Diseño de una propuesta de gestión para la instalación de actualizaciones de software utilitario y/o componentes de Windows en equipos de cómputo de usuario final en ECOPETROL

Avila Antonio Diego Ernesto, Lozano Álvarez Michael David, Cundumi Carvajal Brayan Alexander, Gachancipa Gutierrez Andres Felipe y Walteros Lopez Jeison Joann

Especialización en Seguridad Informática, Fundación Universitaria Compensar

Propuesta de Consultoría

María Fernanda Montero Molina

13 de noviembre de 2024

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional

Diseño de una propuesta de gestión para la instalación de actualizaciones de software utilitario y/o componentes de Windows en equipos de cómputo de usuario final en ECOPETROL

Jeison Joann Walteros Lopez
Diego Ernesto Avila Antonio
Michael David Lozano Álvarez
Brayan Alexander Cundumi Carvajal
Andres Felipe Gachancipa Gutierrez

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista en Seguridad Informática

Director (a):

Ingeniera, María Fernanda Montero Molina

Línea de Investigación:

Consultoría Seminario Grado

Grupo de Investigación:

Especialización en Seguridad Informática

Fundación Universitaria Compensar

Facultad de Ingeniería, Especialización en Seguridad Informática

Bogotá, Colombia

2024

Resumen

El proyecto tiene como objetivo diseñar una propuesta de implementación del proceso de gestión para la instalación de actualizaciones de software utilitario y componentes de Windows en los equipos de cómputo de usuario final en ECOPETROL. La necesidad surge a raíz de la identificación de una vulnerabilidad crítica en la versión 2.50 del software KeePass Pro, que compromete la seguridad del sistema operativo mediante la elevación de privilegios a nivel del kernel de Windows.

Esta vulnerabilidad afecta a los sistemas que no han sido actualizados a la versión 2.57 del software. Adicional, se evidencia que una cantidad significativa de equipos no han recibido los parches de seguridad correspondientes a varios componentes de Windows distintos al software KeePass Pro lo que expone a la organización a riesgos considerables en términos de seguridad y operatividad.

El proyecto propone un enfoque sistemático para garantizar la instalación oportuna de actualizaciones de software, mitigando riesgos y mejorando la seguridad operativa de usuario final en la infraestructura tecnológica de ECOPETROL.

Palabras clave:

Kernel, Software, Vulnerabilidad, Riesgos, Seguridad

Abstract

The project aims to design an implementation proposal for the management process of installing utility software updates and Windows components on end-user computers at ECOPETROL. The need arises from identifying a critical vulnerability in version 2.50 of the KeePass Pro software, which compromises the operating system's security by elevating privileges at the Windows kernel level.

This vulnerability affects systems that have not been updated to version 2.57 of the software. Additionally, a significant number of computers have not received the necessary security patches for various Windows components other than KeePass Pro, exposing the organization to considerable risks in terms of security and operability.

The project proposes a systematic approach to ensure the timely installation of software updates, mitigating risks, and improving the operational security of end-user systems within ECOPETROL's technological infrastructure.

Keywords:

- **Kernel, Software, Vulnerability, Risks, Security**

Contenido

RESUMEN ..... **V**

INTRODUCCIÓN **2**

ANTECEDENTES Y JUSTIFICACIÓN 3

Antecedentes: *3*

Justificación: *4*

FORMULACIÓN DEL PROBLEMA 4

Pregunta de Investigación: *4*

OBJETIVO GENERAL 5

Objetivos Específicos *5*

ALCANCES Y LIMITACIONES 5

Alcance: *5*

Limitaciones: *5*

1. MARCO TEÓRICO **7**

2. DISEÑO METODOLÓGICO **10**

2.1 FASE 1: DIAGNOSTICO 11

2.1.1 Inventario *11*

2.1.2 Informe Escaneo De Vulnerabilidades *12*

2.2 FASE 2: PLANIFICACIÓN 12

2.2.1 Análisis de impacto en la organización *12*

2.2.2 Validación de estándares y marcos normativos de seguridad *13*

2.3 FASE 3: DESARROLLO 15

2.3.1 Desarrollo de la propuesta *15*

2.3.2 Desarrollo de propuesta de cronograma de despliegue de actualizaciones. *16*

3. RESULTADOS ESPERADOS **16**

3.1 CONCLUSIONES 18

3.2 RECOMENDACIONES 19

BIBLIOGRAFÍA **21**

ANEXOS **23**

Introducción

Hoy la seguridad informática es prioridad para las Empresa, la gestión de actualizaciones de software es esencial para mitigar riesgos y garantizar la seguridad en los sistemas. ECOPETROL, como empresa líder en el sector energético, depende de una infraestructura tecnológica robusta que se debe mantenerse actualizada para protegerse contra amenazas emergentes.

