Es una organización que ofrece pruebas sistemáticas que comprueban si el software de seguridad, como los productos antivirus basados en PC/Mac y las soluciones de seguridad móvil, está a la altura de sus promesas. La certificación de AV-Comparatives proporciona un sello oficial de aprobación para el rendimiento del software que es reconocido a nivel mundial.” (AV Comparatives, s.f.)²².

De acuerdo con una evaluación de pruebas de seguridad por AV Comparatives en los meses de marzo a junio del año 2023, Kaspersky pudo obtener la certificación como Approved Business Security Product Award, dicha certificación se puede obtener con una puntuación de al menos el 90% en la prueba de protección contra malware, además, los productos deben obtener una puntuación de al menos el 90 % en la prueba general de protección en el mundo real.



Figura 16 Certificación Approved Business Security Product Award por AV Comparatives. [AV Comparatives, s.f.]

A continuación, se muestra una tabla la cual contiene información acerca del tipo de prueba realizada al antivirus de Kaspersky en su versión empresarial por parte de la organización AV Comparatives, además de una descripción de dicha prueba realizada y el porcentaje de amenazas bloqueadas.

Tabla 38 Porcentaje de amenazas bloqueadas en pruebas realizadas por AV Comparatives [AV Comparatives, s.f.].

Tipo de prueba	% de amenazas bloqueadas	Descripción de prueba
Protección en el mundo real	100%	El resultado obtenido se basa en un conjunto de pruebas que consta de 526 casos de prueba (como URL maliciosas), probados desde marzo - junio de 2023.
Protección contra malware	99.6%	El resultado obtenido se basa en la prueba de protección contra malware empresarial.

5.2 Hacer la planeación, justificación y negociación del uso del antivirus Kaspersky como nuevo método de protección de sistemas en la empresa.

Descripción de la actividad

En esta actividad se debe de realizar la planeación, contemplar las posibles reuniones que se llevarán a cabo para la negociación del nuevo antivirus que se va a implementar, para

ello se tiene que buscar primeramente el mejor proveedor del antivirus de Kaspersky realizando una comparativa entre sus partner, posteriormente se debe de realizar una negociación con el proveedor para buscar el licenciamiento que más se adecue a las necesidades de las empresa, después se debe de hacer una reunión con el gerente de TI para exponer las cotizaciones de los proveedores y finalmente una reunión con el Director General de Equilibrio Farmacéutico y el gerente de TI para la autorización del proyecto.

Resultado de la actividad

Comparación de proveedores del antivirus de Kaspersky

En la tabla que se presenta a continuación se muestran cinco opciones de los mejores partner oficiales del antivirus de Kaspersky, en los que refleja el rango que tienen dentro del programa de afiliados de Kaspersky y la ubicación donde se encuentran sus instalaciones (Kaspersky, 2023)²³.

Tabla 39 Partner Oficiales de Kaspersky [Elaboración propia].

Partner distribuidor de Kaspersky	Nivel de socio	Ubicación
ARRME Consultores, S.C.	Platinum Partner	Cuautitlan Izcalli
TODO EN LA NUBE S DE R.L DE C.V.	Platinum Partner	Naucalpan
Sistemas Stone	Platinum Partner	Ecatepec de Morelos
CRONOS NETWORKS S.A. DE C.V.	Platinum Partner	Ciudad de México
Tecnec One	Gold Partner	Ciudad de México

Ahora se muestra una tabla con la comparativa de precios que brindan los distintos proveedores, en la que se da un presupuesto de licencia por equipo durante un año de servicio del antivirus Kaspersky.

Tabla 40 Comparativa de precios de partner de Kaspersky [Elaboración propia].

Partner distribuidor de Kaspersky	Precio total de licencia por equipo durante 1 año
	\$470.00

ARMME CONSULTORES, S.C	
 T O D O E N LA NUBE TODO EN LA NUBE S DE R.L. DE C.V.	\$ 430.00
 SISTEMAS STONE	\$390.00
 CRONOS NETWORKS S.A. DE C.V.	\$ 450.00
 TECNEC ONE	\$500.00

De acuerdo con las comparativas de las tablas anteriores se puede deducir que la mejor opción en cuanto a costos, ubicación y nivel de socio en Kaspersky es Sistemas Stone por lo que posteriormente se contactara con el proveedor para realizar la negociación de las licencias.

Negociación de licenciamiento para los equipos de Equilibrio Farmacéutico

Para realizar la negociación con el proveedor de Sistemas Stone se contempla hacer una reunión la primera semana de diciembre del año 2023 en la cual se tiene como objetivo obtener el mejor costo para un total de 560 licencias las cuales representan los equipos con los que cuenta Equilibrio Farmacéutico.

Durante la reunión que se llevó a cabo con el proveedor se logró obtener un licenciamiento durante tres años de servicio de Kaspersky para los 560 equipos contemplados con el mejor costo posible, además de que se pudo obtener un descuento de licencia por parte del proveedor debido a los tres años de servicio que se negociaron.

A continuación, se muestra una tabla con la comparativa del precio inicial, el precio que se logró obtener y el precio total de la negociación.

Tabla 41 Comparativa de precios de licenciamiento [Elaboración propia].

Precio inicial de licencia por equipo durante un año	Precio obtenido de licencia por equipo durante 3 años	Precio total obtenido para los 560 equipos durante 3 años de licenciamiento
\$390	\$374.73	\$209,848.80

Reuniones con el director general de Equilibrio Farmacéutico y el gerente de TI para exponer costos de la implementación del proyecto.

Después de realizar la negociación con el proveedor, se tiene que realizar una reunión con el gerente de TI el día 11 de diciembre del año 2023 para exponer los costos de los proveedores que se contemplaron y cuál de estos resulta ser la mejor opción, además de mencionar la negociación que se logró obtener con el proveedor al que se decidió contratar de acuerdo a las necesidades de la empresa.

Posteriormente, se contempla realizar una reunión el día 13 de diciembre del año 2023 con el Gerente de TI y el Director General del corporativo de Equilibrio Farmacéutico, en la cual se va a exponer los beneficios de implementar un nuevo antivirus como nueva medida de seguridad tanto para los equipos como para los servicios que se utilizan día con día, además de ello mencionar que se contemplaron los diversos antivirus disponibles en el mercado y que se optó por implementar el antivirus Kaspersky en su nivel empresarial, de igual manera se mencionaran los principales proveedores de Kaspersky y cuál de ellos ofrecía la mejor opción monetaria.

Durante la reunión que se llevó a cabo el día 11 de diciembre del año 2023, el director general de Equilibrio Farmacéutico dio la autorización para llevar a cabo la implementación del proyecto de la instalación del nuevo antivirus acompañado de las nuevas medidas de

seguridad, por lo que se contempla pagar el licenciamiento de los equipos la primera semana del mes de enero del año 2024 (Anexo 1) y así poder iniciar con la instalación del antivirus.

Actividad 5.3 Crear una estrategia y plan de implementación del software antivirus en los dispositivos de la corporativo y sucursales de EQF.

Descripción de la actividad

Para realizar esta actividad se debe de hacer la estrategia y planeación de instalación del antivirus en los equipos de cómputo del corporativo y sucursales, en las que se tiene que priorizar en base a sus ventas y/o nivel de operación durante el día, para que de esta manera no se llegue a tener una afectación significativa durante el proceso de instalación.

Resultado de la actividad

Para iniciar con la implementación del nuevo antivirus se deben de considerar los siguientes aspectos:

- Contemplar el tipo de impacto o afectación tendrá la instalación en los equipos, esto debido a que no todos los dispositivos tienen las mismas características de hardware por lo tanto se debe tener en cuenta si la instalación del antivirus afectara o no, en el rendimiento de los dispositivos.
- Considerar el tiempo aproximado que tardara la instalación por dispositivo, esto con la finalidad de no interrumpir tanto tiempo en las actividades del usuario, además de avisarle para que tenga en consideración el tiempo en que se realizara la instalación.
- Tener en cuenta el nivel de prioridad de actividades de cada área y/o sucursal, esto quiere decir que para aquellas áreas y/o sucursales que tengan mayor nivel de operación, la instalación se debe de realizar primero además de la manera más rápida posible de acuerdo con las características de los dispositivos.

Una vez considerando los puntos anteriores, se continua con el plan de implementación del antivirus para ello primeramente se empezará por instalarlo en los dispositivos del corporativo siendo este el principal objetivo para la protección de los equipos e información y posteriormente se continuará con la instalación en las demás sucursales.

A continuación, se muestra el cronograma el cual presenta la instalación del antivirus por área durante una semana.

		DÍAS DE SEMANA DE IMPLEMENTACIÓN		
		Martes	Miercoles	Jueves
AREAS DE CORPORATIVO	TI			
	Gerentes de ventas			
	Insumos			
	Logística			
	RH			
	Contabilidad			
	SAP			
	Inventarios			
	Mercadotecnia			
	SGC			
	Líder de proyectos			
	Capacitación			
	Operaciones			
	Normatividad			
	Asuntos regulatorios			
	Planificación			
	Jurídico			
	Protección civil y Seguridad e higiene			

Figura 17 Cronograma de implementación de antivirus en dispositivos del corporativo. [Elaboración propia]

Posteriormente se continuará con la instalación en los dispositivos de las tres sucursales con mayor índice de actividades, las cuales son Iztapalapa I, Iztapalapa II y Ecatepec, por lo tanto, para llevar a cabo dicha instalación se consideran dos semanas. A continuación, se mostrar un cronograma indicando el tiempo de instalación del antivirus para estas 3 sucursales.

		SEMANAS DE IMPLEMENTACIÓN						
		PRIMERA SEMANA			SEGUNDA SEMANA			
		Martes	Miercoles	Jueves	Lunes	Martes	Miercoles	Jueves
SUCURSALES	Ecatepec							
	Iztapalapa I							
	Iztapalapa II							

Figura 18 Cronograma de implementación del antivirus en dispositivos de sucursales. [Elaboración propia]

Ya que se tienen los puntos a considerar para la instalación del antivirus y teniendo los cronogramas para asignar el tiempo de instalación tanto para el corporativo como para sucursales, lo que sigue es dar inicio con la implementación del nuevo antivirus.

Actividad 5.4 Instalar la versión empresarial del agente de Kaspersky en todos los equipos de cómputo de EQF con el propósito de asegurar su correcto funcionamiento.

Descripción de la actividad

Para el desarrollo de esta actividad se debe de instalar el aplicativo del antivirus Kaspersky en su versión empresarial que se proporcionara a todos los dispositivos de acuerdo con los cronogramas vistos en la actividad anterior, de igual manera contemplando los aspectos mencionados en la actividad anterior. Por lo tanto, se va a realizar la instalación del agente antivirus de Kaspersky primeramente todos los dispositivos del corporativo.

Resultado de la actividad

Para comenzar con la instalación del agente de Kaspersky en los equipos de cómputo, primeramente, se tiene que iniciar sesión con la cuenta administrador. En seguida se presenta una pantalla la cual muestra la empresa o el grupo de empresas que tienen contratado el servicio de Kaspersky. Por lo que se dará clic a la que corresponda, en este caso la de “Grupo Viso” (Empresa central a la cual EQF pertenece), posteriormente se desplegaran algunas opciones, entre ellas se tiene que seleccionar la opción de “Ir al espacio de trabajo” para poder acceder a la consola la cual administra todo lo referente al antivirus de Kaspersky.

Grupo Viso

Fecha de registro: 30/6/2023 9:24:18 (UTC -6:00)

Descripción: Grupo Viso

[Mostrar control de acceso](#)

Kaspersky Security Center Cloud Console
Número de espacios de trabajo: 1

[Grupo Viso](#)

[Ir al espacio de trabajo](#)

ID: c62fe0ab-19ad-4c40-af1b-f125a80b7898

Figura 19 Interfaz para poder acceder a la consola de administración de Kaspersky. [Elaboración propia]

A continuación, se presenta la interfaz donde se muestra el panel general sobre algunos eventos de ataques ocurridos, el estatus de protección de los dispositivos, amenazas que fueron detectadas, entre otras características. Además de ello, se muestran las diferentes opciones para poder llevar a cabo la administración de los dispositivos que están protegidos, políticas de restricción, operaciones, los usuarios y roles, configuración, entre otras opciones para poder llevar a cabo la administración de protección de los dispositivos.



Figura 20 Panel general de Kaspersky. [Elaboración propia]

Ahora para poder empezar con la instalación del agente de Kaspersky en cada uno de los dispositivos, se tiene que descargar el instalador de dicho agente. Para ello se debe ingresar al menú de “Descubrimiento y despliegue” el cual se encuentra en el panel de la parte izquierda de la interfaz; aquí se visualizan diversas opciones entre ellas la de “Despliegue y asignación” que es la que se debe de seleccionar para que despliegue las diversas opciones que esta contiene, de igual manera se muestran más opciones de las cuales se debe de seleccionar la de “Paquetes de instalación”, para ingresar y poder generar el instalador del agente de Kaspersky.

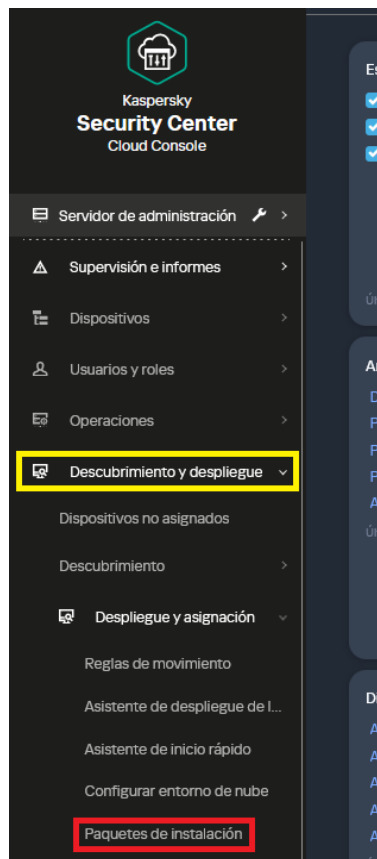


Figura 21 Menú para ingresar a la descarga del agente de Kaspersky. [Elaboración propia]

Una vez dentro de “Paquetes de instalación”, se presenta una pantalla la cual contiene diversos paquetes, sin embargo, el que se va a utilizar es el de “Kaspersky Security Center 14 Network Agent (Español (México)) 14 2.0.35148”, por lo tanto, se tiene que ingresar a esta opción dando clic.

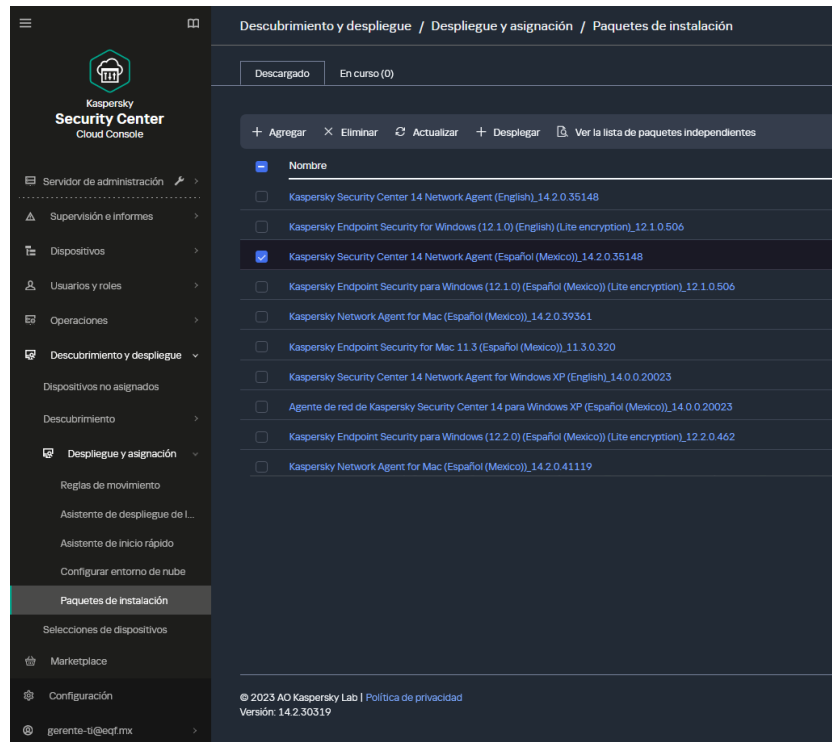


Figura 22 Paquetes de instalación (parte 1). [Elaboración propia]

Origen	Aplicación	Versión	Idioma	Tipo
Kaspersky	Kaspersky Security Center ...	14.2.0.35148	en	Aplicación
Kaspersky	Kaspersky Endpoint Securit...	12.1.0.506	en	Aplicación
Kaspersky	Kaspersky Security Center ...	14.2.0.35148	es-MX	Aplicación
Kaspersky	Kaspersky Endpoint Securit...	12.1.0.506	es-MX	Aplicación
Kaspersky	Kaspersky Network Agent f...	14.2.0.39361		Aplicación
Kaspersky	Kaspersky Endpoint Securit...	11.3.0.320		Aplicación
Kaspersky	Kaspersky Security Center ...	14.0.0.20023	en	Aplicación
Kaspersky	Agente de red de Kaspersky...	14.0.0.20023	es-MX	Aplicación
Kaspersky	Kaspersky Endpoint Securit...	12.2.0.462	es-MX	Aplicación
Kaspersky	Kaspersky Network Agent f...	14.2.0.41119		Aplicación

Figura 23 Paquetes de instalación (parte 2). [Elaboración propia]

Dentro del paquete de instalación se muestran sus propiedades que este contiene como la información general del paquete, la configuración, sus paquetes independientes de instalación y el historial de las versiones del agente. La propiedad a la que se debe de ingresar para la descarga del agente es la de “Paquetes independientes”.



Figura 24 Propiedades del paquete independiente. [Elaboración propia]

Dentro de los paquetes independiente se muestran dos opciones, sin embargo, la que es de interés para la descarga del agente es la primera de ellas, por lo tanto, se tiene que seleccionar, después se debe de dar clic en “Descargar” y se comenzara a realizar la descarga del instalador del agente de Kaspersky.

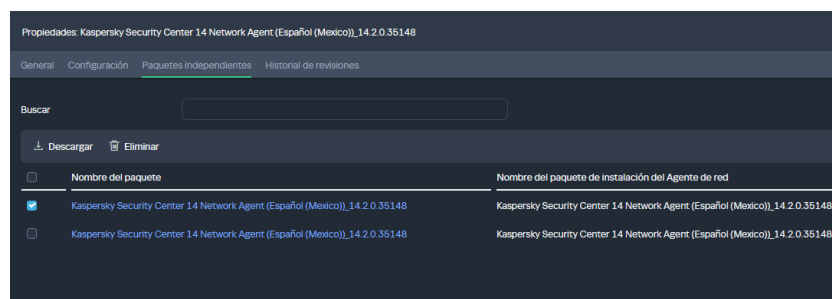
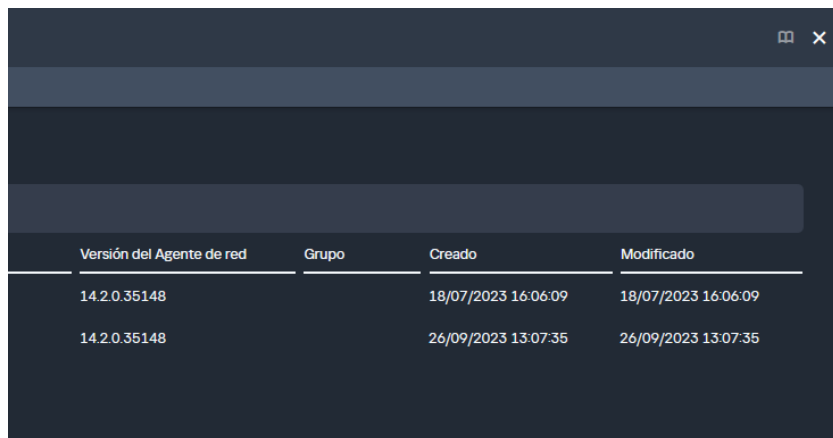


Figura 25 Opciones del instalador del agente de Kaspersky (parte1). [Elaboración propia]



Versión del Agente de red	Grupo	Creado	Modificado
14.2.0.35148		18/07/2023 16:06:09	18/07/2023 16:06:09
14.2.0.35148		26/09/2023 13:07:35	26/09/2023 13:07:35

Figura 26 Opciones del instalador del agente de Kaspersky (parte 2). [Elaboración propia]

A continuación se muestra el ejecutable del agente del antivirus de Kaspersky que se genera a partir de la consola de administración, el cual se tiene que instalar posteriormente en los dispositivos de EQF.

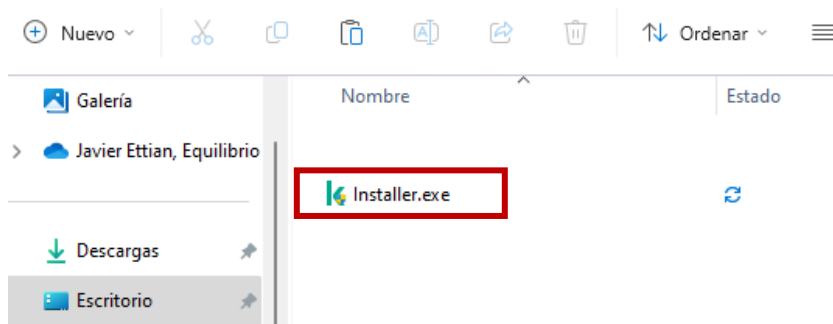


Figura 27 Archivo ejecutable del agente. [Elaboración propia]

Para iniciar con la instalación se debe de ejecutar el instalador del agente como administrador, después se mostrará la interfaz para iniciar con la instalación del agente, por lo que se tiene que dar clic en el botón de “Iniciar instalación” y comenzara con el proceso de instalación en el dispositivo.

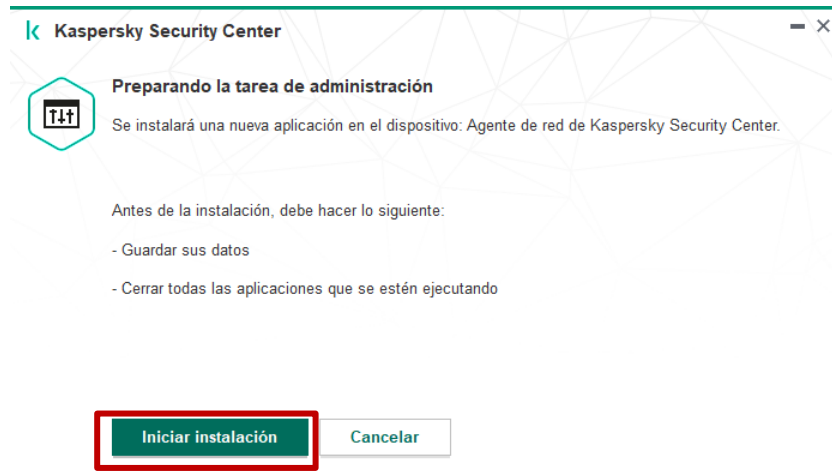


Figura 28 Comienzo de instalación del agente. [Elaboración propia]

Posteriormente se mostrará otra ventana donde se muestra el avance del proceso de instalación el cual conste de tres procesos, el primero de ellos es la extracción del archivo a una ubicación temporal, después la instalación del agente y por último se comprueba la conexión al servidor de administración.



Figura 29 Proceso de instalación. [Elaboración propia]

Ya que se terminó exitosamente el proceso de instalación del agente, el último paso que queda es dar clic en el botón de “Aceptar”.



Figura 30 Termino del proceso de instalación del agente de Kaspersky. [Elaboración propia]

Para comprobar que se instaló el agente de Kaspersky en el dispositivo, se debe de ingresar a los programas que están instalados en el dispositivo y verificar que el agente de Kaspersky se encuentre aquí.

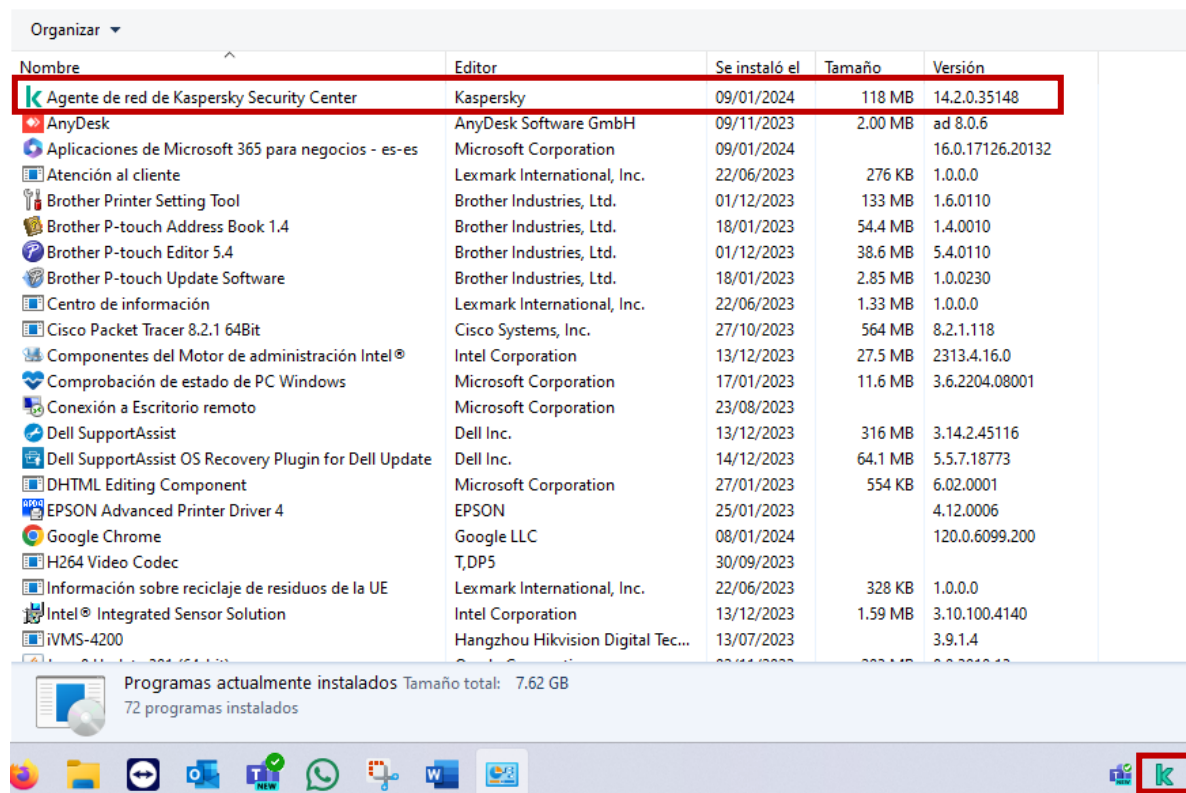


Figura 31 Comprobación de la instalación del agente de Kaspersky. [Elaboración propia]

Después de que se instaló del agente de Kaspersky en los dispositivos, lo que sigue es asignarlos al grupo de EQF para poder instalar el antivirus en dichos equipos de este grupo. Para esto en el menú de la parte izquierda se muestra la opción de “Descubrimiento y

despliegue” a la cual se le dará clic para desplegar su menú de opciones, dentro de estas se dará clic en la opción de “Dispositivos no asignados”. Aquí se mostrarán todos los dispositivos en los que se ha instalado el agente y no han sido asignados a un grupo para su administración.

Ahora para mover un dispositivo a un grupo, primeramente, se debe de seleccionar el dispositivo el cual se va a mover y después de tiene que dar clic en la opción de “Mover a un grupo” la cual se encuentra en el menú de la parte superior de los dispositivos.

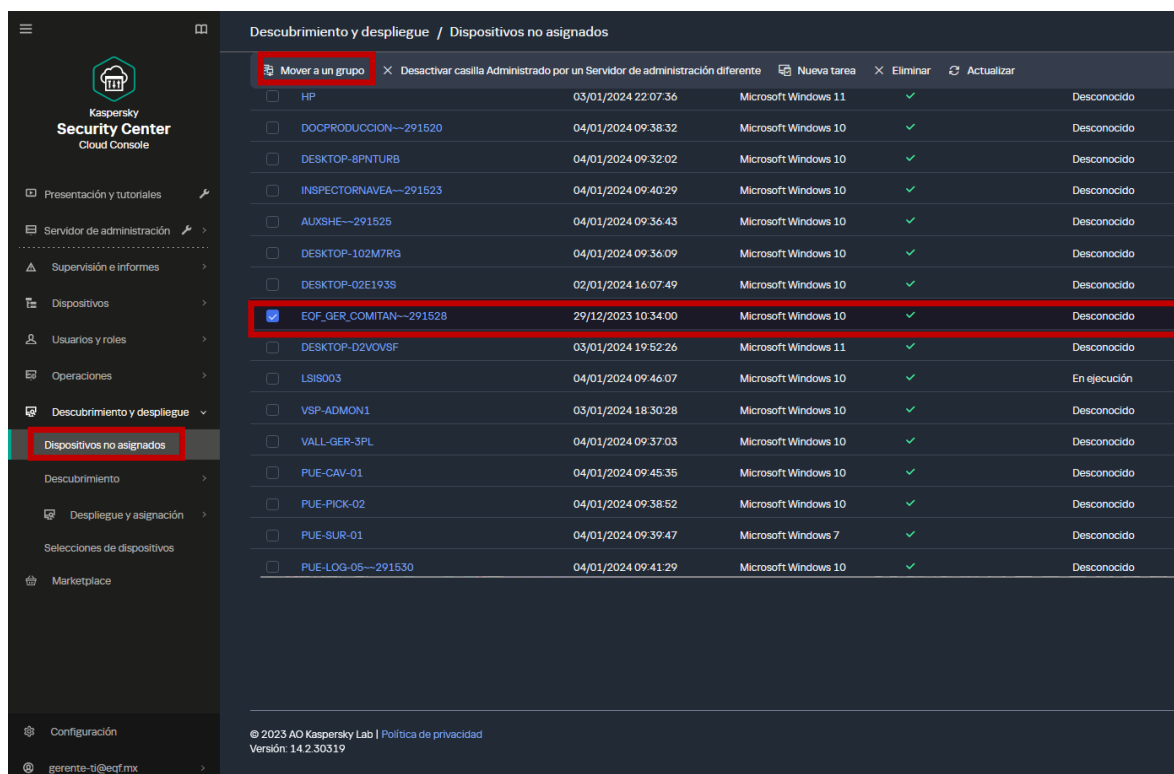


Figura 32 Dispositivos no asignados a un grupo. [Elaboración propia]

Después se muestran las diferentes empresas que se encuentran dentro de un grupo (si es que lo hay), por lo que se tiene que seleccionar la casilla de la empresa a la cual se le va a asignar el dispositivo que no tiene un grupo asignado y de esta manera el equipo se moverá al grupo que le corresponde.

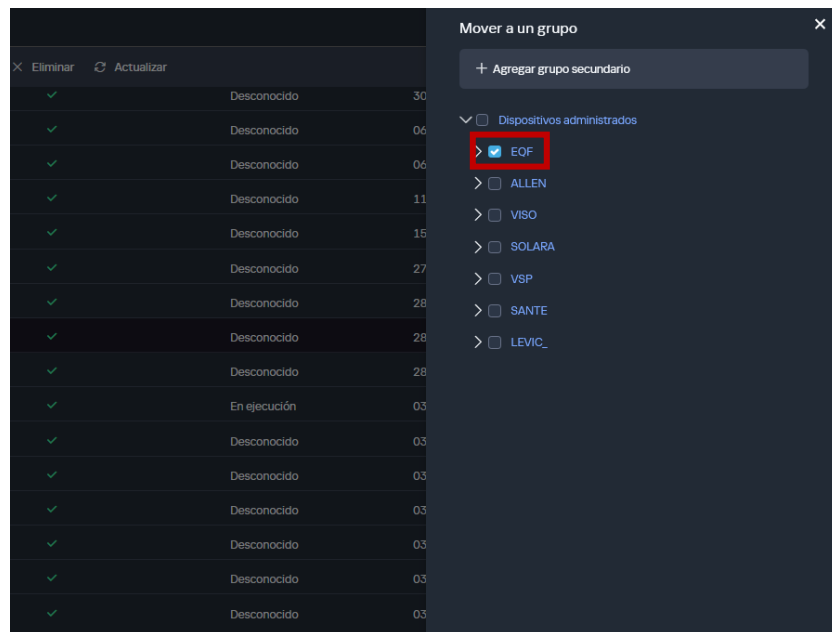


Figura 33 Asignación de grupo. [Elaboración propia]

Para verificar que el dispositivo si se haya asignado al grupo de dispositivos de EQF, en el menú de la parte izquierda se debe de dar clic para desplegar el submenú “Dispositivos”, dentro de este submenú se encuentra la opción de “Dispositivos administrados”. Aquí se muestran todos los dispositivos que pertenecen al grupo de EQF y los cuales pueden ser administrados o se le pueden realizar diversas acciones.

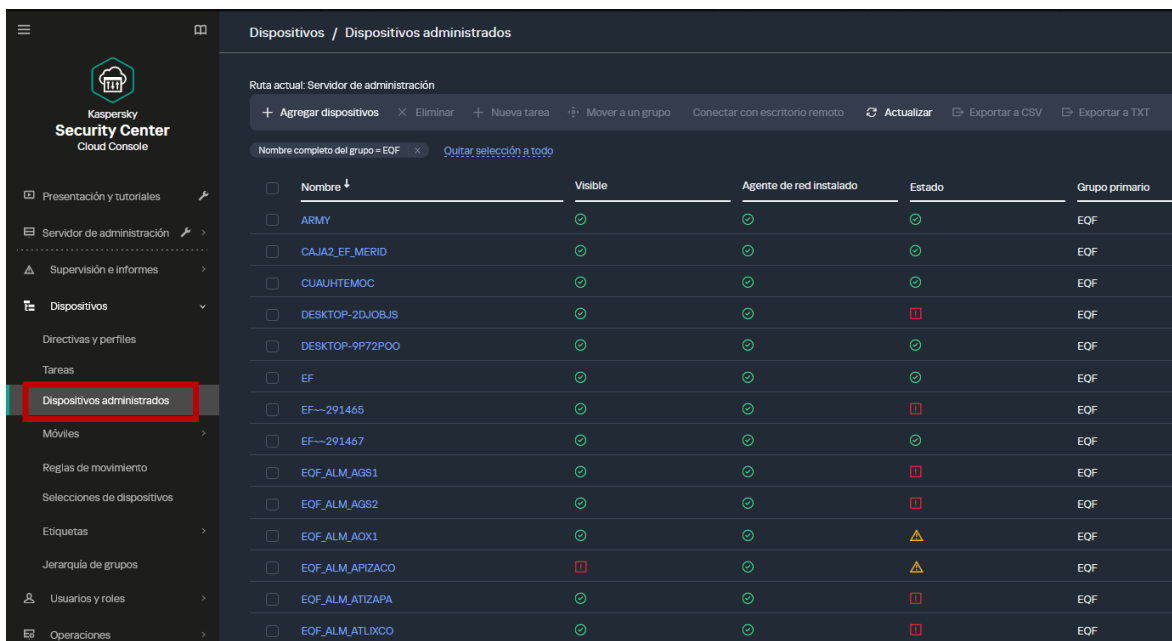


Figura 34 Dispositivos administrados dentro del grupo de EQF. [Elaboración propia]

Una manera más sencilla de buscar que un dispositivo se encuentre dentro de un grupo en este caso el de EQF, es buscándolo por su nombre, para esto en el menú de la parte superior de los dispositivos asignados se encuentra un buscador, aquí daremos clic y se podrá el nombre del dispositivo que se quiere encontrar por ejemplo “EQF_GER_COMITAN” y como se puede observar este dispositivo si se encuentra dentro del grupo de EQF.

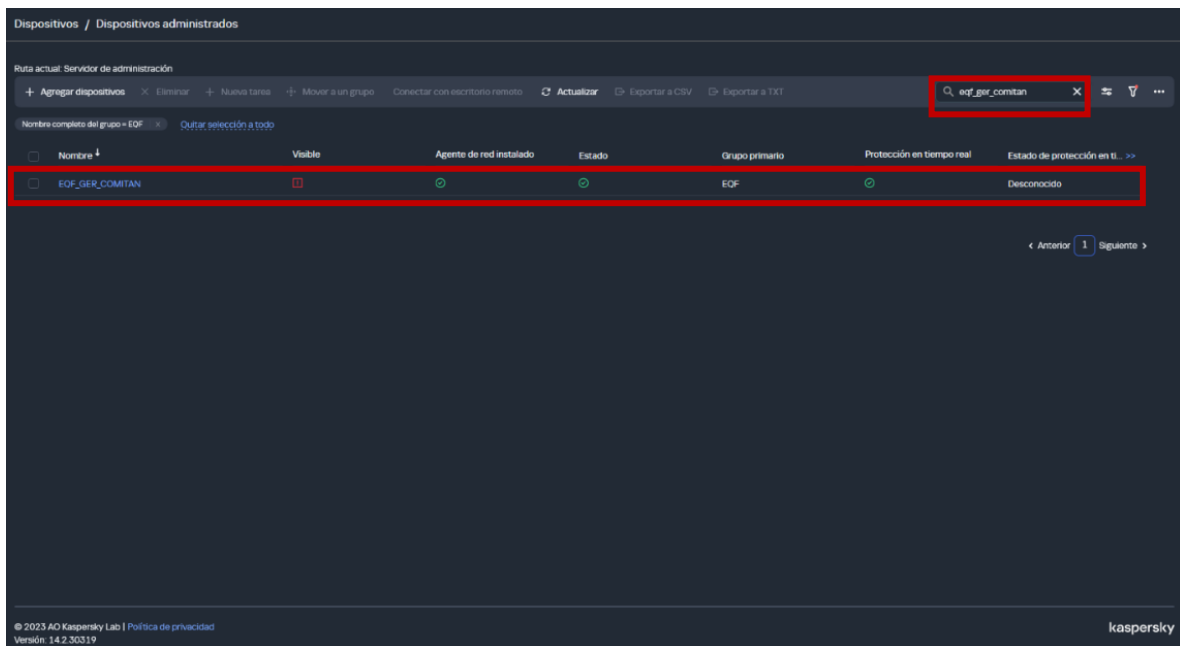


Figura 35 Búsqueda de dispositivos. [Elaboración propia]

Por último, se pueden ver las propiedades que el dispositivo tiene dentro de Kaspersky, para esto se tiene que dar doble clic sobre el dispositivo al cual se le quieran revisar las propiedades, por ejemplo, el de “EQF_GER_COMITAN”. A continuación, se muestran todas las propiedades que el dispositivo tiene como su información general, las aplicaciones de Kaspersky que tiene instaladas, las directivas y perfiles de directivas activos, las tareas asignadas para este dispositivo, los eventos que este contiene, incidentes, etiquetas y otras propiedades avanzadas.

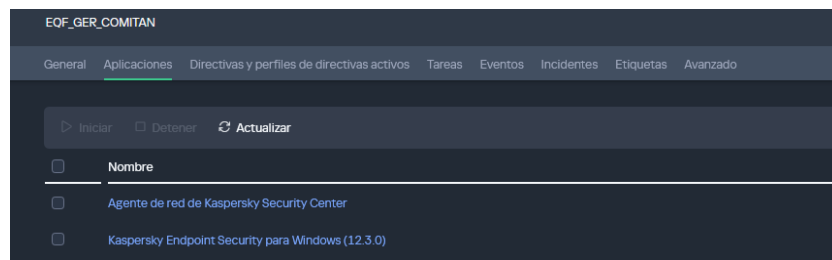
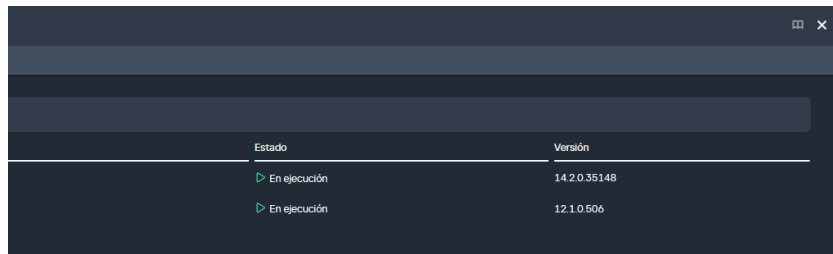


Figura 36 Propiedades del dispositivo seleccionado (parte 1). [Elaboración propia]



Estado	Versión
En ejecución	14.2.0.35148
En ejecución	12.1.0.506

Figura 37 Propiedades del dispositivo seleccionado (parte 2). [Elaboración propia]

De esta manera se instala el agente antivirus de Kaspersky a los dispositivos y la asignación del grupo que le corresponde a cada uno de estos.

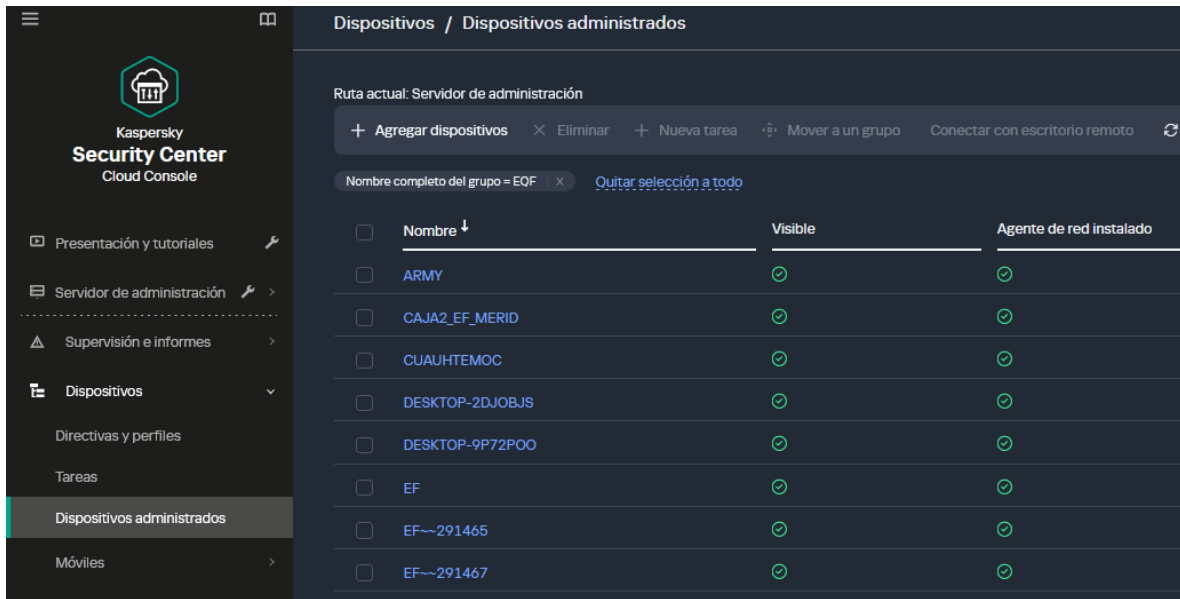
Actividad 5.5 Instalar el antivirus desde el servidor mediante una consola del mismo agente.

Descripción de la actividad

Para realizar esta actividad de instalación del antivirus de Kaspersky, se tiene que ingresar a la consola de administración, posteriormente se asignan los dispositivos al grupo de EQF y la instalación se hace automáticamente cuando los dispositivos son asignados al grupo.

Resultado de la actividad

Dentro de la consola de administración en el menú de la parte izquierda se debe de dar clic para desplegar el submenú “Dispositivos”, dentro de este submenú se encuentra la opción de “Dispositivos administrados”. Aquí se muestran todos los dispositivos que pertenecen al grupo de EQF y los cuales pueden ser administrados o se le pueden realizar diversas acciones.



Dispositivos / Dispositivos administrados

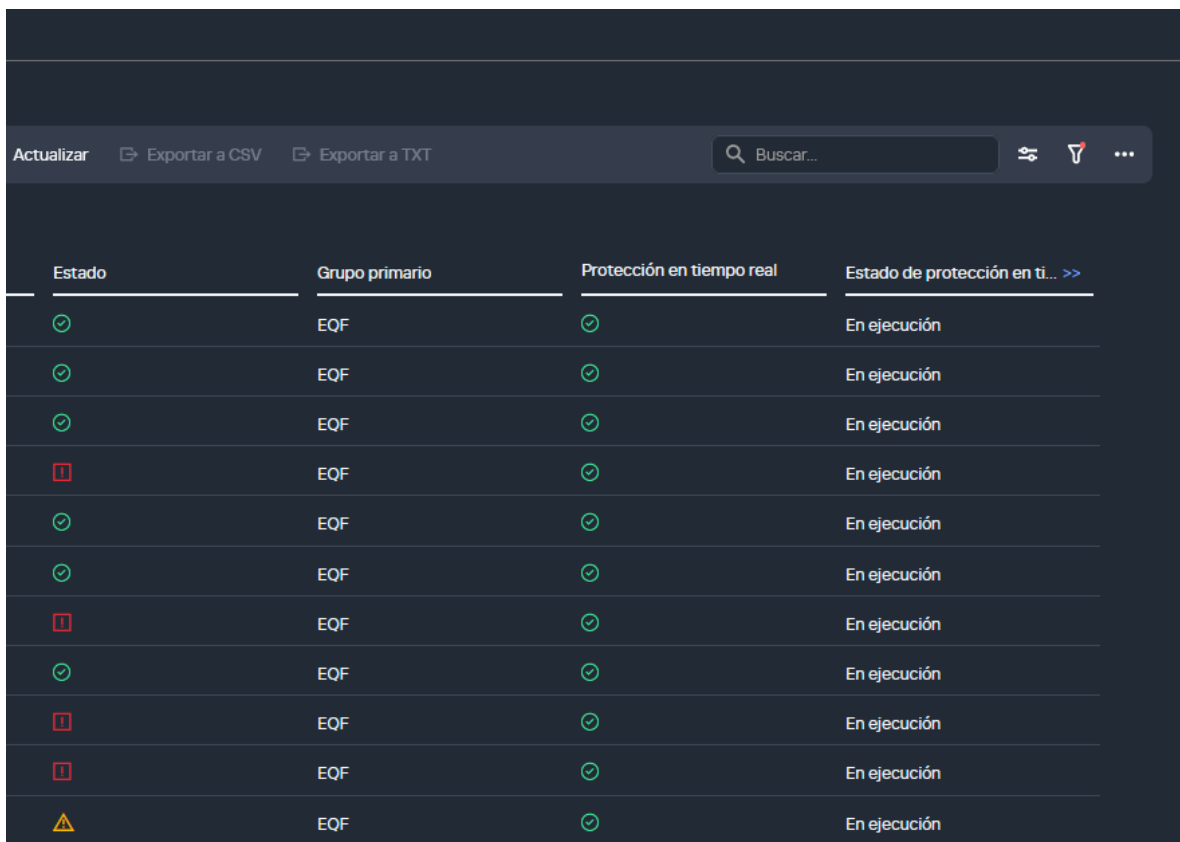
Ruta actual: Servidor de administración

+ Agregar dispositivos × Eliminar + Nueva tarea ⇅ Mover a un grupo Conectar con escritorio remoto ↺

Nombre completo del grupo = EQF × Quitar selección a todo

☐	Nombre ↓	Visible	Agente de red instalado
☐	ARMY	✓	✓
☐	CAJA2_EF_MERID	✓	✓
☐	CUAUHTEMOC	✓	✓
☐	DESKTOP-2DJOBJS	✓	✓
☐	DESKTOP-9P72POO	✓	✓
☐	EF	✓	✓
☐	EF~291465	✓	✓
☐	EF~291467	✓	✓

Figura 38 Dispositivos administrados (parte 1). [Elaboración propia]



Actualizar Exportar a CSV Exportar a TXT

Buscar...

Estado	Grupo primario	Protección en tiempo real	Estado de protección en ti... >>
✓	EQF	✓	En ejecución
✓	EQF	✓	En ejecución
✓	EQF	✓	En ejecución
⚠	EQF	✓	En ejecución
✓	EQF	✓	En ejecución
✓	EQF	✓	En ejecución
⚠	EQF	✓	En ejecución
✓	EQF	✓	En ejecución
⚠	EQF	✓	En ejecución
⚠	EQF	✓	En ejecución
⚠	EQF	✓	En ejecución

Figura 39 Dispositivos administrados (parte 2). [Elaboración propia]

Como se puede observar al momento de que los dispositivos son asignados a un grupo de muestran diversas características:

- “Agente de red instalado”, indica que el dispositivo tiene instalado el agente de Kaspersky.
- “Estado”, indica el estado en que se encuentra el dispositivo.
- “Grupo”, indica el grupo al que pertenece.
- “Protección en tiempo real”, indica si el dispositivo está protegido en tiempo real
- “Ejecución de protección en tiempo real”, muestra si la protección en tiempo real se esté ejecutando.

☐ Nombre ⁺	Visible	Agente de red instalado	Estado	Grupo primario	Protección en tiempo real	Estado de protección en ti... >>
☐ ARMY	🟢	🟢	🟢	EQF	🟢	En ejecución
☐ CAJ2_EF_MERID	🟢	🟢	🟢	EQF	🟢	En ejecución
☐ CUALHTEMOC	🟢	🟢	🟢	EQF	🟢	En ejecución
☐ DESKTOP-2DJ0BJS	🟢	🟢	🔴	EQF	🟢	En ejecución
☐ DESKTOP-9P72POO	🟢	🟢	🟢	EQF	🟢	En ejecución

Figura 40 Propiedades del estado de protección de los dispositivos. [Elaboración propia]

De esta manera al momento de asignar los dispositivos a un grupo como se muestra en la actividad anterior, de manera automática la consola de Kaspersky instala el antivirus en los dispositivos.

Actividad 5.6 Dar seguimiento y programa de mantenimiento para validar que la actualización de la base de datos de virus se mantenga al día y en correcto funcionamiento.

Descripción de la actividad

Para realizar esta actividad se tiene que actualizar la base de datos de virus del antivirus de Kaspersky, para ello se tiene que ingresar a la consola o panel de administración, para poder crear una tarea la cual ayude a buscar vulnerabilidades para que de esta manera se pueda actualizar la base de datos de virus, con aquellas vulnerabilidades, virus o amenazas que sean nuevas, además de actualizar el antivirus en los dispositivos los cuales se encuentren dentro del grupo de EQF.

Resultado de la actividad

Para actualizar de la base de datos de virus de Kaspersky se puede hacer por medio de una tarea la cual realice esta actividad en todos los dispositivos que se encuentren dentro del grupo de EQF. Por lo tanto, para crear dicha tarea primeramente se debe de desplegar el

submenú de “Dispositivos” el cual se encuentra en el panel de la parte izquierda, posteriormente dentro de este submenú se encuentra la opción de “Tareas” a la cual se tiene que dar clic.

Dentro de la opción de “Tareas” se muestra una interfaz la cual contiene todas las tareas que se hayan creado con anterioridad, además de ello se muestra un menú el cual permite realizar diversas acciones con las tareas ya creadas o de lo contrario crear una nueva tarea de acuerdo a la necesidad que se tenga.

Ahora para crear una nueva tarea, se debe de dar clic en la opción de “Agregar”, la cual se encuentra en el menú de la parte superior donde se reflejan las tareas que se han creado.

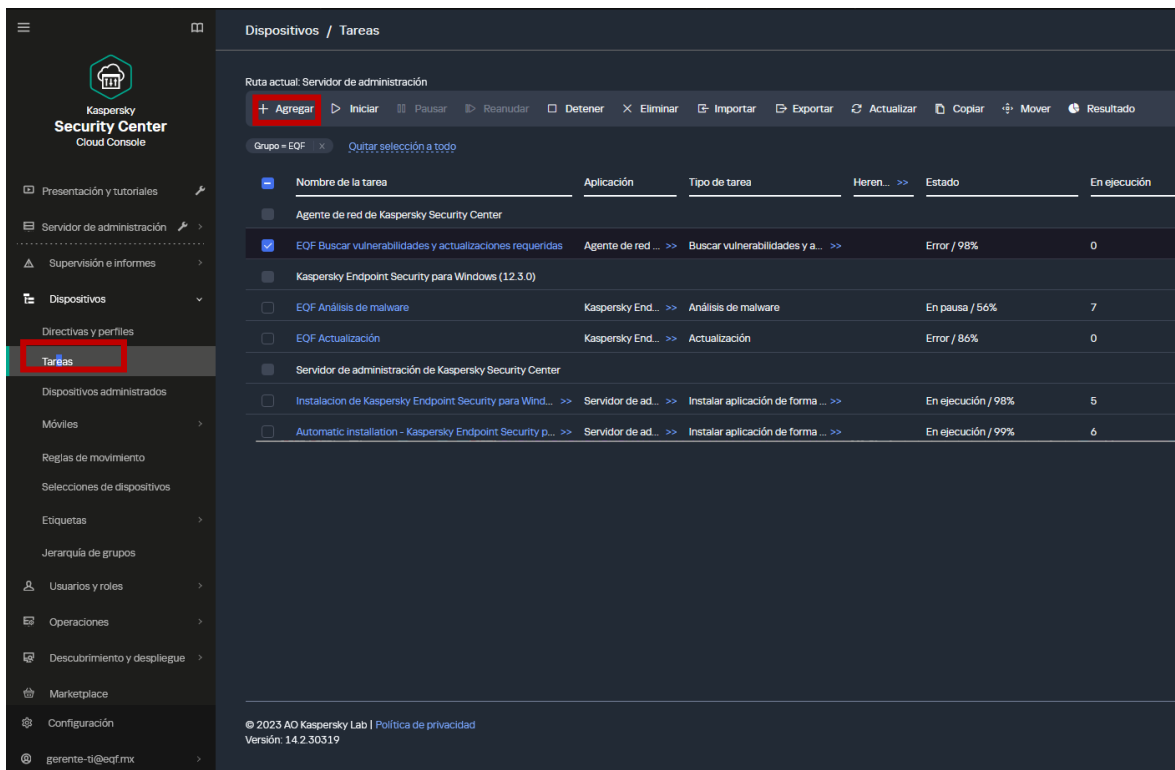


Figura 41 Interfaz de las tareas de Kaspersky. [Elaboración propia]

Una vez que se dio clic en la opción de “Agregar”, se muestra un asistente para crear una nueva tarea en la cual muestra diversas características para la creación de una tarea como la aplicación a la cual se le va a realizar alguna acción, el tipo de tarea que se requiera realizar, el nombre de la tarea y por último un checklist para seleccionar los dispositivos a los cuales se le aplicara la tarea que se va a crear.

Primeramente, para la creación de la tarea se seleccionará la aplicación a la cual se le va a aplicar, en este caso la de “Kaspersky Security Center 14.2”.

Figura 42 Asistente para crear una nueva tarea. [Elaboración propia]

El siguiente paso es seleccionar el tipo de tarea que se va a realizar, para ello se tiene que dar clic en “Tipo de tarea” y se desplegaran diversas opciones de tareas que se pueden realizar, en este caso la tarea que se creara será para la actualización de la base de datos de virus. Por lo tanto, se tiene que seleccionar la opción de “Buscar vulnerabilidades y actualizaciones requeridas”.

Figura 43 Tipos de tareas en Kaspersky. [Elaboración propia]

Ya que se realizó lo anterior, a continuación, se muestra el alcance que tendrá la tarea, aquí se pueden seleccionar las diferentes empresas a las cuales se puede aplicar la tarea que se está creando, esto dependerá si hay una o más empresas dentro de un grupo de empresas. Sin embargo, el alcance de la tarea solamente se realizará para los dispositivos de EQF, por lo que se debe de seleccionar la opción de “EQF”.