De acuerdo con la investigación del equipo de Inteligencia de CrowdStrike donde identificó que el mayor número de operaciones de extorsión de datos por ransomware durante este año se presentó en el sector industrial y de ingeniería (229 incidentes), seguido de cerca por el sector manufacturero (228 incidentes). Una alteración en las operaciones diarias afecta el núcleo del negocio de las empresas donde no logran satisfacer las demandas de producción como consecuencia de interrupciones en el sistema.

En la Figura 1 se evidencia la cantidad de ataques o incidentes de ransomware que afectaron a la industria durante el año 2022, con un mayor impacto en el sector industrial y de ingeniería, al cual pertenece la compañía Ecopetrol.

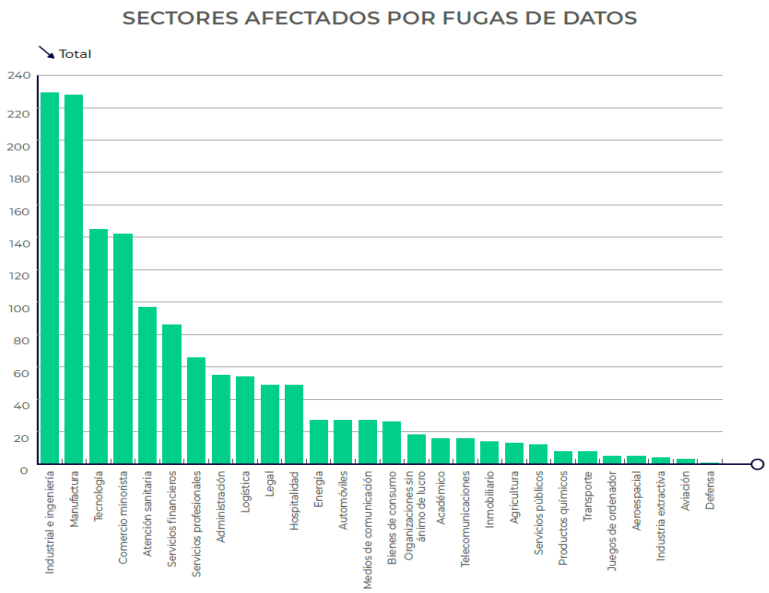


Figura 1. Sectores afectados por fugas de datos. (Buatista Garcia, 2022)

Este proyecto se enfoca en el diseño de una propuesta para la implementación de un proceso de gestión destinado a la instalación de actualizaciones de software utilitario y componentes de Windows en los equipos de cómputo de usuarios finales. La motivación principal del proyecto surge a partir de la identificación de una vulnerabilidad crítica en la

versión 2.50 del software KeePass Pro, un gestor de contraseñas que ayuda a almacenarlas de forma segura sin necesidad de memorizarlas. Esta herramienta compromete la seguridad del sistema operativo mediante la elevación de privilegios al nivel del kernel de Windows. Dicha vulnerabilidad, documentada en el Catálogo de Vulnerabilidades Explotadas Conocidas (CVE) de la CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos), representa un rieSgo significativo para la integridad y confidencialidad de la información manejada por los usuarios finales.

Adicionalmente, se ha evidenciado que en numerosos equipos dentro de la organización no se ha realizado la instalación de los parches de seguridad correspondientes a varios componentes de Windows, lo que incrementa la exposición a posibles ataques cibernéticos. La ausencia de un proceso estructurado para la gestión de estas actualizaciones ha dejado la infraestructura tecnológica de Ecopetrol vulnerable a brechas de seguridad.

Antecedentes y Justificación

Antecedentes:

Recientemente, el departamento de ciberseguridad de la organización identificó un incidente crítico relacionado con una vulnerabilidad en la aplicación KeePass versión 2.50, que afecta al kernel de Windows. Este problema, está en el Catálogo de Vulnerabilidades Explotadas Conocidas (CVE) de la CISA, la cual un posible atacante puede explotar y realizar una elevación de privilegios a nivel del sistema, así generando un potencial riesgo a la seguridad del sistema operativo y el acceso a información confidencial.

En respuesta a esta situación, se solicitó un análisis en algunos de los equipos del parque, descubriendo que numerosos equipos están expuestos a riesgos por no actualizar regularmente su software y los componentes de Windows. Este análisis también reveló la falta de un procedimiento estandarizado para la instalación de actualizaciones en los dispositivos de nuestros usuarios, así como la ausencia de un responsable dedicado a la gestión preventiva de estas actualizaciones, lo que eleva considerablemente nuestra vulnerabilidad en un entorno de aproximadamente 9,584 endpoints.

Justificación:

La falta de un procedimiento estandarizado para la gestión de actualizaciones y la carencia de un procedimiento donde indique quién tiene a cargo su ejecución preventiva ponen en riesgo la integridad y seguridad del entorno informático de la organización.