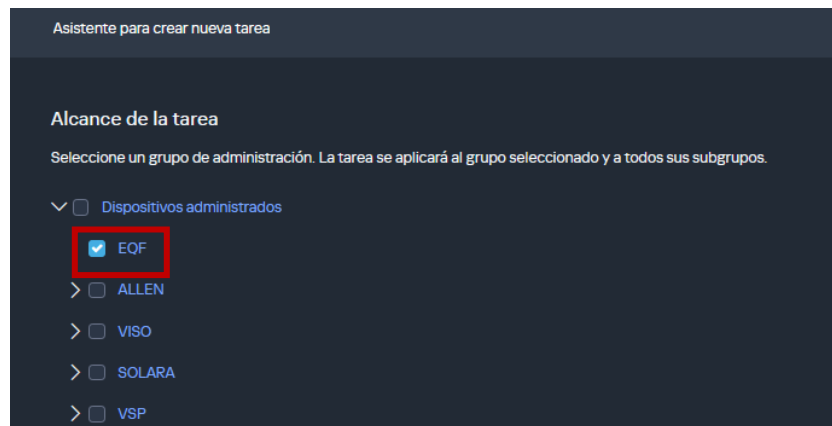


Figura 44 Alcance de la tarea. [Elaboración propia]

Después de haber seleccionado la empresa, a continuación, se muestran más acciones que se pueden realizar como la especificación de los métodos que se van a utilizar para detectar aplicaciones que tengan vulnerabilidades o que deban actualizarse, también se pueden especificar las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos y, por último, el tamaño que debe de tener el archivo de diagnóstico avanzado. Sin embargo, estas opciones se dejarán tal cual se muestran en la interfaz.

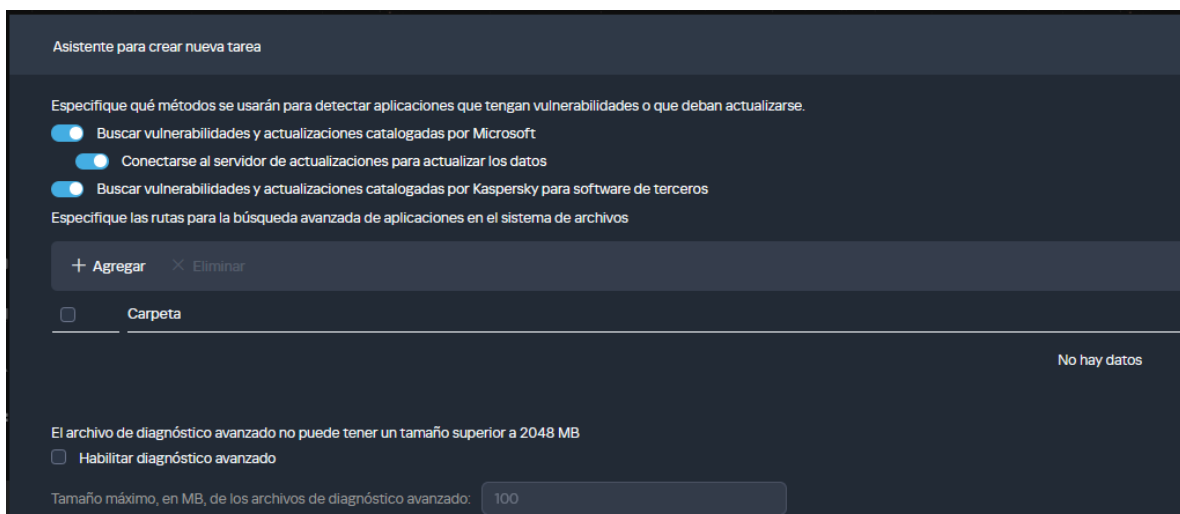


Figura 45 Especificaciones de la tarea. [Elaboración propia]

Finalmente, ya que se realizó todo lo anterior para crear la tarea se muestra una interfaz en que se muestra una casilla que permite abrir los detalles de la tarea cuando se complete la creación, esta opción puede ser opcional, en este caso no se seleccionará y solamente se dará clic en el botón de “Finalizar”, esto creara la tarea con las características que se le asignación.

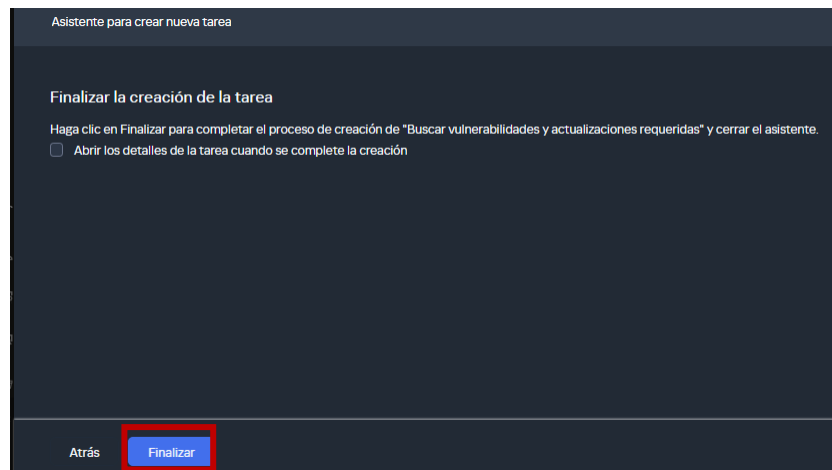


Figura 46 Termino de la tarea creada. [Elaboración propia]

A continuación, se muestra en el panel de tareas, la tarea ya creada a la cual se le pueden realizar diversas acciones las cuales se encuentran en el menú de la parte superior. Ahora para poder iniciar la tarea y que se pueda realizar la actualización de la base de datos de virus, de debe de seleccionar la tarea que se creó y después en el menú de la parte superior se tiene que dar clic en la opción de “Iniciar”.

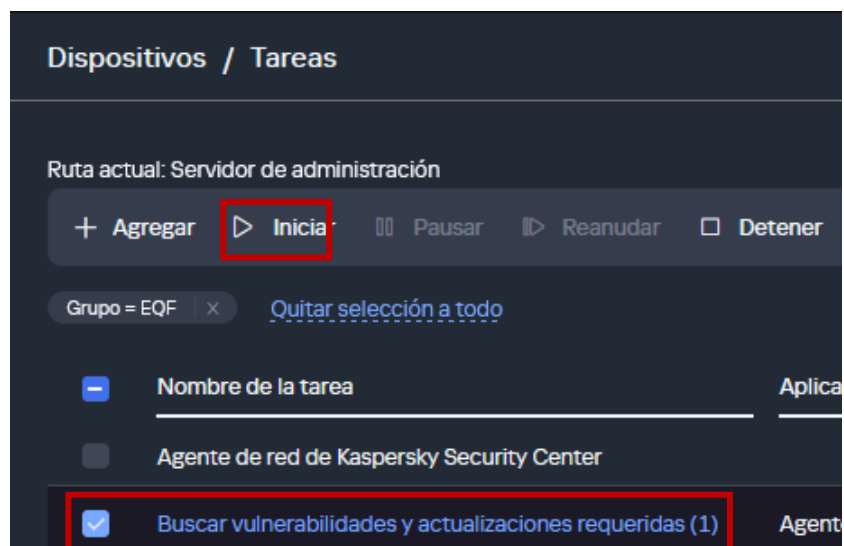
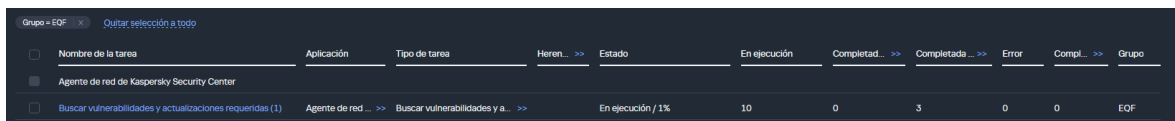


Figura 47 Inicio de la tarea creada para la actualización de la base de datos de virus. [Elaboración propia]

Ya que se inició la tarea, en esta misma en el apartado de “Estado” se muestra el estado de cómo va avanzando su ejecución, en el apartado de “Ejecución” se indica el número de dispositivos en los que se está ejecutando la tarea, en “Completado” se indica el número de dispositivos en los que se completó la tarea, y en “Error” el número de errores que se tuvieron durante la ejecución de la tarea.



Nombre de la tarea	Aplicación	Tipo de tarea	Heren...	Estado	En ejecución	Completad...	Completada...	Error	Compl...	Grupo
Agente de red de Kaspersky Security Center										
Buscar vulnerabilidades y actualizaciones requeridas (1)	Agente de red ... >>	Buscar vulnerabilidades y a... >>		En ejecución / 1%	10	0	3	0	0	EOF

Figura 48 Estado de la tarea en ejecución. [Elaboración propia]

De esta manera se puede mantener y dar seguimiento a la actualización de la base de datos de virus para tenerla al día y pueda proteger a los dispositivos de aquellas amenazas o virus que sean nuevos.

Actividad 5.7 Aplicar pruebas piloto conforme a las instalaciones del agente para verificar su correcto funcionamiento.

Descripción de la actividad

Esta actividad implica la ejecución de pruebas piloto específicas, alineadas con la instalación del antivirus, con el propósito de verificar su correcto funcionamiento. Durante estas pruebas, se evaluará la capacidad del antivirus para detectar y neutralizar amenazas en un entorno controlado. Asegurando la eficacia del software antivirus en el contexto operativo de la empresa, garantizando así una protección sólida contra posibles ciberataques.

Resultado de la actividad

Para comenzar con las pruebas de protección primeramente en el panel general, se muestra una sección donde se indica de forma gráfica las amenazas que fueron detectadas, clasificándolas por componentes, por ejemplo, se puede observar que se lograron detectar 36 amenazas contra archivos, los cuales contenían un tipo de virus.

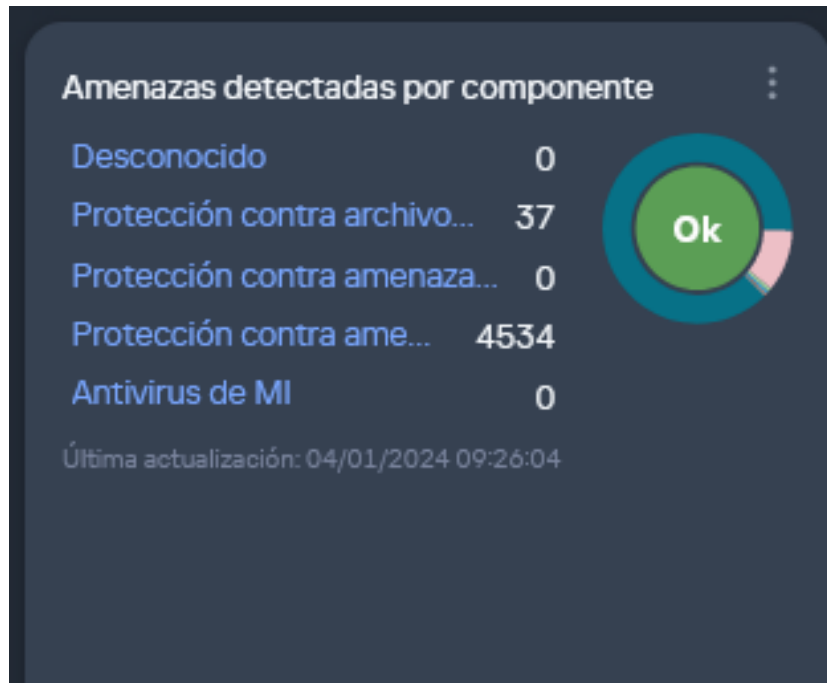


Figura 49 Amenazas detectadas por componente. [Elaboración propia]

Posteriormente se realizaron otras pruebas en las cuales se lograron detectar otro tipo de amenazas, como se puede observar en la siguiente imagen, se muestra un panel el cual indica las amenazas que ocurren con más frecuencia, sin embargo, se puede notar que dichas amenazas son enlaces a sitios web, los cuales no son seguros y/o contienen otro tipo de ataques cibernéticos.

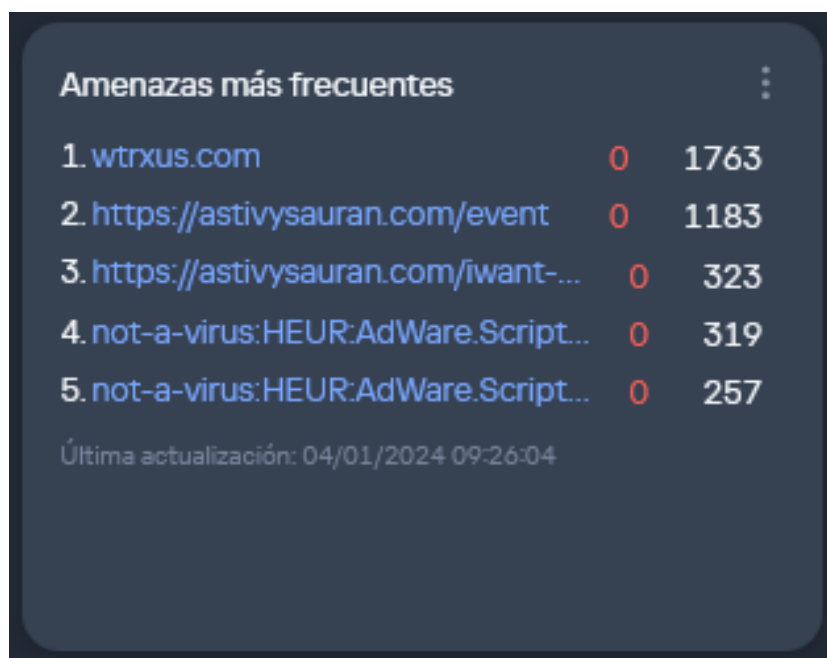
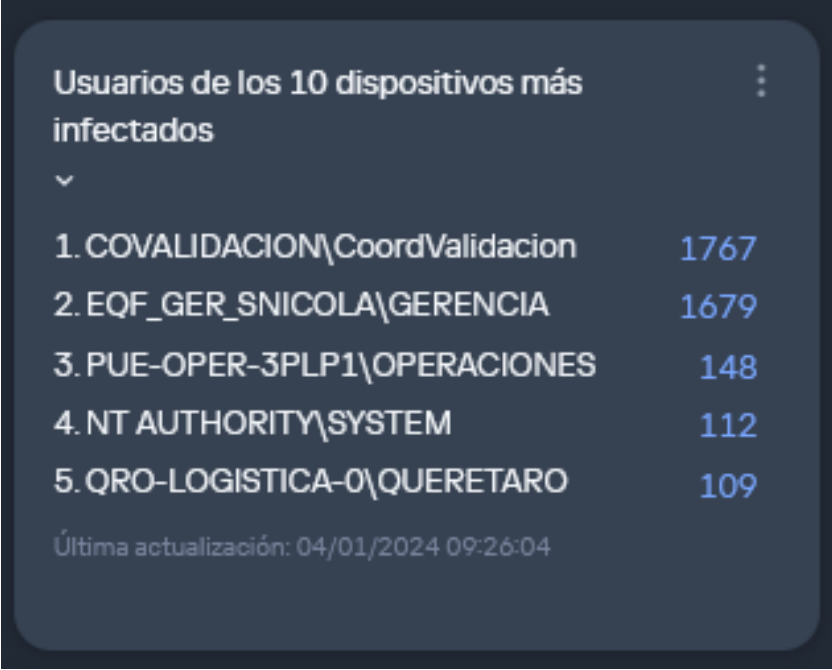


Figura 50 Amenazas más frecuentes. [Elaboración propia]

En la imagen que se presenta a continuación, se muestra un panel el cual menciona el top 10 de los dispositivos más infectados, los cuales muestran el total de amenazas a los cuales fueron expuestos y por lo tanto necesitan de una atención urgente para su protección ya que pueden representar un gran riesgo para la empresa al estar infectados con un gran número de amenazas.



Usuarios de los 10 dispositivos más infectados	
1. COVALIDACION\CoordValidacion	1767
2. EQF_GER_SNICOLA\GERENCIA	1679
3. PUE-OPER-3PLP1\OPERACIONES	148
4. NT AUTHORITY\SYSTEM	112
5. QRO-LOGISTICA-0\QUERETARO	109

Última actualización: 04/01/2024 09:26:04

Figura 51 Top 10 de los dispositivos más infectados. [Elaboración propia]

Como se puede observar el antivirus logra cumplir con su objetivo que es proteger los equipos ante diferentes amenazas, ya sean archivos o sitios web que sean maliciosos o no seguros, además de ello con la ayuda de los diversos paneles es más fácil identificar información tanto de las amenazas que han ocurrido como de aquellos dispositivos los cuales pueden representar un riesgo significativo para la empresa al estar infectados.

Actividad 5.8 Utilizar las herramientas de control: monitoreo, políticas de restricciones, etc.

Descripción de la actividad

Esta actividad se centra en la implementación y utilización efectiva de herramientas de control que brinda Kaspersky. Se llevará a cabo investigación de cómo realizar la configuración y aplicación de estas herramientas para supervisar de manera proactiva las

actividades y garantizar el cumplimiento de políticas de seguridad. Esto con el propósito de fortalecer la seguridad informática mediante el control activo y la aplicación coherente de políticas que reduzcan la exposición a riesgos y mantengan la integridad y confidencialidad de los datos de EQF.

Resultado de la actividad

Para llevar a cabo la implementación de las políticas de acceso se hará uso de la función de directivas que brinda la consola de administrador del antivirus de Kaspersky, dichas directivas se pueden aplicar para un solo usuario, un grupo de usuarios en específico o para todos los usuarios en general que se encuentren dentro del grupo principal.

Para realizar la creación y configuración de directivas se deben de seguir los siguientes pasos dentro de la consola de administración, en base a la documentación oficial de Kaspersky. De igual manera en la actividad 5.9 se realizarán estos pasos dentro de la consola para visualizarlo de manera más gráfica y clara.

1. “En el menú principal, vaya a Activos (dispositivos) → Directivas y perfiles.
2. Haga clic en Agregar. Se abre la ventana Seleccionar aplicación.
3. Seleccione la aplicación para la que desee crear la directiva.
4. Haga clic en Siguiente. Se abre la ventana de configuración de la nueva directiva, con la pestaña General seleccionada.
5. Si lo desea, cambie el nombre predeterminado, el estado predeterminado y las opciones de directiva predeterminadas.
6. Haga clic en la pestaña Configuración de la aplicación. O, si lo prefiere, haga clic en Guardar y salga de la ventana. La directiva se mostrará en la lista de directivas y podrá editar su configuración en otro momento.
7. En la pestaña Configuración de la aplicación, en el panel izquierdo, seleccione una categoría de su interés. En el panel de resultados de la derecha, modifique la configuración de la directiva. Puede editar los ajustes de configuración disponibles en cada categoría (sección). Los ajustes de configuración disponibles dependen de la aplicación a la que corresponde la directiva.

Al editar la configuración, puede hacer clic en Cancelar para cancelar la última operación.

8. Haga clic en Guardar para guardar la directiva. La directiva aparecerá en la lista de directivas.” (Kaspersky, 22)

Actividad 5.9 Instalar las políticas que brinda la herramienta conforme a las necesidades de la empresa.

Descripción de la actividad

Para realizar esta actividad se implementarán las políticas de restricción de acceso a los sitios web no seguros y a las plataformas de streaming como Spotify, Netflix, entre otras. Para ello se tiene que ingresar a la consola de administración de Kaspersky con las respectivas credenciales que brindan el acceso y posteriormente realizar la configuración de dichas políticas de restricción para los dispositivos que se encuentren dentro del grupo de EQF.

Resultado de la actividad

Para comenzar con la instalación de las políticas de restricción de acceso de acuerdo con las necesidades de la empresa, primeramente, se debe de tener el agente y el antivirus de Kaspersky instalado en los equipos los cuales pertenecen al grupo de EQF. En seguida se tiene que ingresar a la opción de **“Activos (dispositivos)”**, posteriormente se desplegaran varias opciones a la cual se debe ingresar en la de **“Directivas y perfiles”**, la cual se encuentra en el menú de lado izquierdo de la interfaz, dentro de esta opción se muestran los aplicativos del antivirus a los cuales se pueden realizar diversas configuraciones y la parte más importante es aplicar las políticas de restricción.

Por lo tanto, se debe de dar doble clic en el aplicativo al cual se va a realizar la configuración, en este caso, es el de **“Kaspersky Endpoint Security para Windows EQF 2024”**.



Figura 52 Directivas y perfiles. [Elaboración propia]

Dentro de la configuración del aplicativo se encuentran diversas secciones de configuración las cuales se utilizarán de acuerdo con las necesidades de la empresa. Un aspecto importante a mencionar es que el estado de la directiva debe de estar **“Activa”** para que pueda funcionar correctamente en la protección de los dispositivos. Además de ello se muestra un mensaje que indica que el nivel de protección es bajo, esto es debido a que los componentes que se van a configurar aún no están activos o en funcionamiento, por lo tanto, se tienen que configurar y activar, para esto en el menú de la parte superior se debe de dar clic en la opción de **“Configuración de la aplicación”**.



Figura 53 Configuración general del aplicativo. [Elaboración propia]

Dentro la configuración de la aplicación se muestran diversas opciones las cuales brindan diversos niveles de seguridad como protección avanzada y básica contra amenazas, controles de seguridad, detección y respuesta, cifrado de datos, entre otras opciones las cuales contienen diferentes medidas de seguridad, sin embargo, la opción de interés es la de **“Controles de seguridad”**, por lo tanto, se tiene que dar clic en esta función.

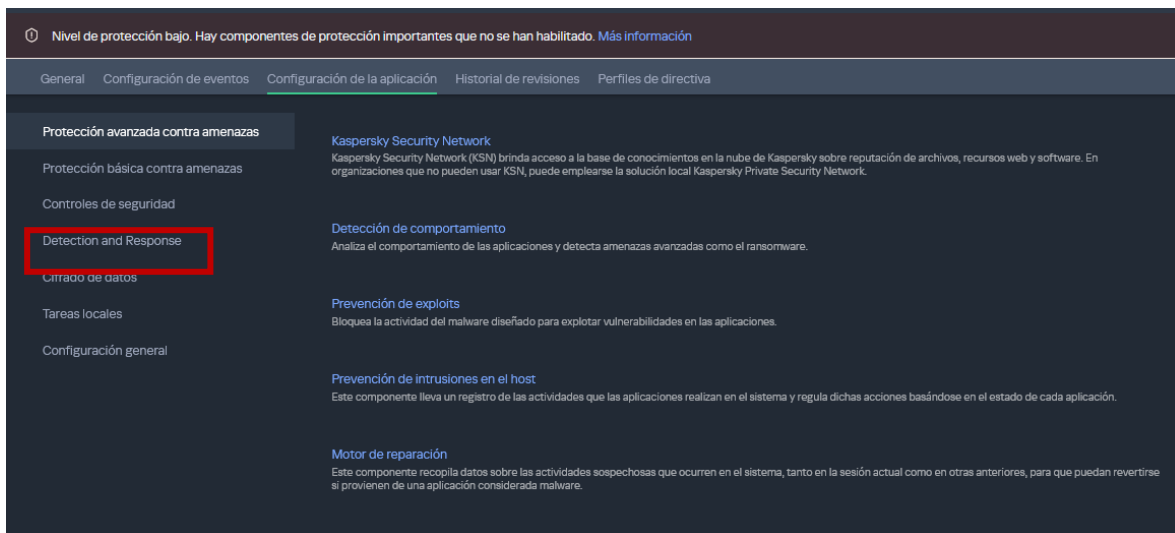


Figura 54 Configuración de la aplicación. [Elaboración propia]

Una vez dentro de la configuración de los controles de seguridad, se muestran diferentes opciones las cuales sirven para poder establecer las políticas de restricción de acceso, las principales funciones que se utilizaran para la creación de estas políticas son las de **“controles de aplicaciones”**, **“control de dispositivos”** y **“control web”**, por lo que primeramente se debe de comenzar por configurar las políticas de control web, para ello se dará clic en la opción **“Control web”**.

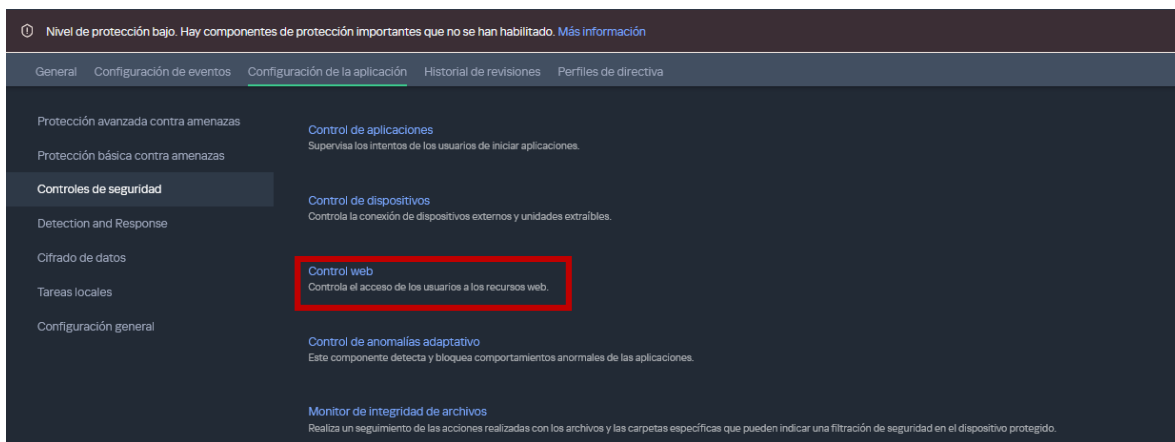


Figura 55 Opciones de controles de seguridad. [Elaboración propia]

Una vez estando dentro de la configuración de control web, primeramente, se muestra una opción la cual se tiene que habilitar para que las políticas de restricción estén en funcionamiento.



Figura 56 Habilitar control web. [Elaboración propia]

En seguida, se muestran las reglas que se han configurado, además de un menú el cual permite configurar las nuevas reglas de restricción, eliminarlas, moverlas de su nivel de prioridad, importarlas o exportarlas. Por tanto, al no tener ninguna regla, se tendrá que dar clic en la opción “**Agregar**” para crear estas nuevas reglas de restricción.

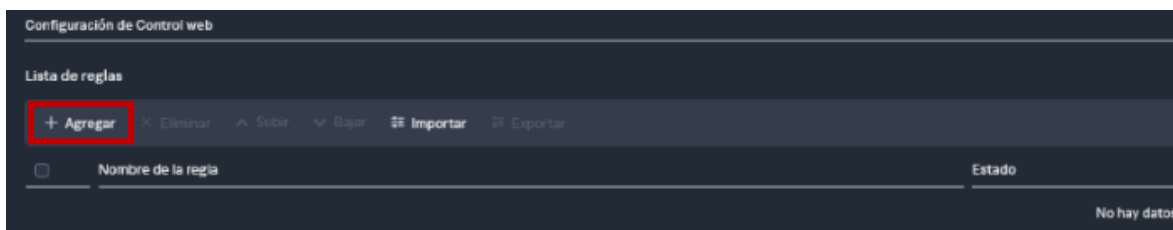


Figura 57 Lista de reglas. [Elaboración propia]

Ahora para crear o agregar la nueva regla de restricción a los sitios web, primeramente, se comienza por ponerle un nombre a esta regla, este nombre puede ser el que la empresa decida asignar, posteriormente se muestra el apartado de “**Estado**”, aquí solamente se debe seleccionar la parte de “**Habilitada**”, esto para indicar que la regla estará activa o en funcionamiento. Después se pueden realizar tres diferentes opciones para los sitios web que no sean permitidos, las cuales constan de “**Permitir**”, “**Bloquear**” o “**Advertir**”, estas se configuran de acuerdo a las necesidades de la organización. En seguida, se muestra el apartado de “**Direcciones**”, aquí es donde se deben de ingresar todos los enlaces de sitios web que no sean permitidos estos pueden ser uno o varios dentro de la misma regla y finalmente se debe de configurar para quien va dirigida esta regla, si es para todos los usuarios en general que se encuentren dentro del grupo de EQF o para usuarios o un grupo de usuarios individual, en este caso se tiene que habilitar la opción “**Aplicar para todos los usuarios**”.

Figura 58 Creación y configuración de la nueva regla. [Elaboración propia]

Para terminar con la configuración de la nueva regla, se puede personalizar el mensaje que aparecerá al usuario cuando ingrese a los sitios web que han sido bloqueados, este mensaje se puede modificar dando clic en la opción “Mensaje para bloqueo” y aquí se puede personalizar dicho mensaje o dejarlo tal cual viene en la configuración por defecto. Finalmente se da clic en crear y se creará la regla con la configuración realizada.

Figura 59 Personalización de mensaje de bloqueo. [Elaboración propia]

Ahora se va a realizar la configuración para el control de aplicaciones, para ello dentro de la opción de controles de seguridad, se debe de ingresar a la sección de “**Control de aplicaciones**” dando clic en esta.

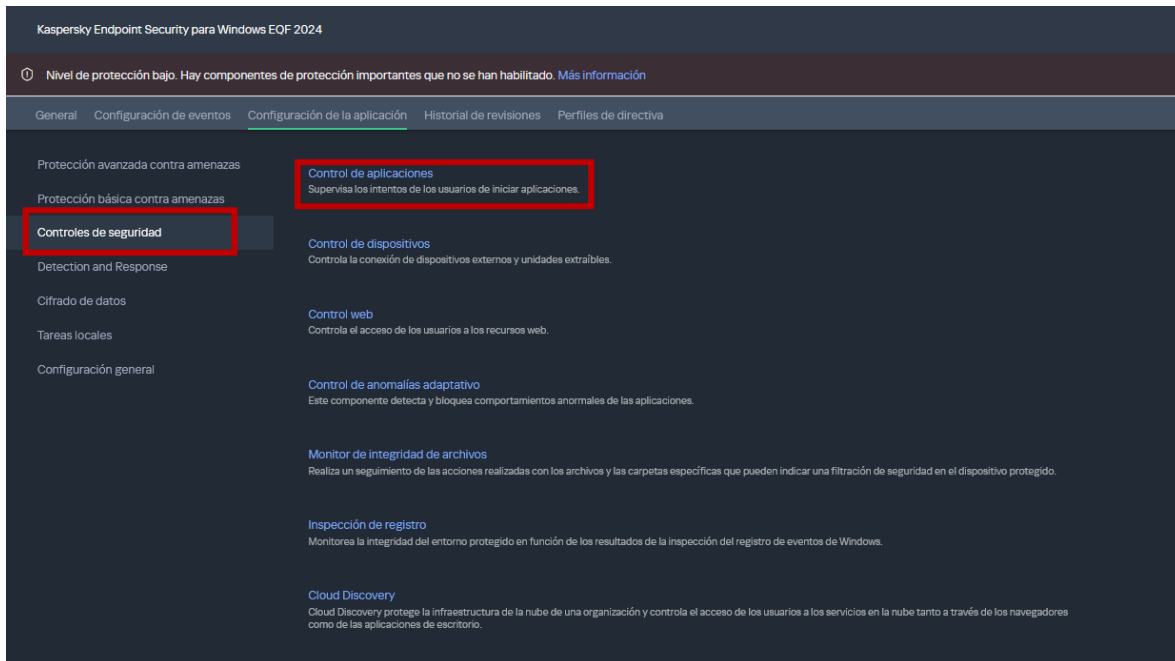


Figura 60 Control de aplicaciones. [Elaboración propia]

Ya que se ingresó a la configuración de control de aplicaciones, primeramente, se muestra una opción la cual se tiene que habilitar para que las políticas de restricción estén en funcionamiento.

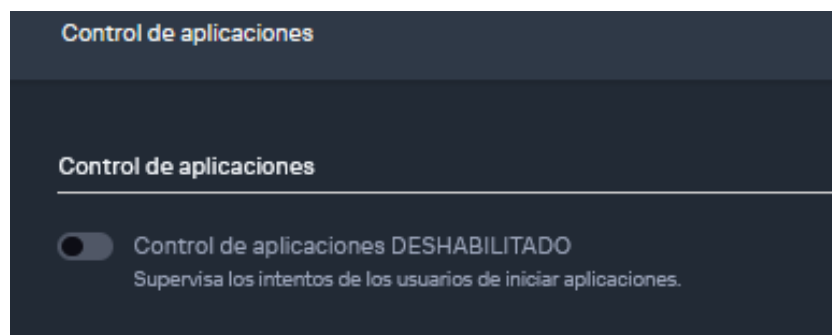


Figura 61 Habilitar control de aplicaciones. [Elaboración propia]

A continuación, se muestran las diversas opciones de configuración para el bloqueo de las aplicaciones, primeramente, se tiene un apartado para indicar que acción de debe de realizar al iniciar una aplicación bloqueada por las reglas, en este caso, se seleccionara la opción de “**Informar**”, la cual manda un aviso de que se está ingresando a una aplicación a

la cual está prohibido dicho acceso. Después se tiene el modo de control de aplicaciones donde se debe de seleccionar la opción de **“Lista de rechazados”**, la cual permite al usuario ingresar a cualquier aplicación a excepción de las que estén agregadas en la regla de bloqueo. Por último, se muestra la configuración avanzada, aquí se dejará tal cual viene por defecto.

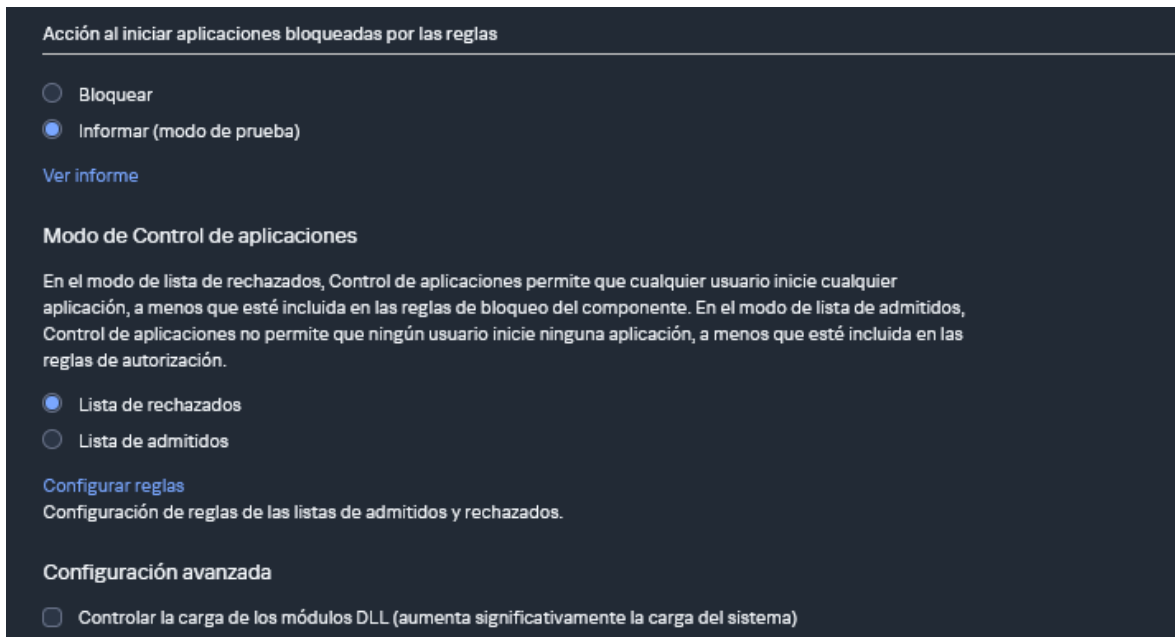


Figura 62 Configuración de regla de bloqueo de aplicaciones. [Elaboración propia]

Para terminar con la configuración, se puede personalizar el mensaje que aparecerá al usuario cuando ingrese a las aplicaciones que han sido bloqueadas, este mensaje se puede modificar dando clic en la opción **“Mensaje para bloqueos”** y aquí se puede personalizar dicho mensaje o dejarlo tal cual viene en la configuración por defecto. Finalmente se da clic en crear y se creará la regla con la configuración realizada.

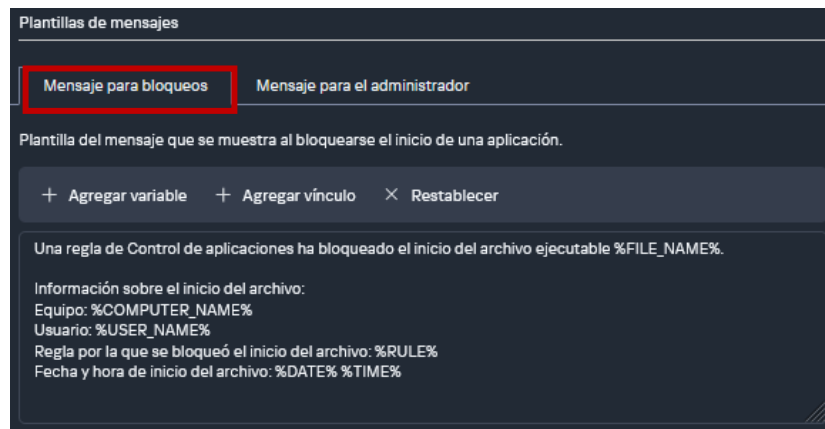


Figura 63 Personalización de mensaje de bloqueo a aplicativos. [Elaboración propia]

Ahora va a abordar la configuración para el control de dispositivos, para ello dentro de la opción de controles de seguridad, se debe de ingresar a la sección de **“Control de dispositivos”** dando clic en esta.

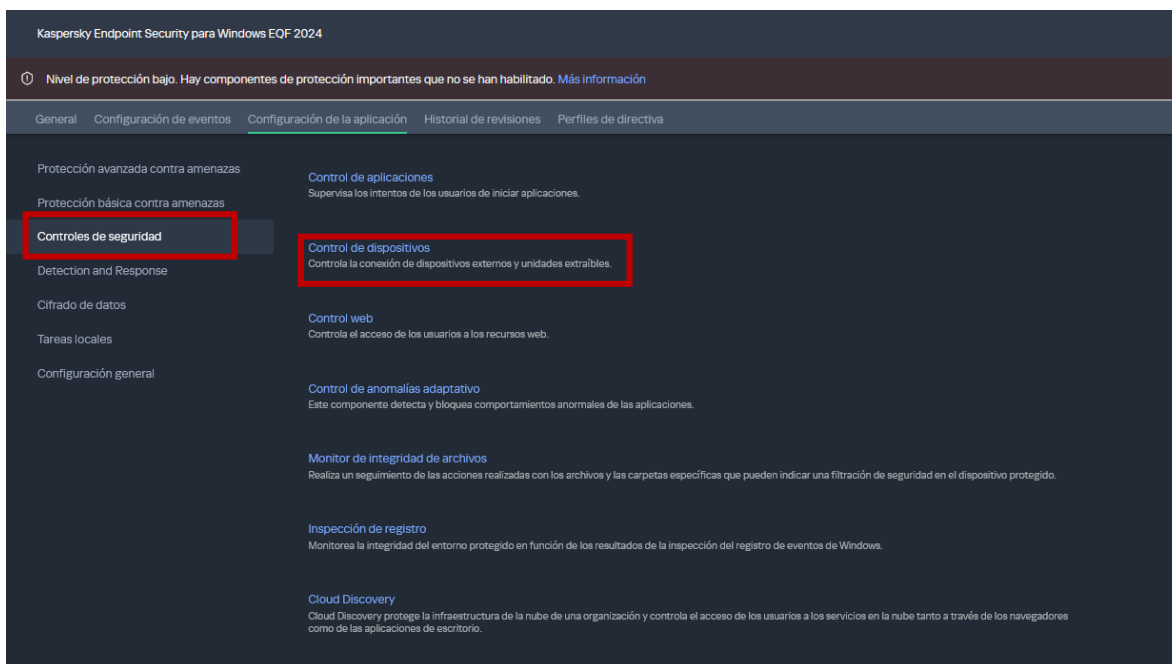


Figura 64 Control de aplicaciones. [Elaboración propia]

Ya que se ingresó a la configuración de control de dispositivos, primeramente, se muestra una opción la cual se tiene que habilitar para que las políticas de restricción estén en funcionamiento.

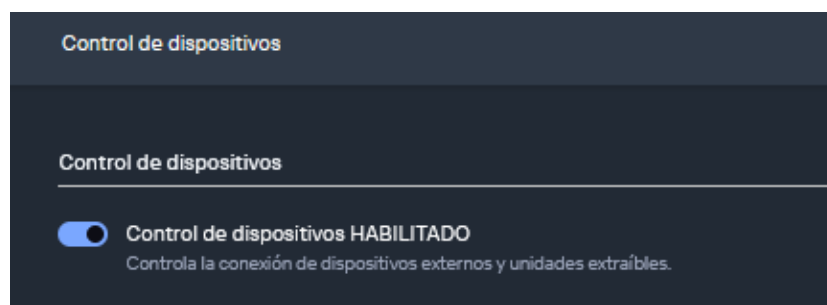


Figura 65 Habilitar control de dispositivos. [Elaboración propia]

A continuación, se muestran todas las opciones que se tienen para configurar el control de los dispositivos los cuales se encuentren dentro del grupo de EQF, en este apartado se dejara tal cual viene la configuración predeterminada y solamente se tiene que habilitar la casilla de **“Permitir solicitudes de acceso temporal”**, sin embargo, al tener la configuración

predeterminada se puede tener un buen control de todos los dispositivos y realizar diversas acciones para aquellos equipos que se encuentren infectados.

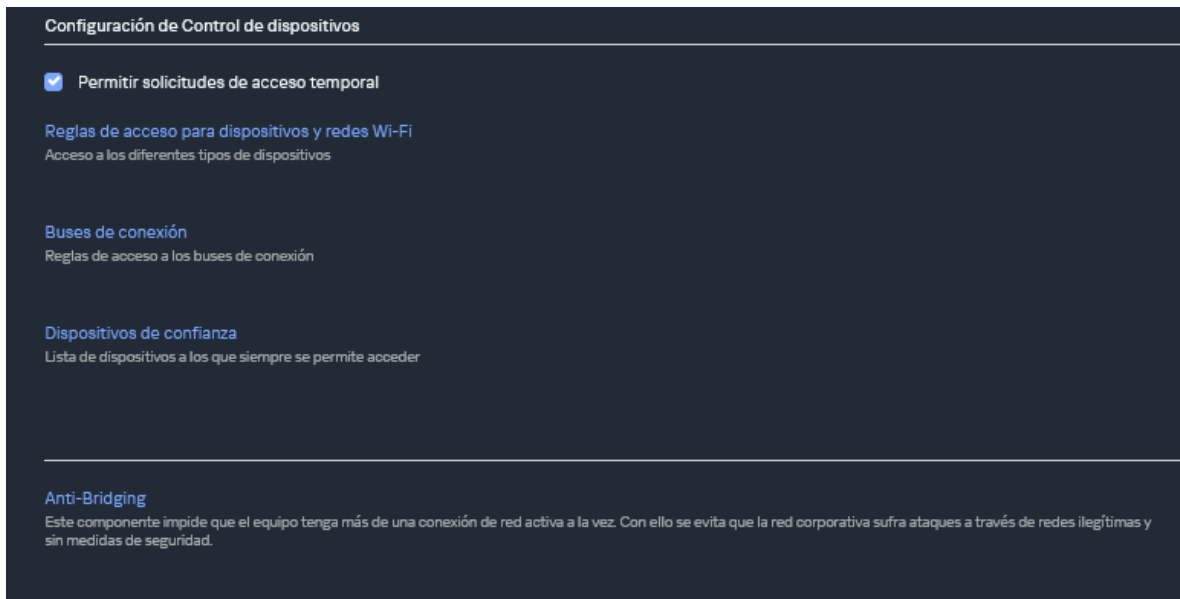


Figura 66 Configuración de control de dispositivos. [Elaboración propia]

Para finalizar con la configuración, se puede personalizar el mensaje que aparecerá a todos los dispositivos los cuales hayan sido bloqueados, este mensaje se puede modificar dando clic en la opción “**Mensaje para bloqueos**” y aquí se puede personalizar dicho mensaje o dejarlo tal cual viene en la configuración por defecto. Finalmente se da clic en crear y se creará la regla con la configuración realizada.

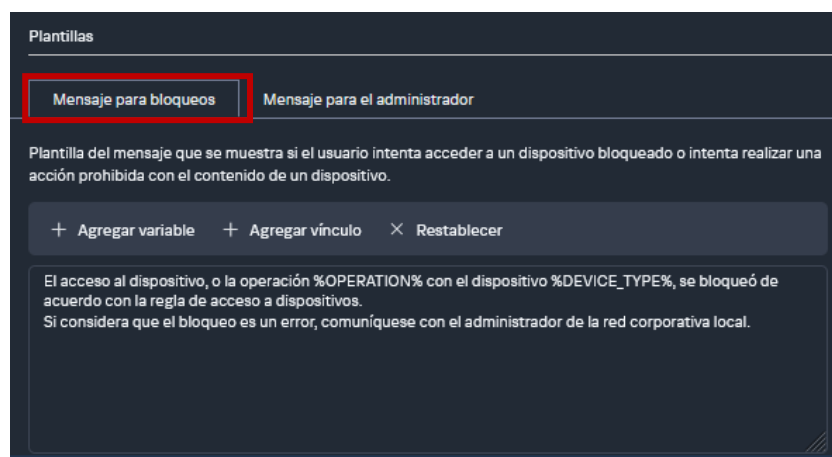


Figura 67 Personalización de mensaje de bloqueo para los dispositivos. [Elaboración propia]

Como ultima política de restricción de acceso, se realizará la configuración de la interfaz del agente de antivirus para los usuarios, esto con la finalidad de tener un mayor control del antivirus y que los usuarios no hagan mal uso de esta medida de seguridad. Por lo tanto, primeramente, en la configuración de la interfaz de tiene como primer apartado la **“Interacción con el usuario”**, aquí se muestran tres opciones las cuales van a permitir que el usuario visualice la interfaz del antivirus de diferente manera, en este caso, se habilitara la opción de **“Con la interfaz simplificada”**.

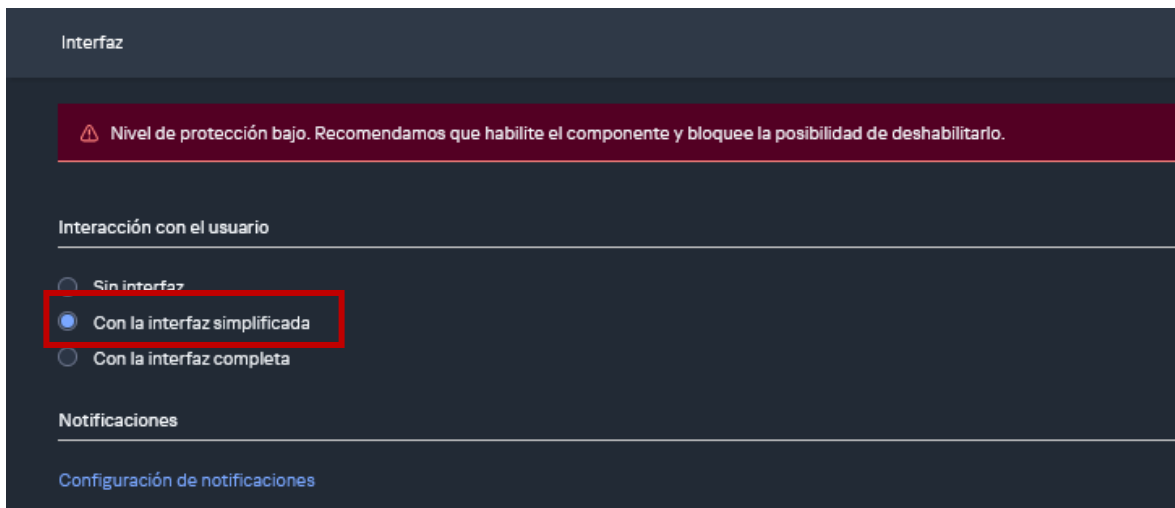


Figura 68 Configuración de interfaz. [Elaboración propia]

A continuación, se muestra la interfaz simplificada que puede observar el usuario al ingresar al aplicativo del antivirus, como se puede observar solamente se muestra la información que corresponde al tipo de licencia de protección que se tiene instalada en el equipo, la clave de licencia que le corresponde, la versión del aplicativo, el nombre del servidor el cual administra el antivirus, la fecha de la última sincronización, además de enlaces los cuales llevan a la documentación oficial acerca del antivirus que se tiene instalado.



Figura 69 Interfaz simplificada del antivirus para el usuario. [Elaboración propia]

De esta manera se realiza la configuración de las políticas de restricción de acceso tanto a sitios web no seguros o que no estén permitidos, como a los diferentes aplicativos e incluso el bloqueo de acceso a los dispositivos los cuales puedan representar un peligro a EQF al estar infectados con algún tipo de virus o amenaza.

Actividad 5.10 Realizar pruebas conforme a las políticas de filtrado del agente para verificar el correcto funcionamiento.

Descripción de la actividad

Para el desarrollo de esta actividad se ingresará a diversos equipos al azar tanto de sucursales como del corporativo de EQF, con la finalidad de realizar las pruebas para testear y comprobar que las políticas de restricción de acceso estén funcionando correctamente.

Resultado de la actividad

Una vez que se implementaron las políticas de restricción de acceso a sitios web, se deberá de acceder a través de un equipo de cómputo al azar, a cualquier sitio web que no tenga un certificado HTTPS, esto con la finalidad de verificar que efectivamente las políticas están funcionando correctamente.

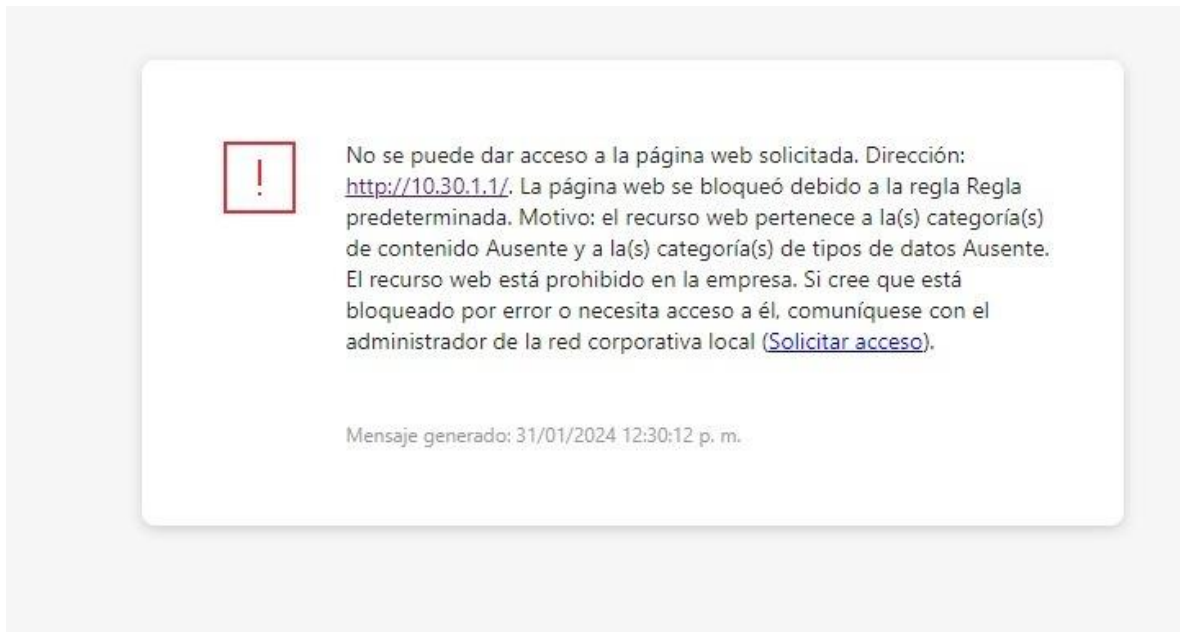


Figura 70 Restricción de acceso a un sitio web no seguro. [Elaboración propia]

En la ilustración que se muestra a continuación se puede observar el bloqueo de un sitio web seguro ya que este tiene el certificado de HTTPS, sin embargo, EQF considera necesario el bloqueo de dicho sitio web.

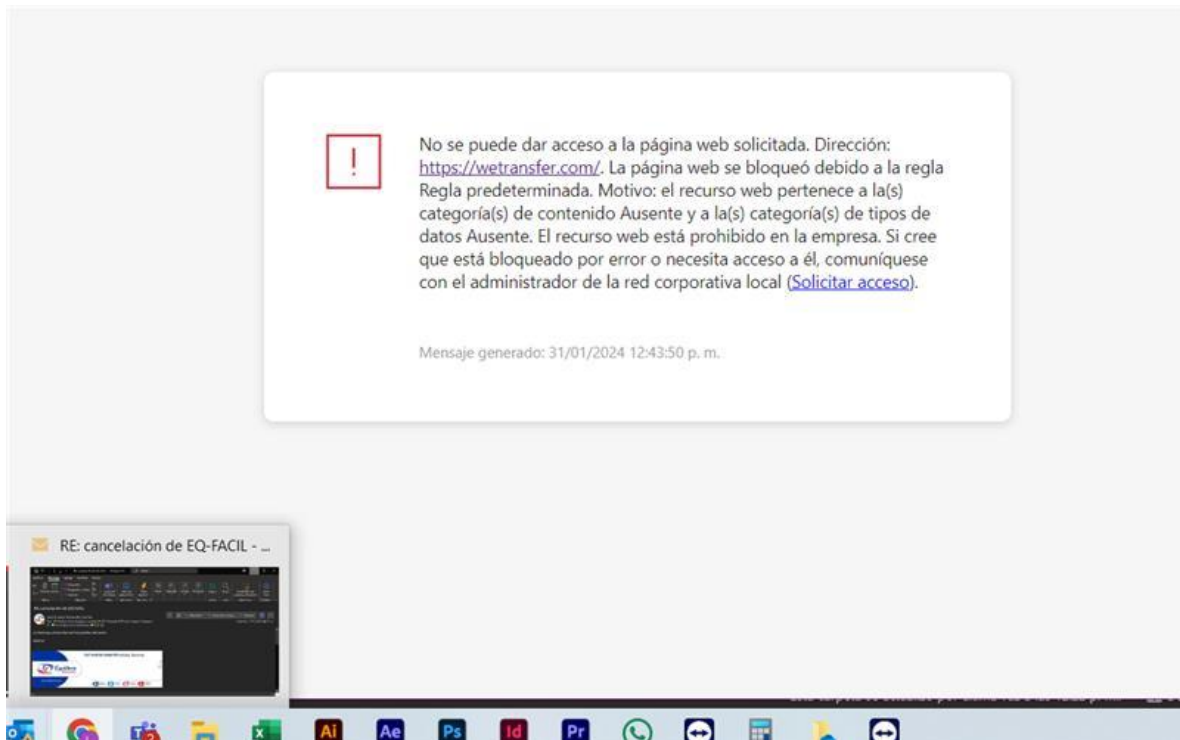


Figura 71 Restricción de acceso a sitio web. [Elaboración propia]

Actividad 5.11 Realizar la documentación respecto a la implementación del agente (antivirus) para posibles fallas de este y como resolver el conflicto.

Descripción de la actividad

En esta actividad se va a realizar un manual técnico donde se concentraran las actividades anteriores que van enfocadas a como se hace la instalación del antivirus de Kaspersky, como se puede generar el instalador del agente debido a que este representa una parte fundamental para poder identificar el equipo en la red de EQF y poder protegerlo, la creación e implementación de tareas las cuales pueden realizar diversas acciones o funciones, creación e implementación de políticas o reglas de acuerdo a las necesidades de EQF.

Resultado de la actividad

El manual técnico de Kaspersky enfocado a las necesidades de EQF se presenta como un archivo de PDF, debido a que la empresa lo requiere en este tipo de formato, sin embargo, se puede consultar en el apartado de anexos (Anexo 2).

CONCLUSIONES

Para concluir este análisis de riesgos, es importante mencionar que a lo largo del desarrollo del presente proyecto se fueron abordando de manera metodológica cada uno de los objetivos establecidos los cuales contribuyeron a establecer una mejoría bastante significativa en cuanto a la seguridad informática dentro del corporativo del EQF, así como de algunas de las sucursales que representan una mayor prioridad de actividad para la empresa. Una de las principales fortalezas que se lograron aportar es tener una mejor protección tanto para dispositivos, la información, y para algunos de los servicios con los cuales se trabajan día con día, además de ello, se logró tener un mejor control en cuanto a los accesos para los usuarios lo cual resulto ser beneficioso tanto para el rendimiento de actividades, como para los servicios de comunicación en los cuales a diario se tratan asuntos de importancia.

A pesar de estos avances, es importante reconocer que aún existen áreas de oportunidad para fortalecer tanto la seguridad física como la lógica. Por lo tanto, abordar estos aspectos permitirá a EQF convertirse en una empresa aún más segura, lo que reflejará mayor confianza y tranquilidad tanto para clientes como para colaboradores.

COMPETENCIAS DESARROLLADAS

Materia: Administración y seguridad en aplicaciones.

Competencias específicas:

- 1. Establece políticas y normas para su uso antes, durante y después de alguna amenaza a los sistemas de información.**

Explicación: Esta competencia se aplicó al momento de implementar las políticas de restricción de acceso a los sitios web no seguros y plataformas de streaming, para poder evitar algún tipo de ciberataque o afectación en el rendimiento de actividades de los usuarios.

Competencias genéricas:

- 1. Capacidad de análisis y síntesis.**

Explicación: La aplicación de esta competencia fue importante debido a que se consultó varia información de la cual se tenía que hacer un análisis de ella para poder llegar a la mejor solución y también al momento de plasmar toda esta información se tuvo que realizar una síntesis de ella la cual tenía que ser de forma clara.

- 2. Habilidad para buscar y analizar información proveniente de fuentes diversas.**

Explicación: A lo largo del proyecto esta competencia fue de gran importancia, ya que para se aplicó en varias ocasiones tanto para teórico al momento de realizar el contenido del marco teórico, como para lo práctico, al momento de buscar la documentación de algunas soluciones que se implementaron o para la búsqueda de los proveedores y las algunas empresas que brindan el servicio del antivirus que se contrató.

- 3. Capacidad de generar nuevas ideas (creatividad).**

Explicación: En la búsqueda de implementar las mejores soluciones de acuerdo con las necesidades de la empresa, la capacidad de generar nuevas ideas resulta de gran

ayuda para poder innovar o implementar cosas nuevas las cuales den el mejor resultado para EQF.

Materia: Administración de la función informática.

Competencias específicas:

1. Manejo de los fundamentos teóricos de seguridad informática para su aplicación en casos prácticos.

Explicación: Esta competencia fue de gran importancia para tener los fundamentos necesarios en base a estándares como la ISO 17799 del porque se tenían que implementar algunas de las soluciones para poder resolver las problemáticas y necesidades que se tenían en la empresa, de igual manera, cuando se evaluaron los controles de riesgo se aplicó esta competencia en el uso de los modelos para utilizar una escala evaluativa.

2. Uso e interpretación de los lineamientos, estándares y marcos referenciales que complementa el conocimiento de la asignatura.

Explicación: Al utilizar una escala evaluativa en base a un modelo en la evaluación de controles de seguridad y en la fundamentación teórica para la implementación de soluciones se aplicó esta competencia durante estas actividades.

3. Uso de técnicas y herramientas de software para comprender el ambiente de seguridad.

Explicación: La aplicación de esta competencia se llevó a cabo en la búsqueda de técnicas para poder realizar algunas de las actividades que se desarrollaron en el proyecto, un claro ejemplo fue durante los tipos de evaluación que se aplicaron en donde se buscaron las mejores técnicas y herramientas para obtener los resultados deseados.

4. Proponer medidas de seguridad basadas en lineamientos y estándares actuales.

Explicación: Esta competencia se aplicó principalmente en el desarrollo de una actividad en la cual se puede observar de forma clara su aplicación, debido a que al proponer las mejores medidas de seguridad estas a su vez fueron fundamentadas en base a estándares.

Competencias genéricas:

1. Comprende las necesidades del medio ambiente y toma decisiones para resolver la problemática que se le presenta.

Explicación: Al realizar el presente análisis de riesgo resulta importante comprender cual es contexto de la empresa y como es que opera, para que al momento de llegar a tomar una decisión esta pueda brindar los mejores beneficios en la empresa, tal cual se pudo reflejar en las propuestas de soluciones al tomar en cuenta cuales eran las principales necesidades de la empresa.

2. Capacidad de organizar y planificar.

Explicación: Esta competencia fue aplicada durante la planeación de la implementación del antivirus ya que se tenían que tomar aspectos importantes para no afectar en las operaciones de la empresa.

3. Comunicación oral y escrita.

Explicación: Esta competencia es de suma importancia, debido a que al momento de realizar la negociación de la implementación del antivirus se tuvo que tratar con los diferentes proveedores en los que se tenía que especificar qué es lo que se quería contratar y en donde se iba a llevar a cabo la aplicación del antivirus.

4. Habilidades de investigación.

Explicación: En la búsqueda de información tanto para el marco teórico, como para los proveedores, la documentación oficial entre otras cosas esta competencia fue aplicada de la mejor manera durante el desarrollo de estas actividades en donde se tenía que consultar diversas fuentes de información las cuales resultaran con gran nivel de confianza.

5. Comprende y manipula ideas y pensamientos respecto a la seguridad lógica.

Explicación: Durante el desarrollo del presente proyecto se trabajó principalmente con la seguridad lógica, ya que las problemáticas principalmente fueron enfocadas a este rubro, por lo que la aplicación de esta competencia se llevó a cabo en actividades como la evaluación de controles y en las propuestas de medidas de seguridad.

6. Capacidad de aplicar los conocimientos en la práctica.

Explicación: Esta competencia se aplicó durante la mayor parte de todo el desarrollo de este análisis de riesgo tanto para la parte del capítulo del desarrollo, como el capítulo de resultados, por lo que para llevar a cabo este proyecto era muy necesario aplicar los conocimientos adquiridos.

7. Comprende y manipula ideas y pensamientos respecto a los modelos de seguridad.

Explicación: Durante el desarrollo de algunas actividades de evaluación se aplicaron modelos como el modelo COBIT, el cual fue de gran ayuda para poder tener una escala evaluativa, por lo que la aplicación de esta competencia principalmente se centró durante el desarrollo de estas actividades.

8. Comprende las necesidades del medio ambiente y toma decisiones para resolver la problemática que se le presentan con respecto al control de accesos.

Explicación: Esta competencia fue aplicada principalmente en la implementación de las nuevas políticas de restricción de acceso donde previamente se encontraron las principales necesidades y problemáticas que se tenían en EQF de acuerdo con las políticas de restricción de acceso que se tenían implementadas anteriormente.

Materia: Administración de la Seguridad en Comunicaciones

Competencias específicas:

1. Toma decisiones para elegir las medidas de seguridad más apropiadas ante un determinado escenario de riesgos.

Explicación: La aplicación de esta competencia principalmente se puede ver reflejada en la actividad donde se llevo a cabo las propuestas de solución, en la cual se dan las mejores medidas de seguridad las cuales puedan brindar la mejor protección ante escenarios de riesgos.

Competencias genéricas:

1. Conocimiento de una segunda lengua

Explicación: Esta competencia fue aplicada principalmente en la investigación de la documentación del antivirus, ya que algunas veces la documentación se encontraba en el idioma inglés, por lo tanto, al tener conocimiento de esta lengua resulto fácil poder entender dicha documentación, de igual manera algunas consultas o búsquedas que se realizaron tuvieron que ser en inglés.

Materia: Taller de investigación II

Competencias genéricas:

1. Capacidad de investigación

Explicación: La aplicación de esta competencia fue llevada a cabo durante la búsqueda de información tanto para el marco teórico como para la documentación del antivirus, en donde se tuvieron que consultar diversas fuentes de información las cuales resultaran confiables, o que el sitio donde consulto fuera de alguna empresa o institución oficial.

2. Habilidad para trabajar en forma autónoma.

Explicación: Esta competencia se aplicó en la mayor parte durante la implementación del antivirus, ya que se tenía que realizar la planificación, la negociación entre otras actividades de manera autónoma para posteriormente poder llevar a cabo su implementación de dichas actividades.

3. Capacidad de trabajar en equipo

Explicación: Esta competencia es fue gran importancia tanto para el desarrollo de este proyecto, como para el contexto en el cual se llevó a cabo, ya que al ser una

empresa se debía tener comunicación con algunos de los colaboradores que trabajan dentro de EQF, incluso para poder desarrollar adecuadamente algunas actividades.

FUENTES DE INFORMACIÓN

- Acces Quality. (11 de agosto de 2020). *¿Qué es un EndPoint? Fundamental para Proteger a tu Empresa*. Obtenido de Acces Quality: <https://www.accessq.com.mx/que-es-un-endpoint>
- AV Comparatives. (s.f.). *Sobre nosotros*. Obtenido de AV Comparatives: <https://www.av-comparatives.org/about-us/>
- Avast. (s.f.). *¿Qué es el malware y cómo protegerse de los ataques?* Obtenido de Avast: <https://www.avast.com/es-es/c-malware>
- AV-Test. (s.f.). *Sobre el instituto AV-TEST*. Obtenido de AV-Test: <https://www.av-test.org/es/sobre-el-instituto/>
- Channel Partner. (04 de mayo de 2023). *Qué es un endpoint y cómo funciona*. Obtenido de Channel Partner: <https://www.channelpartner.es/seguridad/que-es-un-endpoint/>
- Dharma Consulting. (28 de Septiembre de 2023). *Desentrañando el Valor Monetario Esperado: ¿Cómo cuantificar riesgos en proyectos Scrum?* Obtenido de Dharma Consulting: <https://dharmacon.net/2023/09/28/desentrañando-el-valor-monetario-esperado-como-cuantificar-riesgos-en-proyectos-scrum/#:~:text=Consiste%20en%20multiplicar%20el%20impacto,que%20ese%20riesgo%20realmente%20suceda.>
- El Financiero. (07 de septiembre de 2023). *Hackers 'roban' 67 mdp a bancos de México: ¿Qué sabemos de los ataques cibernéticos?* Obtenido de El Financiero: <https://www.elfinanciero.com.mx/economia/2023/09/07/hackers-roban-67-mdp-a-bancos-de-mexico-que-sabemos-de-los-ataques-ciberneticos/>
- Forbes México. (28 de Junio de 2023). *México, blanco de 66% de ataques cibernéticos en América Latina*. Obtenido de Forbes México: <https://www.forbes.com.mx/mexico-blanco-de-66-de-ataques-ciberneticos-en-america-latina/#:~:text=Del%202021%20al%202022%2C%20M%C3%A9xico,Asociaci%C3%B3n%20de%20Bancos%20de%20M%C3%A9xico.>
- Fortinet. (s.f.). *Virus Troyanos*. Obtenido de Fortinet: <https://www.fortinet.com/lat/resources/cyberglossary/trojan-horse-virus>
- Global Suite Solutions. (22 de septiembre de 2023). *¿Qué es la norma ISO 27001 y para qué sirve?* Obtenido de Global Suite Solutions: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>
- gtd Perú. (s.f.). *Sandboxing: ¿Qué es y cómo funciona?* Obtenido de gtd Perú: https://www.gtdperu.com/es/w/novedades/sandboxing_que_es_y_como_funciona
- IBM. (s.f.). *¿Qué es el ransomware?* Obtenido de IBM: <https://www.ibm.com/mx-es/topics/ransomware>
- IBM. (s.f.). *¿Qué es un ataque cibernético?* Obtenido de IBM: <https://www.ibm.com/mx-es/topics/cyber-attack>

- IONOS. (05 de Julio de 2021). *Kernel - El núcleo del sistema operativo*. Obtenido de IONOS: <https://www.ionos.mx/digitalguide/servidores/know-how/que-es-el-kernel/>
- ISACA. (s.f.). *COBIT An ISACA Framework*. Obtenido de ISACA: <https://www.isaca.org/resources/cobit/>
- ISO Tools Excellence. (s.f.). *ISO 27001*. Obtenido de ISO Tools Excellence: <https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/>
- Kallos, J. (20 de septiembre de 2018). *¿Por qué tener una conexión cifrada con SSL si no vendo online?* Obtenido de GoDaddy: <https://es.godaddy.com/blog/tener-una-conexion-cifrada-con-ssl-si-no-vendo-online/>
- Kaspersky. (2023). *Cómo prevenir ciberataques*. Obtenido de Kaspersky: <https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks>
- Kaspersky. (2023). *Kaspersky partner locator*. Obtenido de Kaspersky: https://locator.kaspersky.com/b2b/?locale=la&filter_UF_COUNTRY=a0Ea000000G1K8fEAF&filter_UF_STATE=a0Ra000000AMxFOEA1&filter_ADDRESS=&filter_ADDRESS_S=&filter_ADDRESS_W=&filter_ADDRESS_N=&filter_ADDRESS_E=&filter_UF_COUNTNAME=&set_filter=Buscar
- Kaspersky. (2024 de Enero de 22). *Kaspersky Security Center Cloud Console*. Obtenido de Kaspersky: https://support.kaspersky.com/mx/ksc_cloudconsole/166295
- McAfee. (s.f.). *¿Qué es malware?* Obtenido de McAfee: <https://www.mcafee.com/es-mx/antivirus/malware.html>
- Microsoft. (s.f.). *¿Qué es un firewall?* Obtenido de Microsoft: <https://support.microsoft.com/es-es/office/-qu%C3%A9-es-un-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603>
- Microsoft. (06 de Junio de 2023). *Unidad de disco duro cifrada*. Obtenido de Microsoft: <https://learn.microsoft.com/es-es/windows/security/operating-system-security/data-protection/encrypted-hard-drive>
- Oracle España. (s.f.). *¿Cuáles son los ataques cibernéticos de los que es absolutamente necesario protegerse?* Obtenido de Oracle: <https://www.oracle.com/es/database/security/protecting-from-cyber-attack.html>
- Prado Oseguera, D. M. (Junio de 2009). *Metodología para el establecimiento de de objetivos de control como un medio de seguridad en el área de tecnologías de la información*. Ciudad de México, México.
- PWC. (2023). *Digital Trust Insights 2023, edición México. El camino para fortalecer la ciberseguridad*. Obtenido de PWC: <https://www.pwc.com/mx/es/ciberseguridad/digital-trust.html>
- Richard, R. (18 de agosto de 2016). *NORMA ISO 17799*. Obtenido de Romero Richard: <https://romerorichard.wordpress.com/2016/08/18/norma-iso-17799/>
- SE Labs. (s.f.). *Acerca de SE Labs*. Obtenido de SE Labs: <https://selabs.uk/about/>

Treviño, R. (26 de Octubre de 2021). *¡Protege tus datos! 10 consejos de ciberseguridad para evitar ataques.* Obtenido de Tecnológico de Monterrey: <https://conecta.tec.mx/es/noticias/nacional/educacion/protege-tus-datos-10-consejos-de-ciberseguridad-para-evitar-ataques>

ANEXOS

Anexo 1. Evidencia de la revisión de control donde se muestra que se puede ingresar a la plataforma de YouTube, la cual está prohibido el acceso.

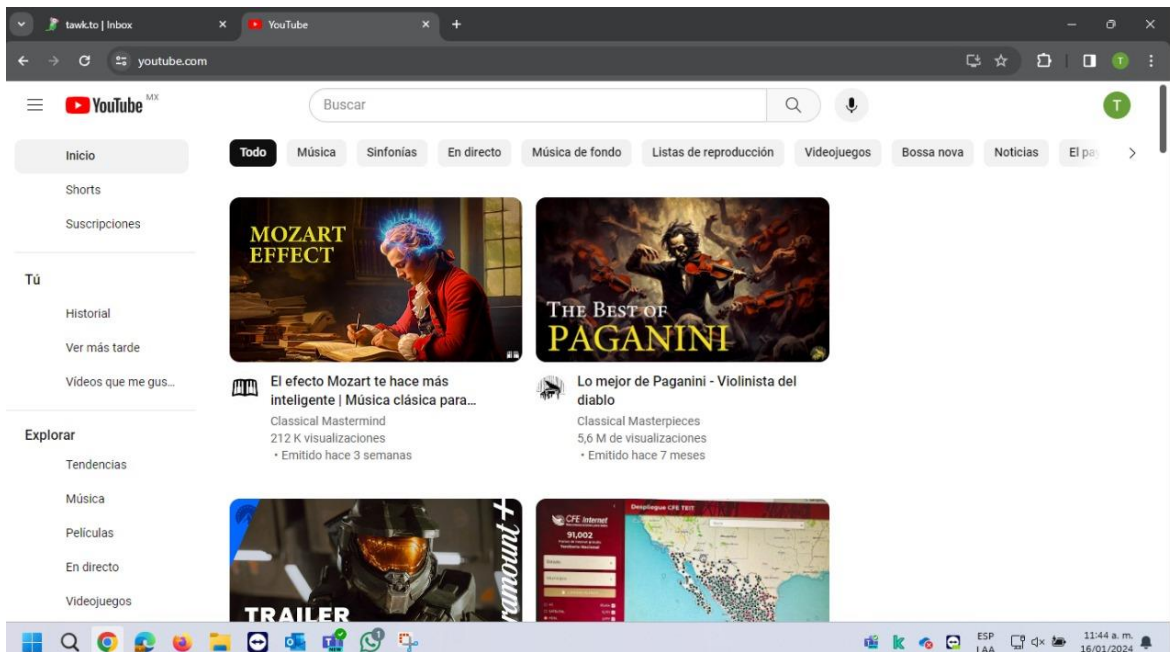


Figura 72 Evidencia de acceso a YouTube. [Elaboración propia]

Anexo 2. Manual técnico de Kaspersky enfocado a las necesidades de EQF.



MANUAL TÉCNICO

KASPERSKY ENPOINT DETECTION AND RESPONSE
OPTIMUM PARA EQUILIBRIO FARMACÉUTICO

Aldo Mota Zarate

Enero, 2024

ÍNDICE

Introducción	191
Agente de Kaspersky.....	192
Descarga del instalador agente de Kaspersky a través de la consola.	192
Instalación del agente de Kaspersky en un equipo de cómputo.	196
Grupos de dispositivos	199
Asignar dispositivos a un grupo.	199
Búsqueda de dispositivos dentro del grupo.	200
Antivirus	201
Instalación de antivirus.....	201
Tareas.....	203
Creación de tareas	203
Actualización de base de datos de virus	207
Políticas de restricción	209
Políticas de restricción a sitios web	209
Políticas de restricción de acceso a aplicativos.....	213
Políticas de restricción de acceso a dispositivos	217
Interfaz	221
Configuración de interfaz para el usuario	221

Introducción

Este manual técnico ofrece una guía integral para la implementación y gestión efectiva del antivirus de Kaspersky en su entorno empresarial para Equilibrio Farmacéutico. Comenzando con la instalación uniforme del agente de Kaspersky en los equipos de la empresa, la guía abarca la instalación centralizada desde el servidor, el seguimiento y mantenimiento para mantener actualizada la base de datos de virus, la personalización de políticas de seguridad según las necesidades de la Equilibrio Farmacéutico, y la realización de pruebas para verificar el correcto funcionamiento. Este enfoque proactivo asegura un entorno computacional seguro y protegido contra amenazas cibernéticas, alineando la seguridad con los objetivos y procesos del negocio.

Agente de Kaspersky.

Descarga del instalador agente de Kaspersky a través de la consola.

1. Iniciar sesión con la cuenta de administrador. En seguida se presenta una pantalla la cual muestra la empresa o el grupo de empresas que tienen contratado el servicio de Kaspersky.
2. Dar clic a la empresa en la cual se va a trabajar, en este caso la de **“Grupo Viso”** (Empresa central a la cual EQF pertenece).
3. Seleccionar la opción de **“Ir al espacio de trabajo”** para poder acceder a la consola la cual administra todo lo referente al antivirus de Kaspersky.

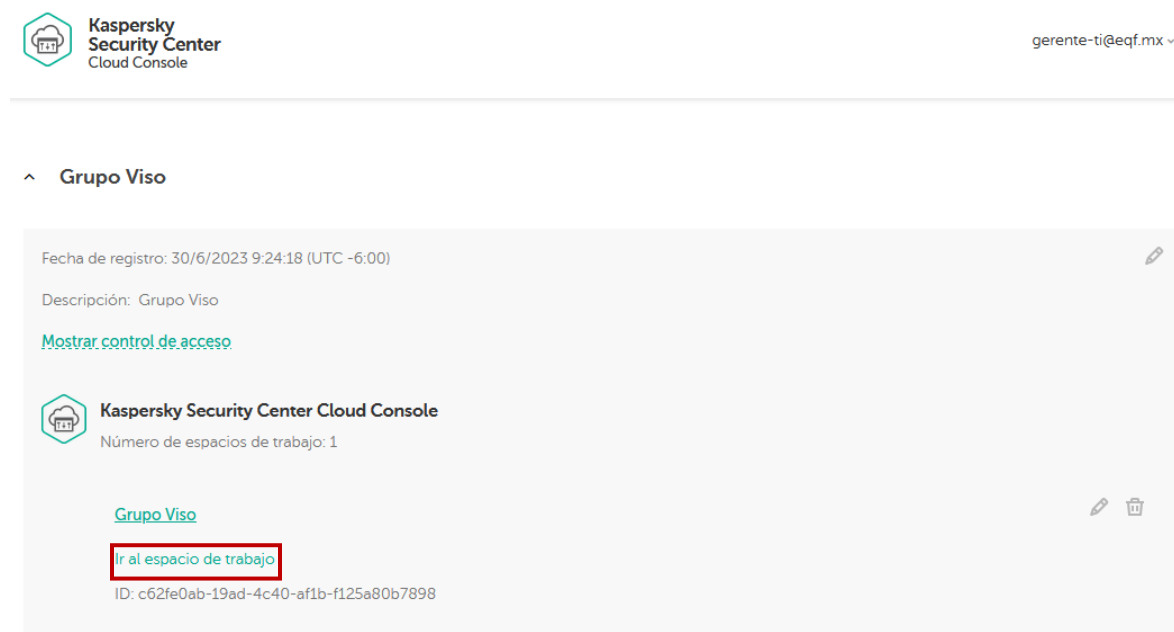


Figura 73 Interfaz para poder acceder a la consola de administración de Kaspersky.

4. Una vez que se ingresó al espacio de trabajo, se presenta la interfaz donde se muestra el panel general sobre algunos eventos de ataques ocurridos, el estatus de protección de los dispositivos, amenazas que fueron detectadas, entre otras características. Además de ello, se muestran las diferentes opciones para poder llevar a cabo la administración de los dispositivos que están protegidos, políticas de restricción, operaciones, los usuarios y roles, configuración, entre otras opciones para poder llevar a cabo la administración de protección de los dispositivos.

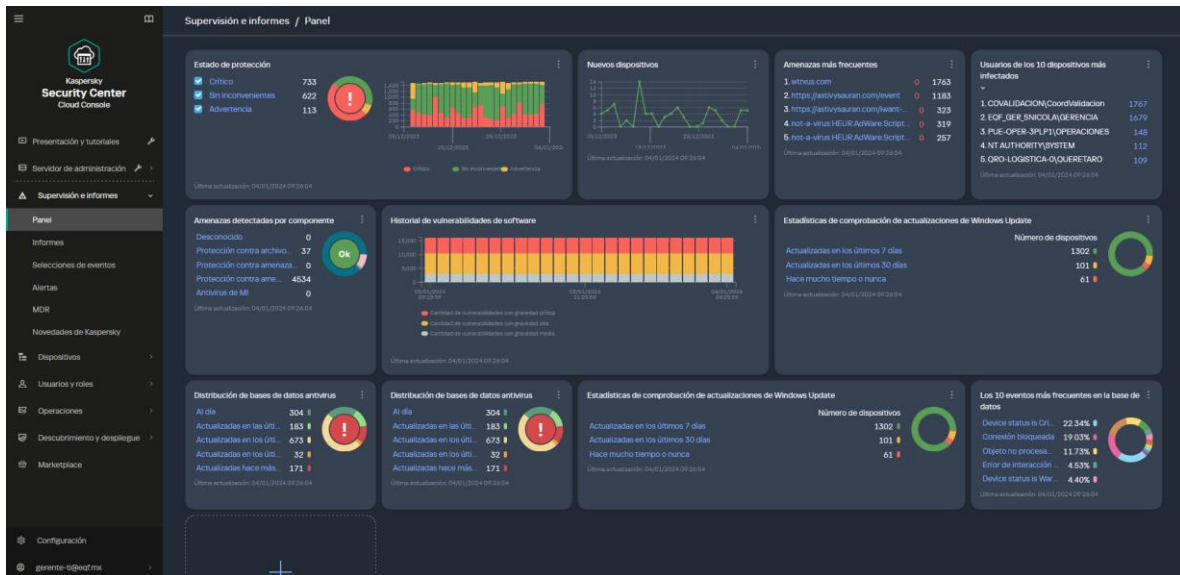


Figura 74 Panel general de Kaspersky.

5. Ingresar al menú de **“Descubrimiento y despliegue”** el cual es encuentra en el panel de la parte izquierda de la interfaz
6. Seleccionar **“Despliegue y asignación”**, aquí se desplegará un submenú con diversas opciones.
7. Después dar clic en **“Paquetes de instalación”**, para ingresar y poder generar el instalador del agente de Kaspersky.

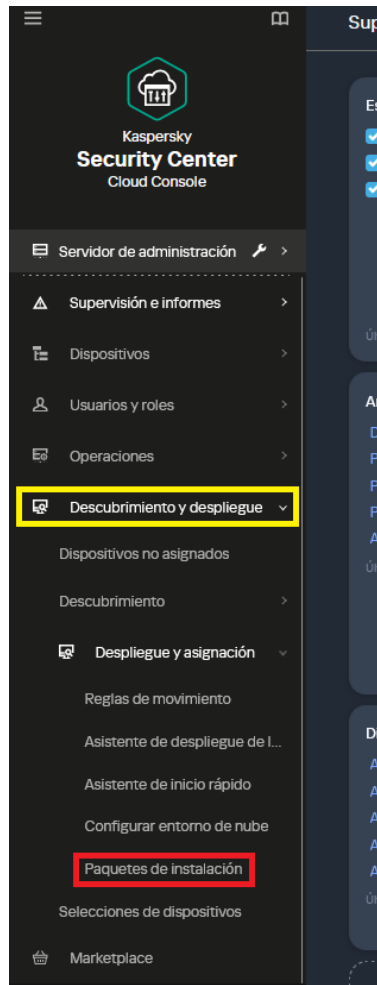


Figura 75 Menú para ingresar a la descarga del agente de Kaspersky.

8. A continuación, se presenta una pantalla la cual contiene diversos paquetes, sin embargo, se tiene que dar clic en la opción de **“Kaspersky Security Center 14 Network Agent (Español (México)) 14 2.0.35148”**.

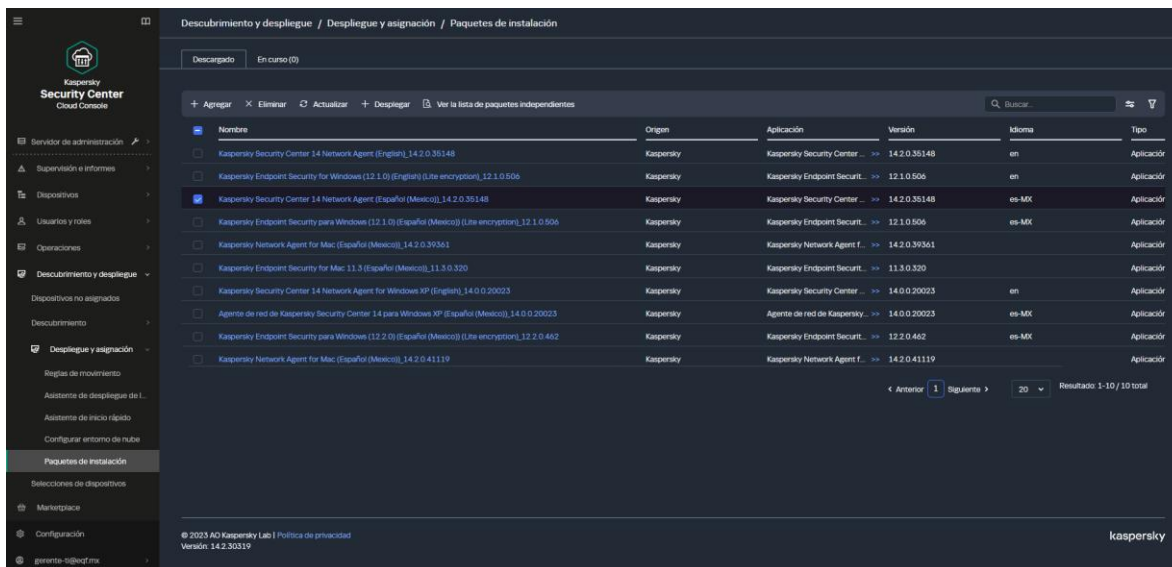


Figura 76 Paquetes de instalación.

Dentro del paquete de instalación se muestran sus propiedades que este contiene como la información general del paquete, la configuración, sus paquetes independientes de instalación y el historial de las versiones del agente.

9. Ingresar a la propiedad de **“Paquetes independientes”**, para la descarga del agente.



Figura 77 Propiedades del paquete independiente.

10. Seleccionar la opción **“Kaspersky Security Center 14 Network Agent (Español (México)) 14.2.0.35148”**

11. Dar clic en “**Descargar**” y se comenzara a realizar la descarga del instalador del agente de Kaspersky.

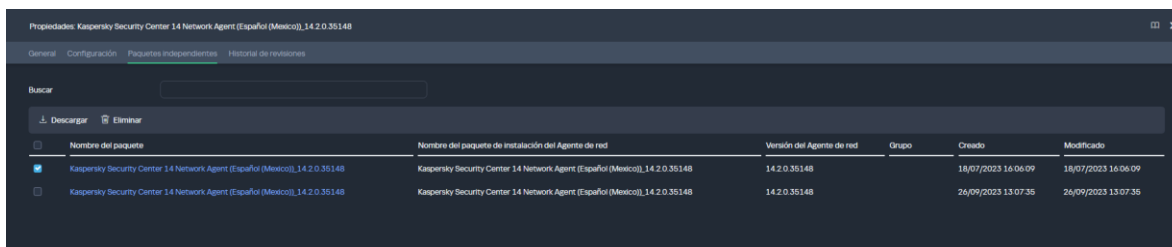


Figura 78 Opciones del instalador del agente de Kaspersky.

A continuación se muestra el ejecutable del agente del antivirus de Kaspersky que se genera a partir de la consola de administración, el cual se tiene que instalar posteriormente en los dispositivos de EQF.

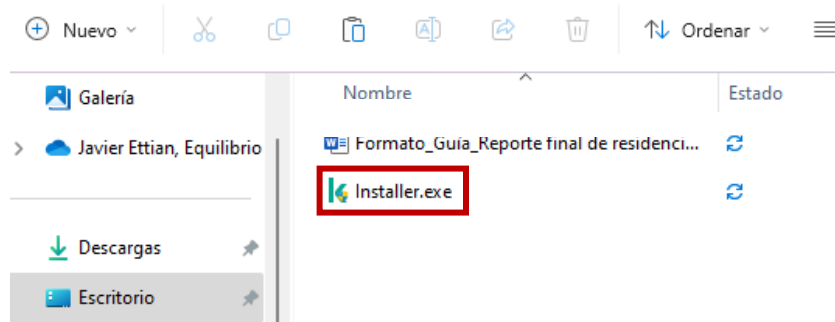


Figura 79 Archivo ejecutable del agente.

Instalación del agente de Kaspersky en un equipo de cómputo.

1. Para iniciar con la instalación se debe de **ejecutar el instalador del agente como administrador**, e ingresar las credenciales en caso de que las pida el sistema.
2. Dar clic en el botón de “**Iniciar instalación**” y comenzará con el proceso de instalación en el dispositivo.

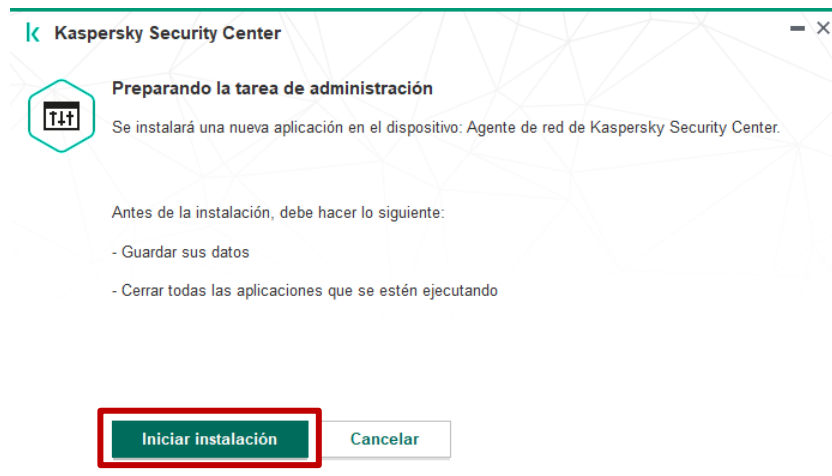


Figura 80 Comienzo de instalación del agente.

Mientras se realiza el proceso de instalación se mostrará una ventana donde se indica el avance del proceso de instalación el cual conste de tres etapas; la primera es la extracción del archivo a una ubicación temporal, después la instalación del agente y por último se comprueba la conexión al servidor de administración.



Figura 81 Proceso de instalación.

3. Ya que se terminó exitosamente el proceso de instalación del agente, el último paso que queda es dar clic en el botón de **“Aceptar”**.



Figura 82 Termino del proceso de instalación del agente de Kaspersky.

4. Para comprobar que se instaló el agente de Kaspersky en el dispositivo, se debe de **ingresar a los programas que están instalados en el dispositivo** y verificar que el agente de Kaspersky se encuentre aquí.

Nombre	Editor	Se instaló el	Tamaño	Versión
Agente de red de Kaspersky Security Center	Kaspersky	09/01/2024	118 MB	14.2.0.35148
AnyDesk	AnyDesk Software GmbH	09/11/2023	2.00 MB	6.0.0.0
Aplicaciones de Microsoft 365 para negocios - es-es	Microsoft Corporation	09/01/2024		16.0.17126.20132
Atención al cliente	Lexmark International, Inc.	22/06/2023	276 KB	1.0.0.0
Brother Printer Setting Tool	Brother Industries, Ltd.	01/12/2023	133 MB	1.6.0110
Brother P-touch Address Book 1.4	Brother Industries, Ltd.	18/01/2023	54.4 MB	1.4.0010
Brother P-touch Editor 5.4	Brother Industries, Ltd.	01/12/2023	38.6 MB	5.4.0110
Brother P-touch Update Software	Brother Industries, Ltd.	18/01/2023	2.85 MB	1.0.0230
Centro de información	Lexmark International, Inc.	22/06/2023	1.33 MB	1.0.0.0
Cisco Packet Tracer 8.2.1 64Bit	Cisco Systems, Inc.	27/10/2023	564 MB	8.2.1.118
Componentes del Motor de administración Intel®	Intel Corporation	13/12/2023	27.5 MB	2313.4.16.0
Comprobación de estado de PC Windows	Microsoft Corporation	17/01/2023	11.6 MB	3.6.2204.08001
Conexión a Escritorio remoto	Microsoft Corporation	23/08/2023		
Dell SupportAssist	Dell Inc.	13/12/2023	316 MB	3.14.2.45116
Dell SupportAssist OS Recovery Plugin for Dell Update	Dell Inc.	14/12/2023	64.1 MB	5.5.7.18773
DHTML Editing Component	Microsoft Corporation	27/01/2023	554 KB	6.02.0001
EPSON Advanced Printer Driver 4	EPSON	25/01/2023		4.12.0006
Google Chrome	Google LLC	08/01/2024		120.0.6099.200
H264 Video Codec	T,DP5	30/09/2023		
Información sobre reciclaje de residuos de la UE	Lexmark International, Inc.	22/06/2023	328 KB	1.0.0.0
Intel® Integrated Sensor Solution	Intel Corporation	13/12/2023	1.59 MB	3.10.100.4140
iVMS-4200	Hangzhou Hikvision Digital Tec...	13/07/2023		3.9.1.4

Programas actualmente instalados Tamaño total: 7.62 GB
72 programas instalados

Figura 83 Comprobación de la instalación del agente de Kaspersky.

Grupos de dispositivos

Asignar dispositivos a un grupo.

1. Ingresar al menú “**Descubrimiento y despliegue**”.
2. Dar clic en la opción “**Dispositivos no asignados**”. Aquí se mostrarán todos los dispositivos en los que se ha instalado el agente y no han sido asignados a un grupo para su administración.
3. Buscar el dispositivo que será asignado a un grupo. **Seleccionar el dispositivo dando clic en la casilla** que se encuentra del lado izquierdo del nombre del equipo
4. Dar clic en la opción de “**Mover a un grupo**”, la cual se encuentra en el menú de la parte superior de los dispositivos.

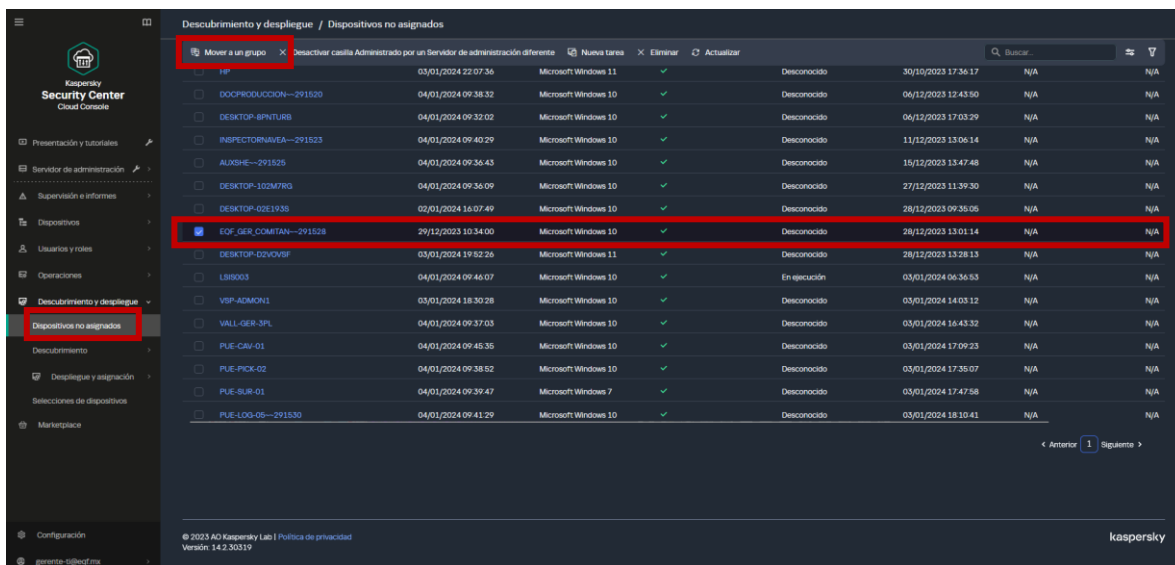


Figura 84 Dispositivos no asignados a un grupo.

5. **Seleccionar la casilla de la empresa** (si es que existe más de una dentro de la configuración) a la cual se le va a asignar el dispositivo que no tiene un grupo.

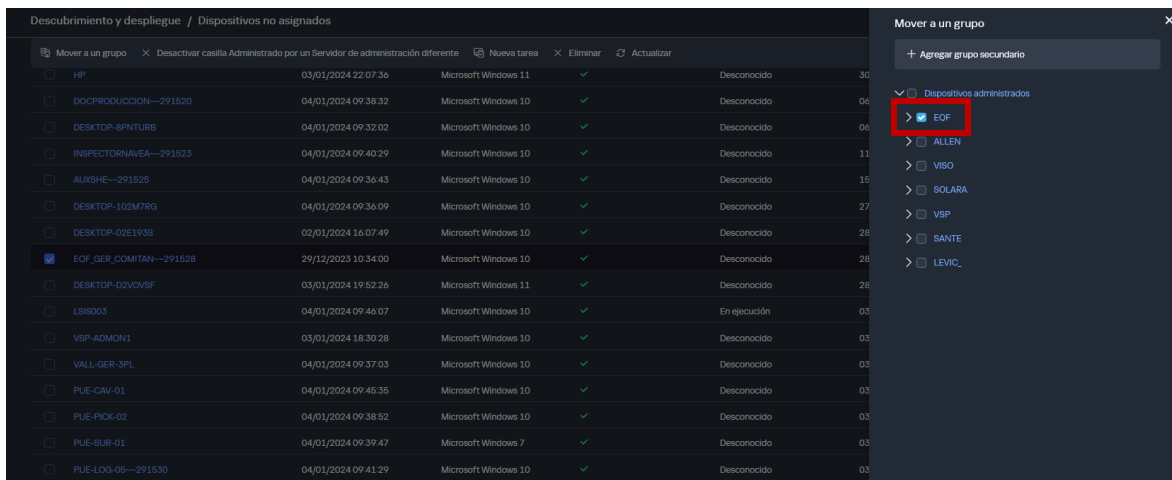


Figura 85 Asignación de grupo.

Búsqueda de dispositivos dentro del grupo.

1. Seleccionar el apartado “**Dispositivos**”, en el menú de la parte izquierda.
2. Dar clic en la opción “**Dispositivos administrados**”. Aquí se muestran todos los dispositivos que pertenecen al grupo de EQF y los cuales pueden ser administrados o se le pueden realizar diversas acciones.

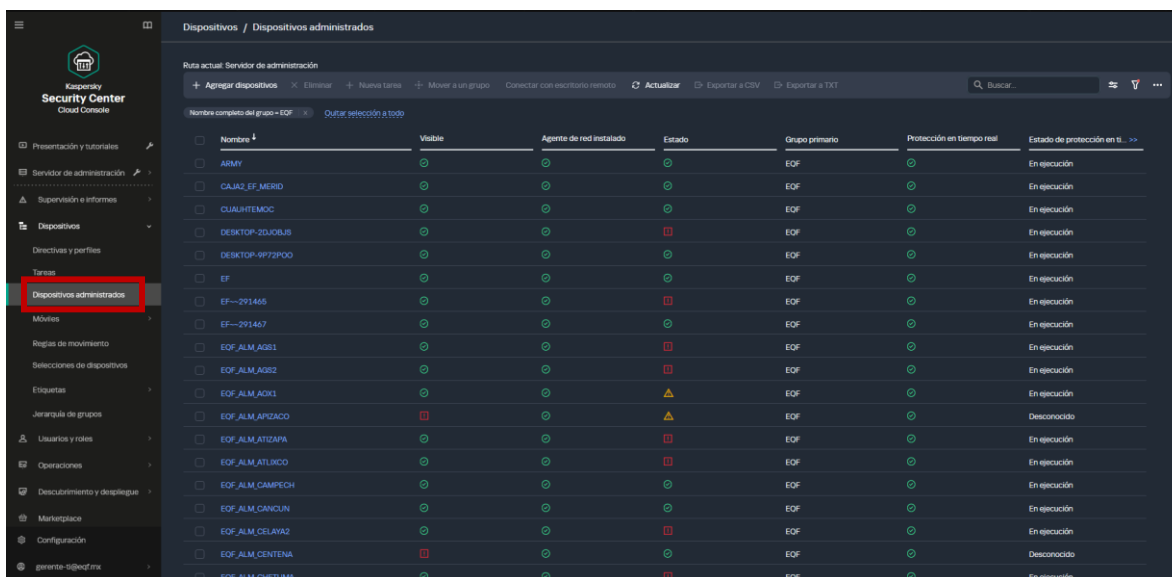


Figura 86 Dispositivos administrados dentro del grupo de EQF.

Una manera más sencilla de buscar que un dispositivo se encuentre dentro de un grupo en este caso el de EQF, es buscándolo por su nombre, para esto se deben de seguir los siguientes pasos:

1. Dar clic en el **“Buscador”**, que se encuentra en el menú de la parte superior de los dispositivos asignados
2. **Ingresa el nombre del dispositivo** que se quiere encontrar, por ejemplo **“EQF_GER_COMITAN”**. Como se puede observar el dispositivo se encuentra dentro del grupo de EQF.

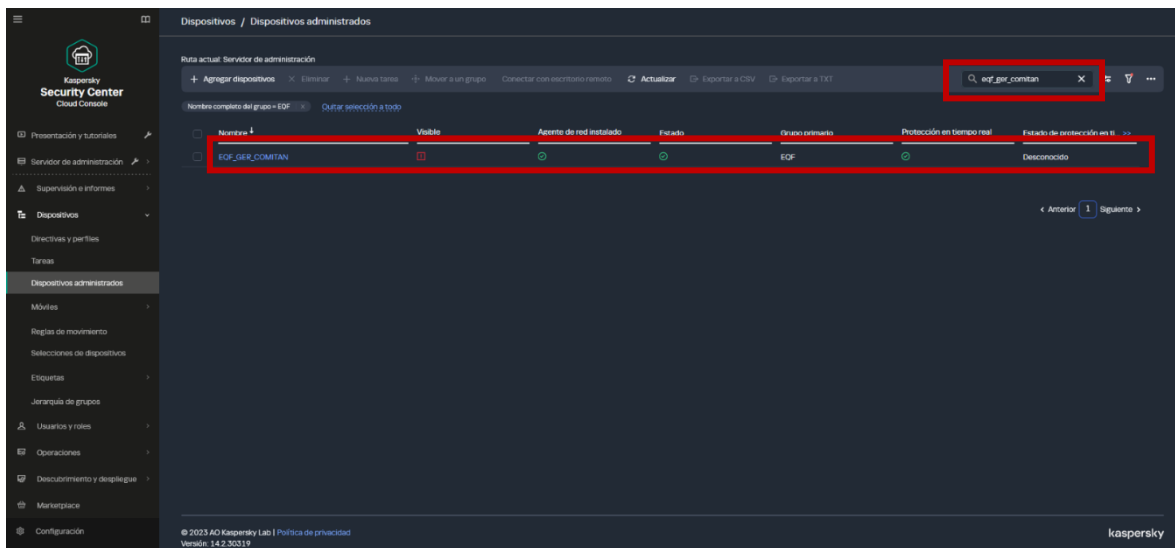


Figura 87 Búsqueda de dispositivos.

Antivirus

Instalación de antivirus

Para la instalación del antivirus en los dispositivos, cabe mencionar que, al momento de asignar los dispositivos a un grupo, en este caso el de EQF, de manera automática la consola de Kaspersky instala el antivirus en los equipos. Sin embargo, para verificar que realmente estén protegidos es necesario seguir los siguientes pasos:

1. Seleccionar el apartado de **“Dispositivos”**, que se sitúa en el menú de la parte izquierda
2. Dar clic en la opción **“Dispositivos administrados”**. Aquí se muestran todos los dispositivos que pertenecen al grupo de EQF y los cuales pueden ser administrados o se le pueden realizar diversas acciones.

Nombre	Visible	Agente de red instalado	Estado	Grupo primario	Protección en tiempo real	Estado de protección en tiempo real
ARMY	✓	✓	✓	EQF	✓	En ejecución
CAJAZ_EF_MERID	✓	✓	✓	EQF	✓	En ejecución
CUALHTEMOC	✓	✓	✓	EQF	✓	En ejecución
DESKTOP-2DU0BUS	✓	✓	✗	EQF	✓	En ejecución
DESKTOP-9F72P00	✓	✓	✓	EQF	✓	En ejecución
EF	✓	✓	✓	EQF	✓	En ejecución
EF--291465	✓	✓	✗	EQF	✓	En ejecución
EF--291467	✓	✓	✓	EQF	✓	En ejecución
EQF_ALM_A001	✓	✓	✗	EQF	✓	En ejecución
EQF_ALM_A002	✓	✓	✗	EQF	✓	En ejecución
EQF_ALM_A003	✓	✓	⚠	EQF	✓	En ejecución
EQF_ALM_A004	✗	✓	⚠	EQF	✓	Desconocido
EQF_ALM_A005	✓	✓	✗	EQF	✓	En ejecución
EQF_ALM_A006	✓	✓	✗	EQF	✓	En ejecución
EQF_ALM_A007	✓	✓	✓	EQF	✓	En ejecución

Figura 88 Dispositivos administrados.

Como se puede observar al momento de que los dispositivos son asignados a un grupo de muestran diversas características:

- **“Agente de red instalado”**, indica que el dispositivo tiene instalado el agente de Kaspersky.
- **“Estado”**, indica el estado en que se encuentra el dispositivo.
- **“Grupo”**, indica el grupo al que pertenece.
- **“Protección en tiempo real”**, indica si el dispositivo está protegido en tiempo real
- **“Ejecución de protección en tiempo real”**, muestra si la protección en tiempo real se esté ejecutando.

Por lo tanto, para saber que el dispositivo está protegido se debe mostrar una palomita de color verde en la columna de **“Ejecución de protección en tiempo real”**.

Nombre	Visible	Agente de red instalado	Estado	Grupo primario	Protección en tiempo real	Estado de protección en tiempo real
ARMY	✓	✓	✓	EQF	✓	En ejecución
CAJAZ_EF_MERID	✓	✓	✓	EQF	✓	En ejecución
CUALHTEMOC	✓	✓	✓	EQF	✓	En ejecución
DESKTOP-2DU0BUS	✓	✓	✗	EQF	✓	En ejecución
DESKTOP-9F72P00	✓	✓	✓	EQF	✓	En ejecución

Figura 89 Propiedades del estado de protección de los dispositivos.

Tareas

Creación de tareas

Las tareas dentro de la consola de administración permiten realizar diversas actividades para los diferentes tipos de protección que se tengan contratados en la empresa. Por lo tanto, para crear dicha tarea se deben de hacer los siguientes pasos:

1. Seleccionar el menú de **“Dispositivos”**, el cual se encuentra en el panel de la parte izquierda.
2. Posteriormente dar clic en la opción de **“Tareas”**.

Dentro de la opción de “Tareas” se muestra un panel el cual contiene todas las tareas que se hayan creado con anterioridad, además de ello se muestra un menú el cual nos permite realizar diversas acciones con las tareas ya creadas o de lo contrario crear una nueva tarea de acuerdo con la necesidad que se tenga.

3. Ahora para crear una nueva tarea, se debe dar clic en **“Agregar”**, la cual se encuentra en el menú de la parte superior donde se reflejan las tareas que se han creado.

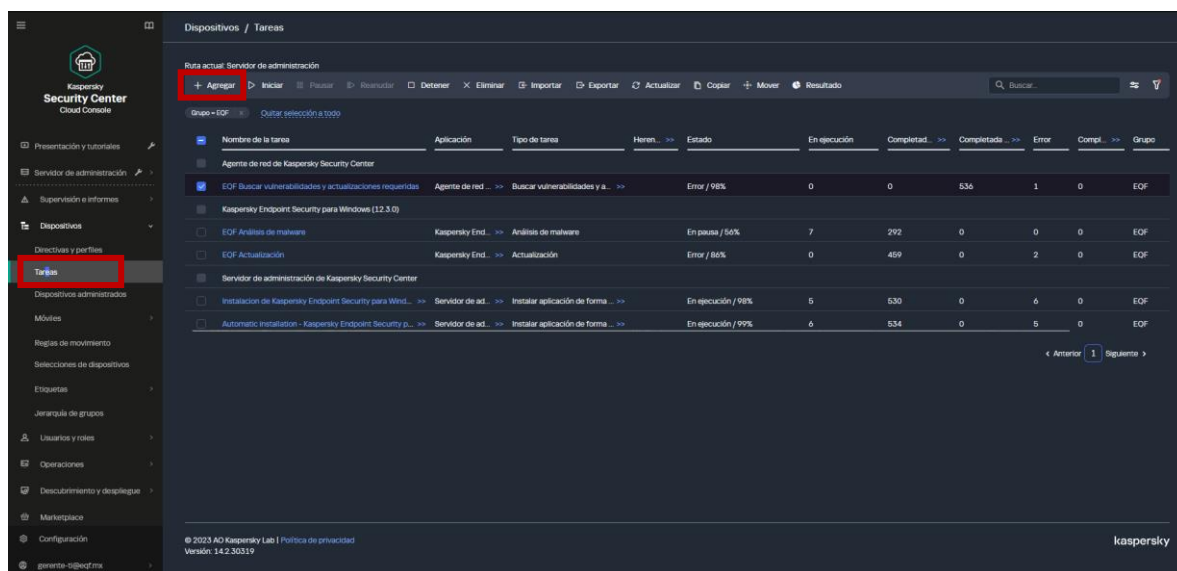


Figura 90 Interfaz de las tareas de Kaspersky.

Posteriormente, se muestra un asistente la cual nos muestra diversas características para la creación de una tarea, al igual que la aplicación a la cual se le va a realizar alguna acción, el tipo de tarea que se requiera realizar, el nombre de la tarea y por último un checklist para seleccionar los dispositivos a los cuales se le aplicara la tarea que se va a crear.

4. Ahora, se tiene que seleccionar la aplicación a la cual se le va a aplicar la tarea, en este caso la de **“Kaspersky Security Center 14.2”**.

Figura 91 Asistente para crear una nueva tarea.

5. Seleccionar el tipo de tarea que se va a realizar, para ello se tiene que dar clic en **“Tipo de tarea”**.
6. Seleccionar el tipo de tarea que se quiera realizar, por ejemplo, la actualización de la base de datos de virus. Por lo tanto, se tiene que elegir **“Buscar vulnerabilidades y actualizaciones requeridas”**.

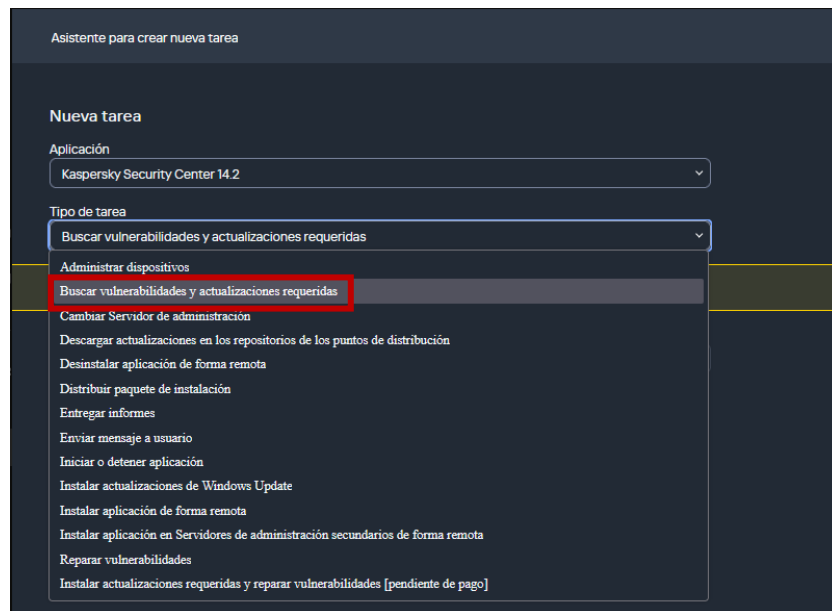


Figura 92 Tipos de tareas en Kaspersky.

7. A continuación, se debe de seleccionar el alcance que tendrá la tarea, es decir, se deben elegir las diferentes empresas a las cuales se puede aplicar la tarea que se está creando, esto dependerá si hay una o más empresas dentro de un grupo de empresas. Sin embargo, para este caso solo se debe **seleccionar la casilla de “EQF”**.

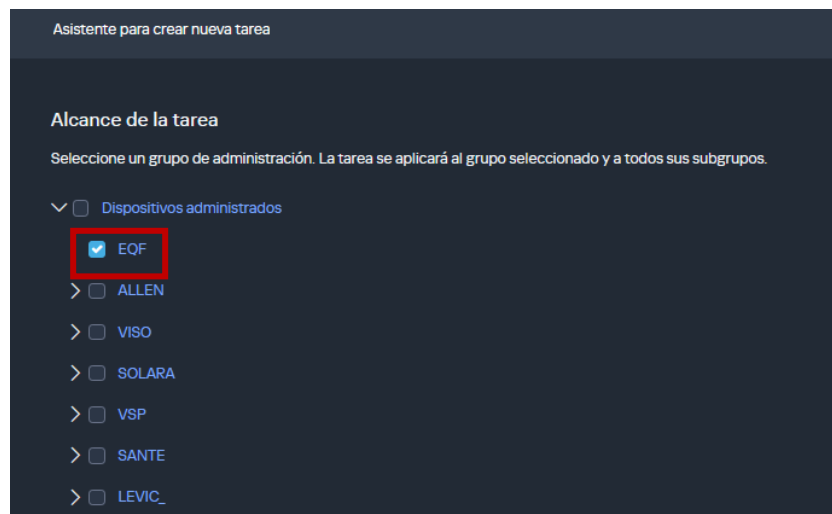


Figura 93 Alcance de la tarea.

8. En seguida, se muestran más acciones que se pueden realizar:
 - a. Especificación de los métodos que se van a utilizar para detectar aplicaciones que tengan vulnerabilidades o que deban actualizarse.

- b. Especificar las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos
- c. Tamaño que debe de tener el archivo de diagnóstico avanzado.

Sin embargo, estas opciones se dejarán por defecto.

Figura 94 Especificaciones de la tarea.

9. Finalmente, se muestra una casilla la cual nos permite abrir los detalles de la tarea cuando se complete la creación, esta opción puede ser opcional, en este caso no se seleccionará y solamente se dará **clic en el botón de “Finalizar”**.

Figura 95 Termino de la tarea creada.

Actualización de base de datos de virus

Para poder actualizar la base de datos de virus en todos los equipos que se encuentren dentro de un grupo, se tienen que realizar los siguientes pasos:

1. Seleccionar el menú de **“Dispositivos”**, el cual se encuentra en el panel de la parte izquierda.
2. Posteriormente dar clic en la opción de **“Tareas”**. Aquí se muestran todas las tareas que se hayan creado con anterioridad.

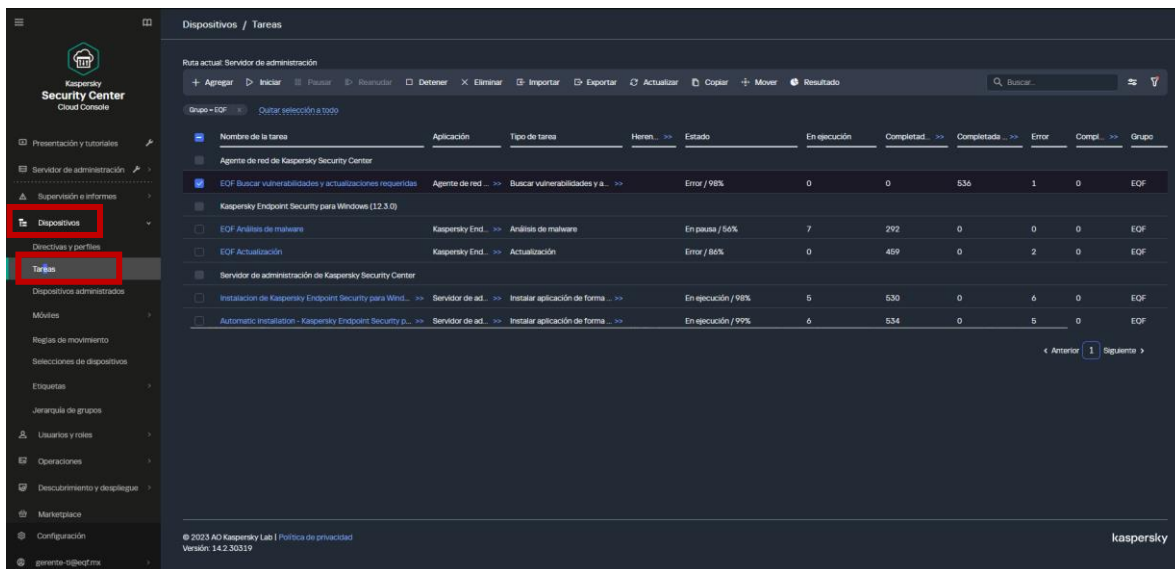


Figura 96 Interfaz de las tareas de Kaspersky.

3. Buscar la tarea que fue creada para la actualización de la base de datos, en este caso, **“Buscar vulnerabilidades y actualizaciones requeridas”** y **seleccionar la casilla que tiene de lado izquierdo**.
4. Dar clic en la opción de **“Iniciar”**, que se encuentra en el menú de la parte superior.

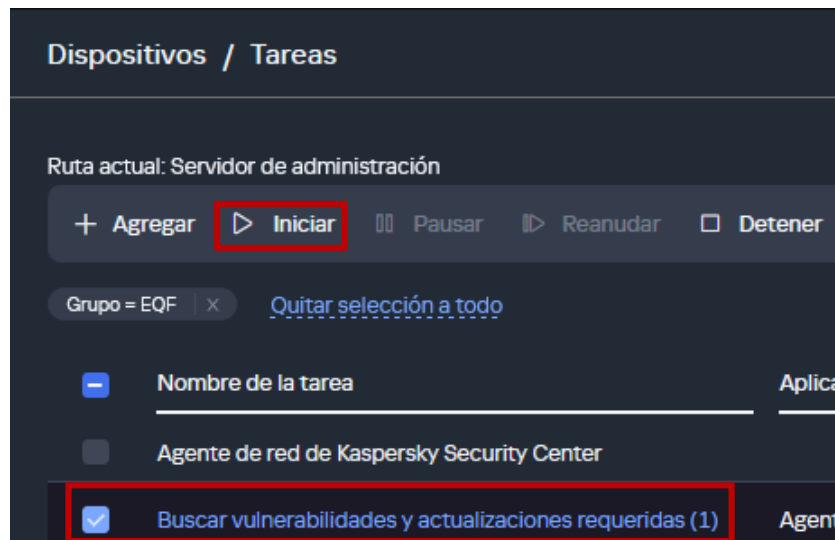


Figura 97 Inicio de la tarea creada para la actualización de la base de datos de virus.

Una vez iniciada la tarea, se muestran los siguientes apartados o columnas:

- **“Estado”**, muestra el estado de cómo va avanzando su ejecución.
- **“Ejecución”**, indica el número de dispositivos en los que se está ejecutando la tarea.
- **“Completado”**, indica el número de dispositivos en los que se completó la tarea
- **“Error”**, el número de errores que se tuvieron durante la ejecución de la tarea.

Grupo = EQF Quitar selección a todo										
☐	Nombre de la tarea	Aplicación	Tipo de tarea	Heren... >>	Estado	En ejecución	Completad... >>	Completada... >>	Error	Compl... >>
☐	Agente de red de Kaspersky Security Center									
☒	Buscar vulnerabilidades y actualizaciones requeridas (1)	Agente de red ... >>	Buscar vulnerabilidades y a... >>		En ejecución / 1%	10	0	3	0	0

Figura 98 Estado de la tarea en ejecución.

De esta manera se puede mantener y dar seguimiento a la actualización de la base de datos de virus para tenerla al día y pueda proteger a los dispositivos de aquellas amenazas o virus que sean nuevos.

Políticas de restricción

Políticas de restricción a sitios web

Para comenzar con la instalación de las políticas de restricción de acceso, primeramente, se debe de tener el agente y el antivirus de Kaspersky en los equipos los cuales pertenecen al grupo de EQF.

1. Ingresar a la opción de **“Activos (dispositivos)”**, en la cual se desplegarán varias opciones
2. Seleccionar la opción de **“Directivas y perfiles”**, dentro de esta opción se muestran los aplicativos del antivirus a los cuales se pueden realizar diversas configuraciones y la parte más importante es aplicar las políticas de restricción.
3. Dar doble clic en el aplicativo **“Kaspersky Endpoint Security para Windows EQF 2024”**, al cual se va a realizar la configuración.

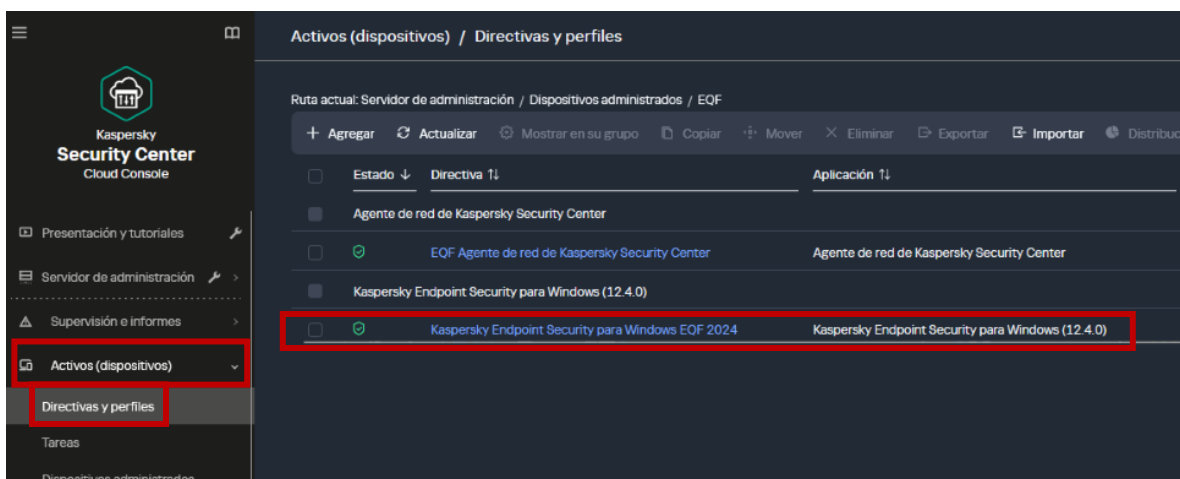


Figura 99 Directivas y perfiles

Un aspecto importante a mencionar es que el estado de la directiva debe de estar **“Activa”** para que pueda funcionar correctamente en la protección de los dispositivos.

4. Dar clic en la opción **“Configuración de la aplicación”**, que se encuentra en el menú de la parte superior.

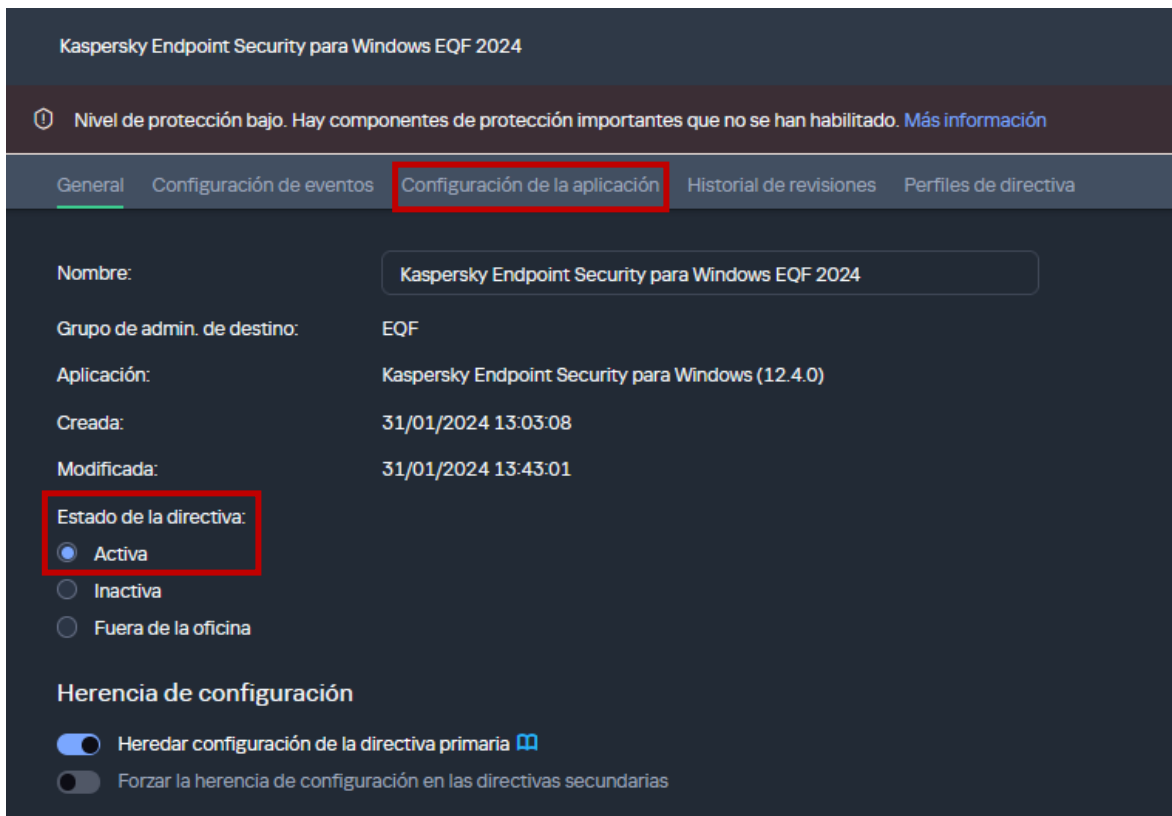


Figura 100 Configuración general del aplicativo.

5. Seleccionar “Controles de seguridad”.

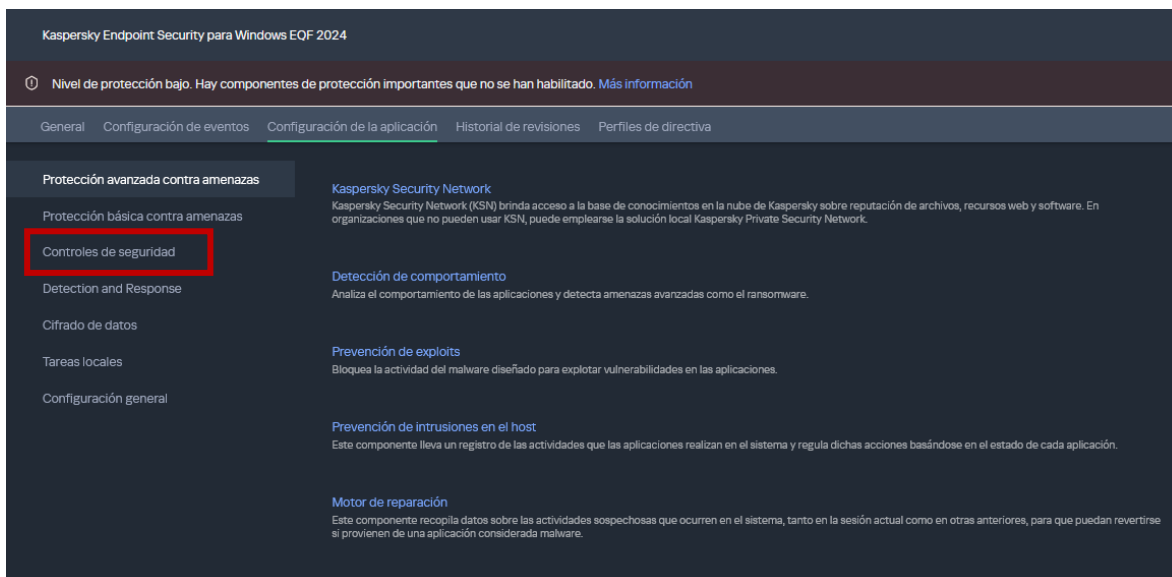


Figura 101 Configuración de la aplicación.

6. Dar clic en “Control web”, para comenzar con la configuración de las políticas de sitios web.

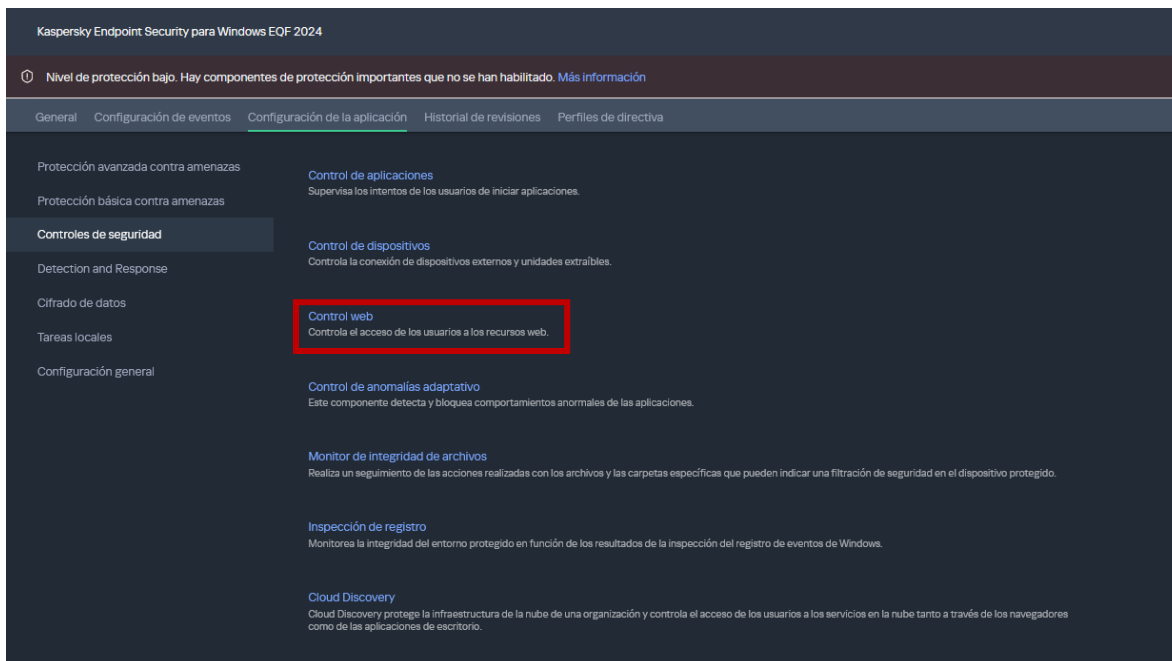


Figura 102 Opciones de controles de seguridad.

7. Habilitar la opción de control web, para que las políticas de restricción estén en funcionamiento.



Figura 103 Habilitar control web.

En seguida, se muestran las reglas que se han configurado, además de un menú el cual permite configurar las nuevas reglas de restricción, eliminarlas, moverlas de su nivel de prioridad, importarlas o exportarlas.

8. Al no tener ninguna regla, se tendrá que dar clic en la opción “**Agregar**” para crear estas nuevas reglas de restricción.

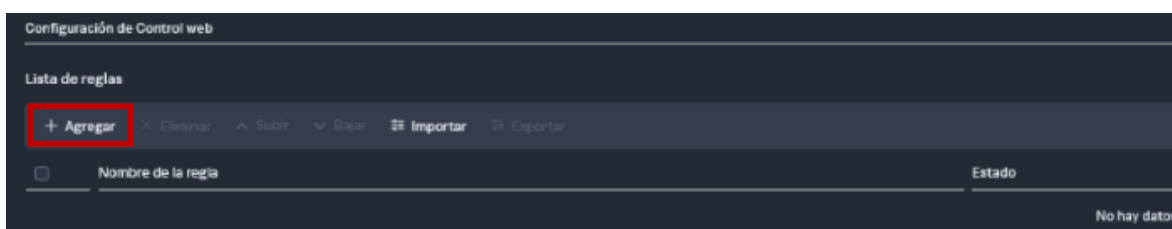


Figura 104 Lista de reglas.

9. Poner un nombre a la nueva regla, este nombre puede ser el que la empresa decida asignar,
10. En el apartado de **“Estado”**, seleccionar la opción **“Habilitada”**, esto para indicar que la regla estará activa o en funcionamiento.
11. Después se pueden realizar tres diferentes opciones para los sitios web que no sean permitidos, las cuales constan de **“Permitir”**, **“Bloquear”** o **“Advertir”**, estas se configuraran de acuerdo a las necesidades de la empresa.
12. En el apartado de **“Direcciones”**, ingresar todos los enlaces de sitios web que no sean permitidos estos pueden ser uno o varios dentro de la misma regla
13. Habilitar la opción **“Aplicar para todos los usuarios”**, esto aplicara la regla a todos los usuarios en general.

The screenshot shows a web-based configuration form titled 'Regla'. It contains several sections with radio button options:

- Nombre de la regla:** A text input field.
- Estado:** Radio buttons for 'Habilitada' (selected) and 'Deshabilitada'.
- Acción:** Radio buttons for 'Permitir' (selected), 'Bloquear', and 'Advertir'.
- Contenido de filtro:** Radio buttons for 'Por categorías de contenido' and 'Por tipos de datos'.
- Categorías de contenido:** A text input field.
- Tipos de datos:** A text input field.
- Direcciones:** Radio buttons for 'Aplicar a todas las direcciones' (selected) and 'Aplicar a direcciones o grupos individuales'.
- Usuarios:** Radio buttons for 'Aplicar a todos los usuarios' (selected) and 'Aplicar a usuarios o grupos individuales'.

At the bottom, there are sections for adding and removing items, and a 'Comentario' field.

Figura 105 Creación y configuración de la nueva regla.

14. Dar clic en la opción **“Mensaje para bloqueo”**, para poder personalizar el mensaje que aparecerá al usuario cuando ingrese a los sitios web que han sido bloqueados. (Opcional)

15. Dar clic en crear.

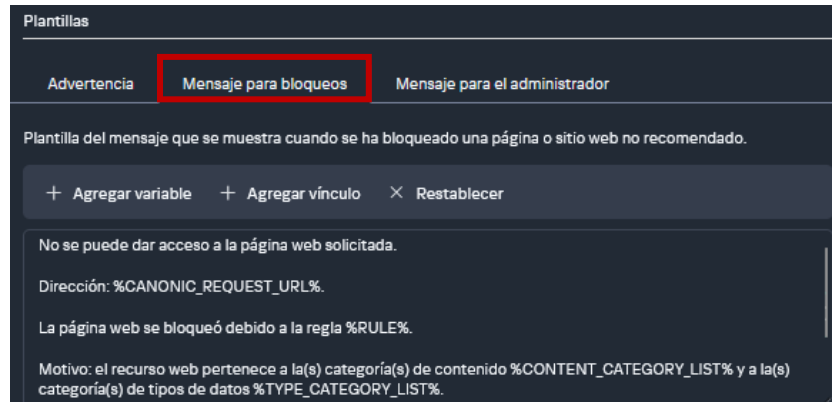


Figura 106 Personalización de mensaje de bloqueo.

Políticas de restricción de acceso a aplicativos

En este apartado se va a realizar la configuración para el control de aplicaciones.

1. Ingresar a la opción de **“Activos (dispositivos)”**, en la cual se desplegarán varias opciones
2. Seleccionar la opción de **“Directivas y perfiles”**, dentro de esta opción se muestran los aplicativos del antivirus a los cuales se pueden realizar diversas configuraciones y la parte más importante es aplicar las políticas de restricción.
3. Dar doble clic en el aplicativo **“Kaspersky Endpoint Security para Windows EQF 2024”**, al cual se va a realizar la configuración.

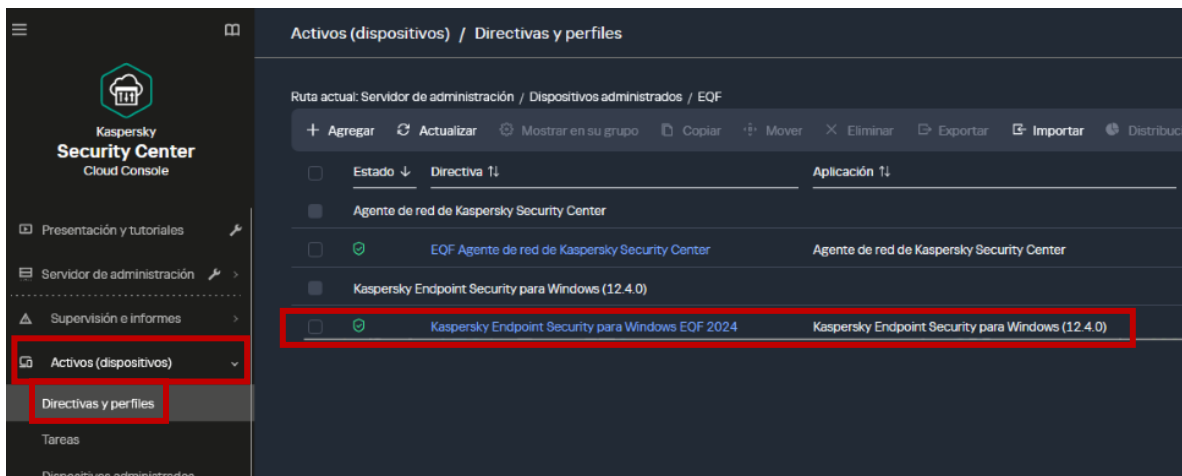


Figura 107 Directivas y perfiles

Un aspecto importante a mencionar es que el estado de la directiva debe de estar “Activa” para que pueda funcionar correctamente en la protección de los dispositivos.

4. Dar clic en la opción “**Configuración de la aplicación**”, que se encuentra en el menú de la parte superior.

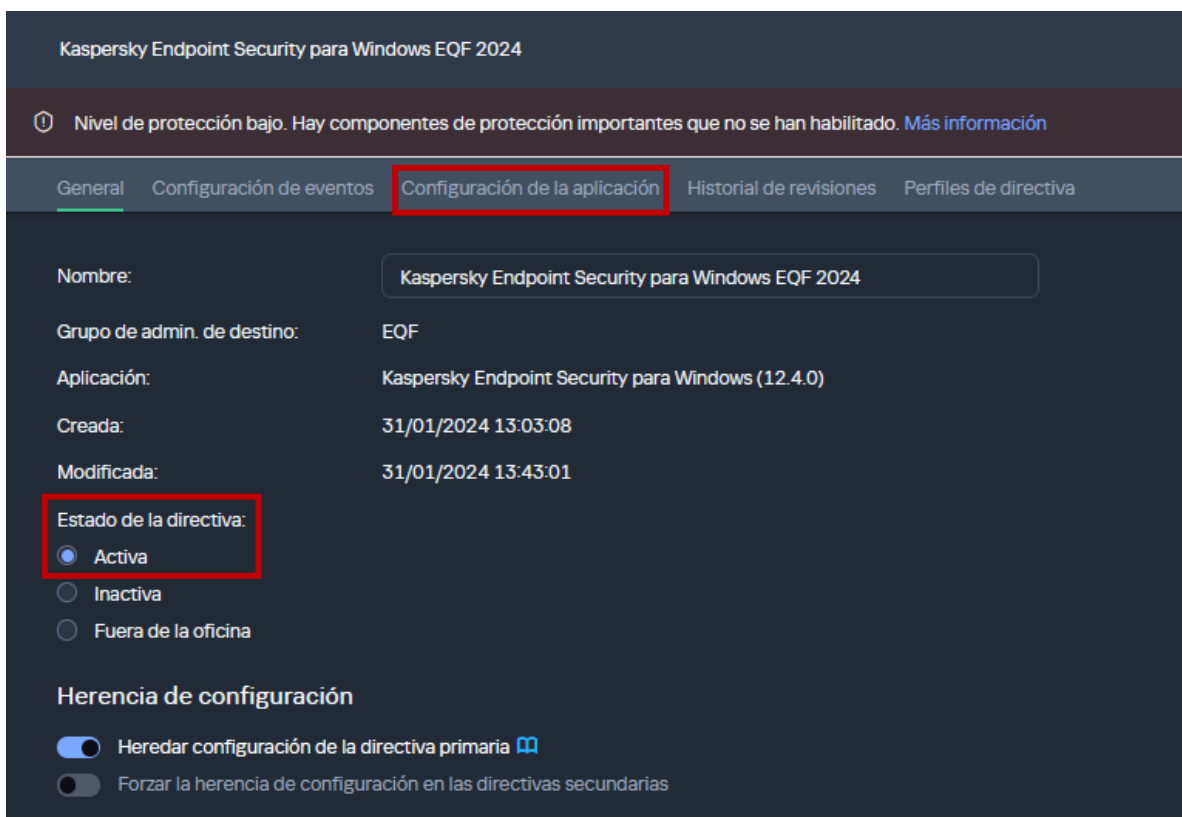


Figura 108 Configuración general del aplicativo.

5. Seleccionar “**Controles de seguridad**”.

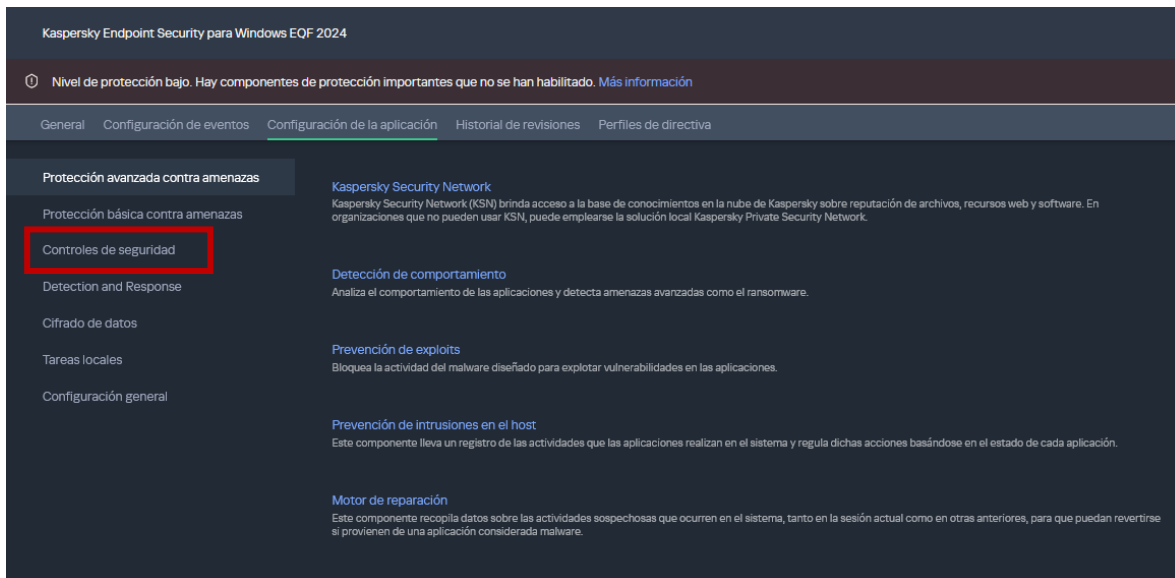


Figura 109 Configuración de la aplicación.

6. Dar clic en “**Control de aplicaciones**”, para comenzar con la configuración de las políticas de sitios web.

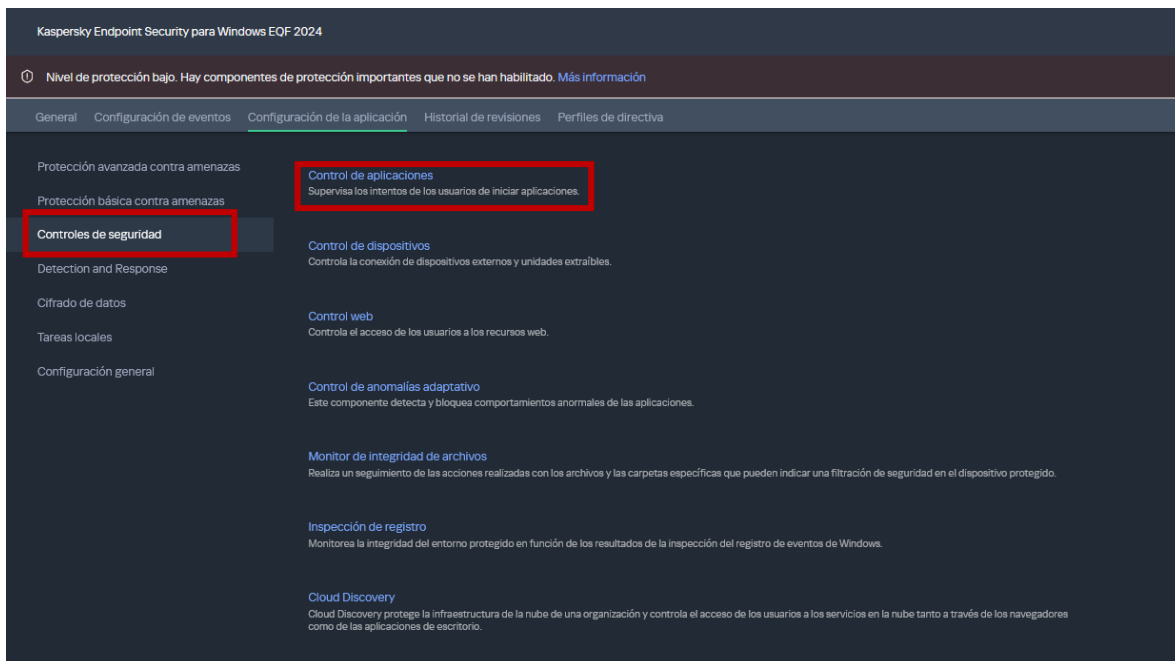


Figura 110 Control de aplicaciones.

7. Habilitar la opción de control de aplicaciones, para que las políticas de restricción estén en funcionamiento.

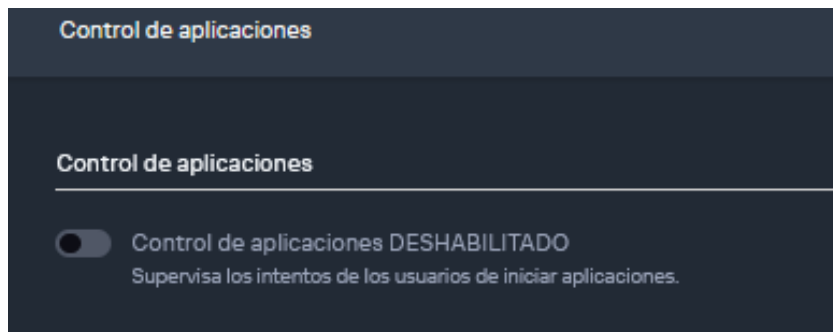


Figura 111 Habilitar control de aplicaciones.

8. Seleccionar la opción de **“Informar”**, la cual manda un aviso de que se está ingresando a una aplicación a la cual está prohibido dicho acceso.
9. Seleccionar la opción de **“Lista de rechazados”**, la cual permite al usuario ingresar a cualquier aplicación a excepción de las que estén agregadas en la regla de bloqueo.
10. Dejar por defecto la configuración avanzada.

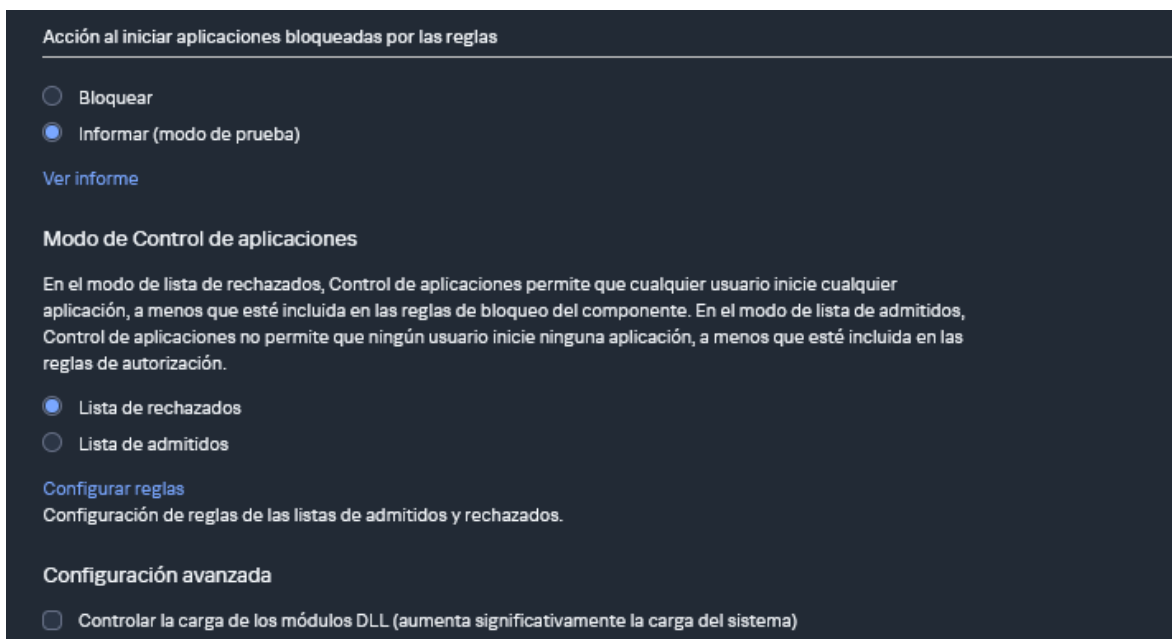


Figura 112 Configuración de regla de bloqueo de aplicaciones.

11. Dar clic en la opción **“Mensaje para bloqueo”**, para poder personalizar el mensaje que aparecerá al usuario cuando ingrese a los aplicativos que han sido bloqueados. (Opcional)

12. Dar clic en crear.

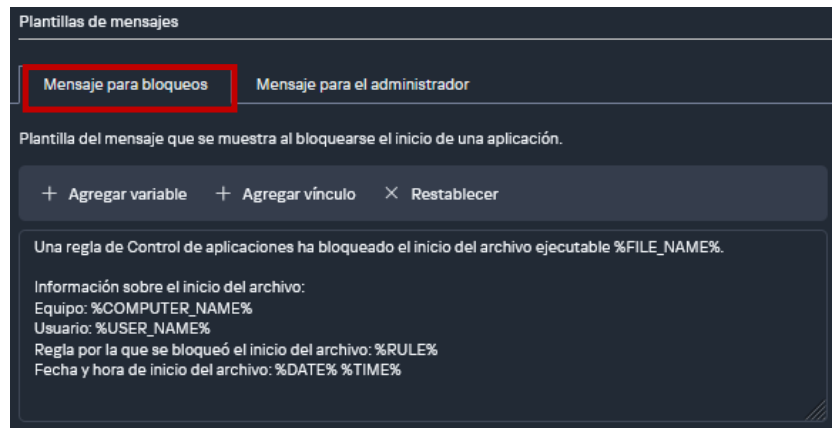


Figura 113 Personalización de mensaje de bloqueo a aplicativos.

Políticas de restricción de acceso a dispositivos

En esta sección se va a abordar la configuración para el control de dispositivos

1. Ingresar a la opción de **“Activos (dispositivos)”**, en la cual se desplegarán varias opciones
2. Seleccionar la opción de **“Directivas y perfiles”**, dentro de esta opción se muestran los aplicativos del antivirus a los cuales se pueden realizar diversas configuraciones y la parte más importante es aplicar las políticas de restricción.
3. Dar doble clic en el aplicativo **“Kaspersky Endpoint Security para Windows EQF 2024”**, al cual se va a realizar la configuración.



Figura 114 Directivas y perfiles

Un aspecto importante a mencionar es que el estado de la directiva debe de estar “Activa” para que pueda funcionar correctamente en la protección de los dispositivos.

4. Dar clic en la opción “**Configuración de la aplicación**”, que se encuentra en el menú de la parte superior.

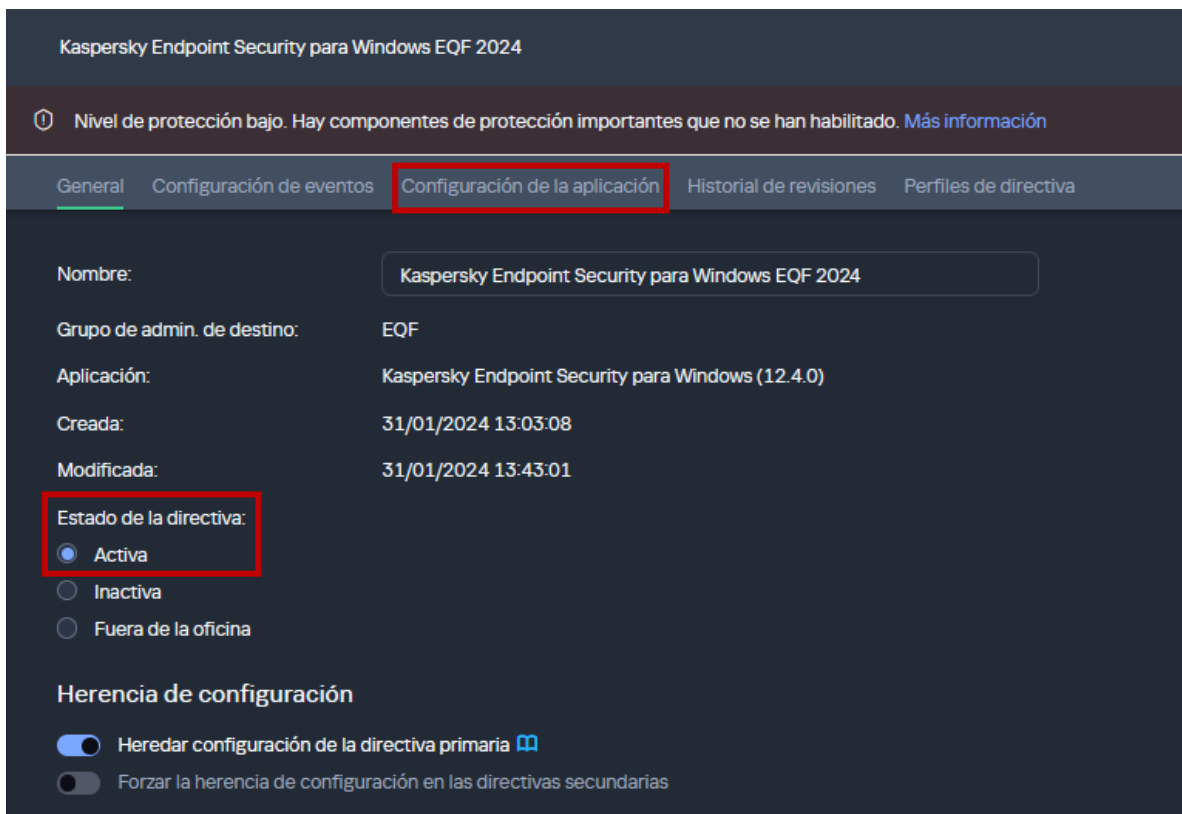


Figura 115 Configuración general del aplicativo.

5. Seleccionar “Controles de seguridad”.

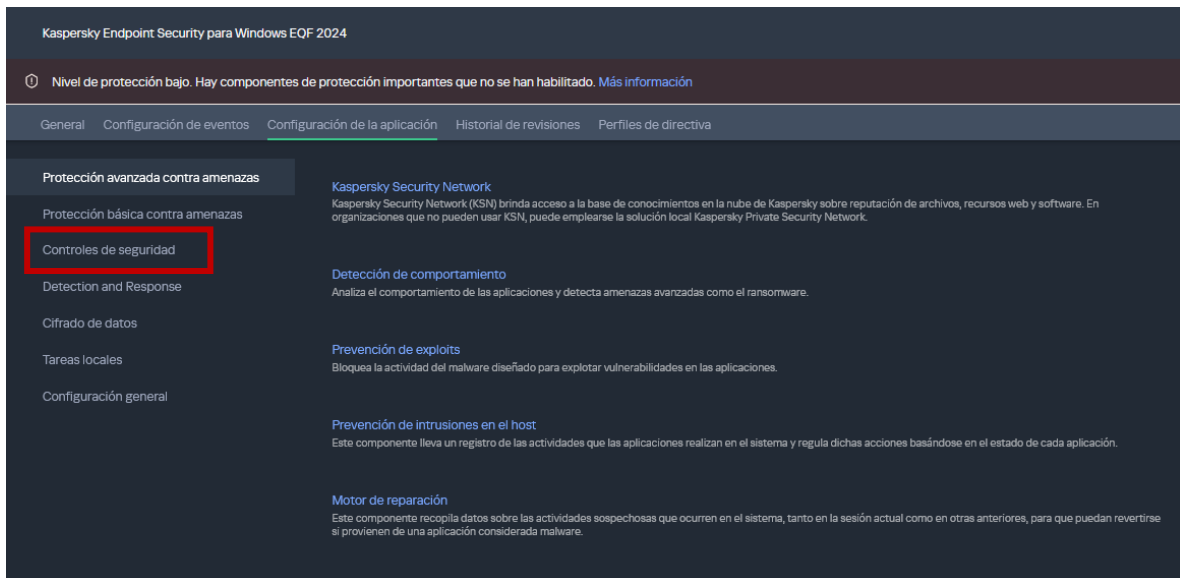


Figura 116 Configuración de la aplicación.

6. Dar clic en “Control de dispositivos”, para comenzar con la configuración de las políticas de sitios web.

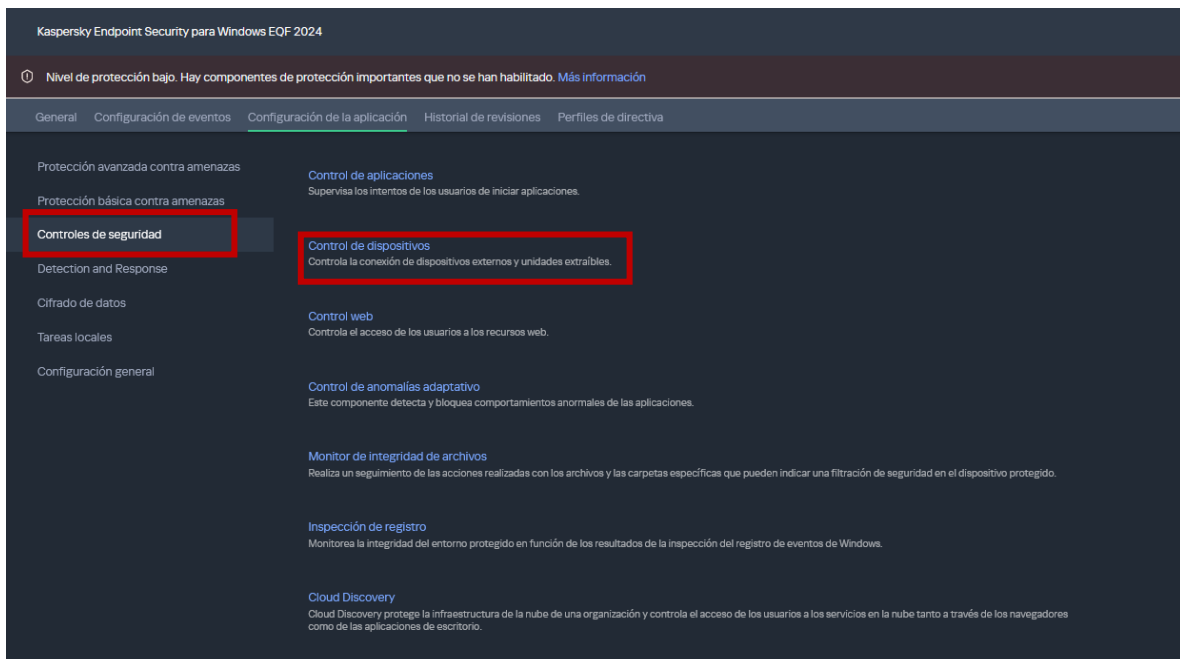


Figura 117 Control de aplicaciones.

7. Habilitar la opción de control de dispositivos, para que las políticas de restricción estén en funcionamiento.

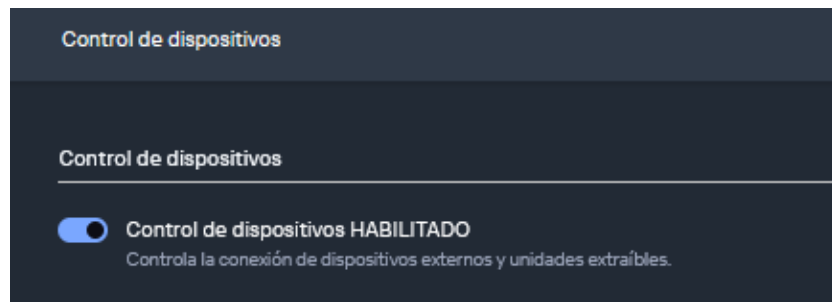


Figura 118 Habilitar control de dispositivos.

8. Habilitar la casilla de **“Permitir solicitudes de acceso temporal”**.
9. Dejar tal cual viene la configuración predeterminada, cabe recalcar que al tener la configuración predeterminada se puede tener un buen control de todos los dispositivos y realizar diversas acciones para aquellos equipos que se encuentren infectados.

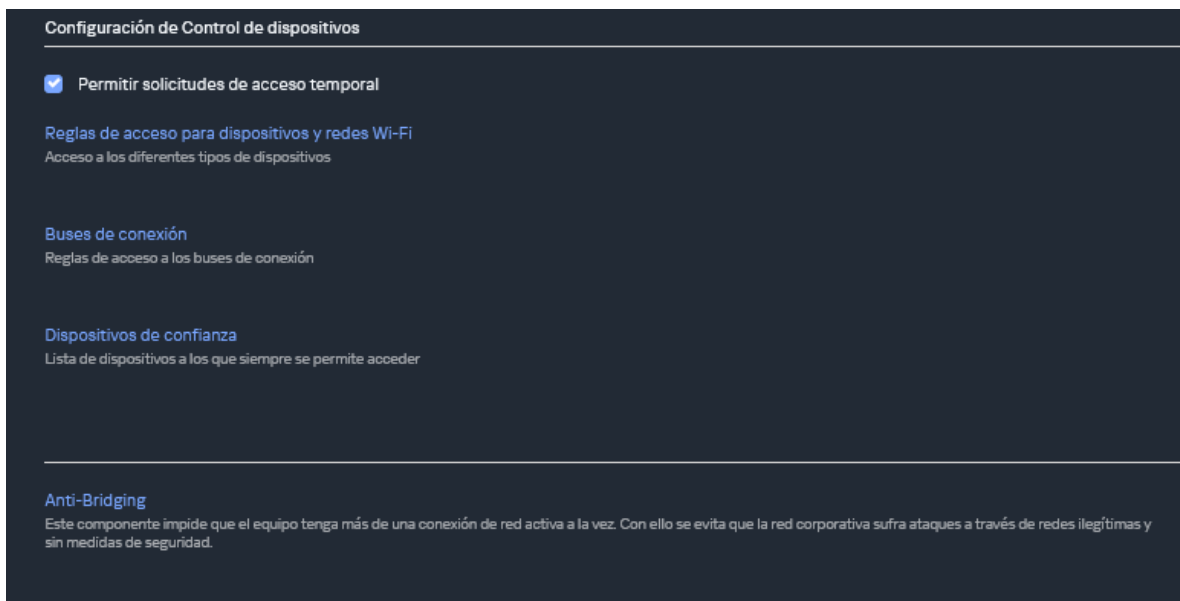


Figura 119 Configuración de control de dispositivos.

10. Dar clic en la opción **“Mensaje para bloqueo”**, para poder personalizar el mensaje que aparecerá al usuario cuando ingrese a un dispositivo que se encuentre bloqueado.
(Opcional)
11. Dar clic en crear.

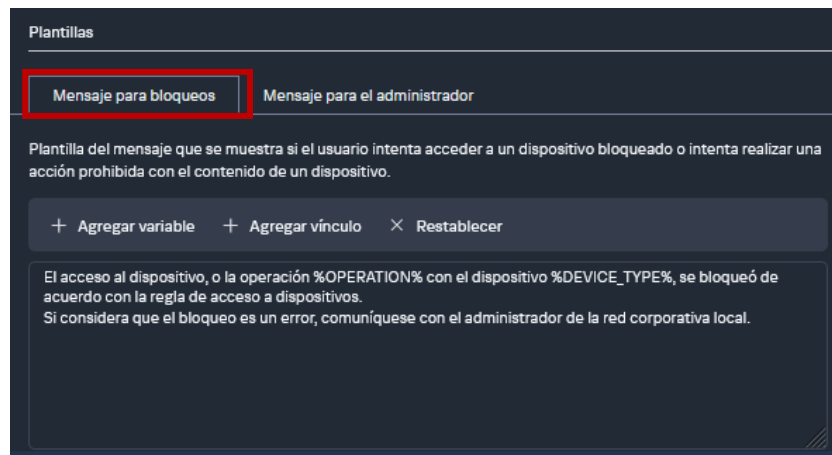


Figura 120 Personalización de mensaje de bloqueo para los dispositivos.

Interfaz

Configuración de interfaz para el usuario

En esta parte, se muestra la configuración de la interfaz del agente de antivirus para los usuarios, esto con la finalidad de tener un mayor control del antivirus y que los usuarios no hagan mal uso de esta medida de seguridad.

1. Habilitar la opción de **“Con la interfaz simplificada”**. La cual permite al usuario solamente mostrar información referente al antivirus que se tiene instalado en el equipo.

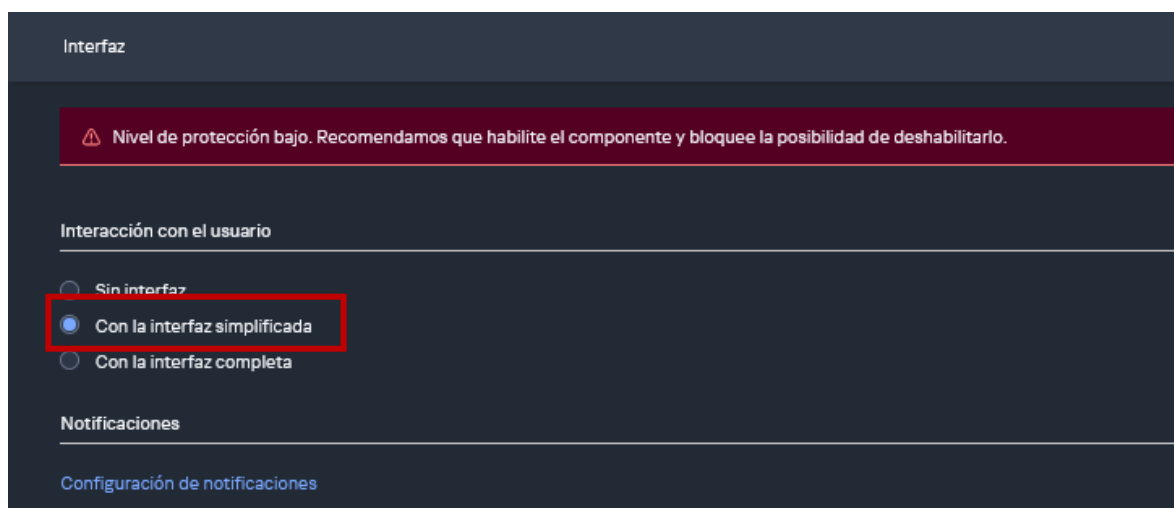


Figura 121 Configuración de interfaz.

A continuación, se muestra la interfaz simplificada que puede observar el usuario al ingresar al aplicativo del antivirus, como se puede observar solamente se muestra la información que corresponde al tipo de licencia de protección que se tiene instalada en el equipo, la clave de licencia que le corresponde, la versión del aplicativo, el nombre del servidor el cual administra el antivirus, la fecha de la última sincronización, además de enlaces los cuales llevan a la documentación oficial acerca del antivirus que se tiene instalado.



Figura 122 Interfaz simplificada del antivirus para el usuario.