La identificación de vulnerabilidades críticas, como la de KeePass, expone a la organización a ataques que pueden comprometer tanto los sistemas operativos como los datos confidenciales almacenados en ellos. Dado que el parque de equipos abarca un aproximado de 9,584 endpoints, es fundamental establecer un proceso estructurado que asegure la actualización constante de software y componentes del sistema operativo. Esto no solo mitiga posibles ataques, sino que garantiza la continuidad operativa y refuerza la confianza en la infraestructura de TI. La implementación de un procedimiento sólido permitirá a la organización prevenir incidentes de seguridad, optimizar recursos y reducir significativamente el riesgo de exposición ante nuevas amenazas.

Formulación del Problema

La organización se encuentra en una situación de riesgo considerable debido a la falta de un proceso estructurado para actualizar el software en los equipos informáticos. Después del incidente reciente relacionado con la vulnerabilidad crítica encontrada en la aplicación KeePass, se ha evidenciado que muchos equipos no cuentan con las actualizaciones necesarias para protegerse contra ataques cibernéticos.

La ausencia de un departamento dedicado a la gestión preventiva de estas actualizaciones agrava esta situación, poniendo en riesgo la seguridad de más de 9,584 equipos pertenecientes a la organización. Además de poner en riesgo la seguridad de la información y la integridad de los sistemas, también se pone en peligro la continuidad operativa de la empresa debido a una falta de procedimiento estandarizado.

Pregunta de Investigación:

¿Cómo puede la falta de un procedimiento estandarizado y la ausencia de un área responsable para la instalación preventiva de actualizaciones de software utilitario y componentes de Windows en los equipos de cómputo de los usuarios finales influir en

la exposición a vulnerabilidades críticas, como la detectada en la aplicación KeePass versión 2?50, en una organización con un parque de 9,584 endpoints?

Objetivo General

Diseñar una propuesta para la creación del proceso de gestión en la instalación de actualizaciones para software utilitarios y/o componentes de Windows en equipos de cómputo de usuarios finales en ECOPETROL.

Objetivos Específicos

- Realizar un diagnóstico del estado actual de los equipos de usuarios finales en la compañía
- Elaborar propuesta de un procedimiento estandarizado para la instalación de actualizaciones para software utilitarios y/o componentes de Windows en equipos de cómputo de uso por usuarios finales en ECOPETROL
- Desarrollar una propuesta de cronograma para las actualizaciones para software utilitarios y/o componentes de Windows en equipos de cómputo de uso por usuarios finales en ECOPETROL

Alcances y Limitaciones

Alcance:

La propuesta se enfocará en el diseño de un proceso de gestión para la instalación de actualizaciones en software utilitario y/o componentes de Windows en equipos de cómputo de uso por usuarios finales dentro de ECOPETROL. Esto incluye la creación de un procedimiento estandarizado que describa detalladamente los pasos a seguir, las herramientas a utilizar, los roles y responsabilidades del proceso de actualización. En el cual se desarrollará un cronograma de actualizaciones que especifique la frecuencia y el tipo de actualizaciones necesarias, alineándose con las políticas de seguridad de la compañía.

Limitaciones:

Esta propuesta se limitará al desarrollo de un proceso de gestión para actualizaciones en el contexto de los equipos de cómputo utilizados por los usuarios finales de

ECOPETROL, sin abordar otros sistemas o infraestructuras de la compañía. Asimismo, el éxito de la implementación dependerá de la disponibilidad de tiempo, recursos financieros, humanos y materiales asignados al proyecto.

Además, factores como el cambio de prioridades dentro de la organización, la resistencia al cambio por parte del personal, y la dependencia de terceros para la actualización de ciertos componentes podrían afectar la efectividad del proceso. Por último, la entrega del proyecto y el cumplimiento de las especificaciones estarán sujetos a la viabilidad técnica y operacional.

1. Marco teórico

En la actualidad de globalización y progreso tecnológico, las organizaciones, como ECOPETROL, están expuestas a un mayor riesgo en ciberseguridad debido a la rápida evolución de la vulnerabilidad y las tácticas del cibercrimen. Por esta razón, una gestión adecuada de las actualizaciones de software es crítica para la protección de los sistemas de información, especialmente en una organización a gran escala donde la seguridad de los datos es de vital importancia. (OEA, 2019) Para ello, es esencial adherirse a marcos normativos, estándares internacionales y procedimientos que regulen la ciberseguridad. Un ejemplo clave es la norma ISO/IEC 27001:2022, que establece controles para garantizar la integridad, confidencialidad y disponibilidad de la información. En particular, el Anexo A de la norma aborda el control relacionado con la "Instalación de software en sistemas operativos" (A.8.19) y la "Gestión de vulnerabilidades técnicas" (A.8.8), los cuales son fundamentales para mitigar los riesgos derivados de software desactualizado. además, el control A.8.1 resalta la importancia de proteger los dispositivos finales de usuario, como computadoras y teléfonos móviles, que a menudo son puntos vulnerables de acceso a los datos. Así, la gestión de actualizaciones no solo se refiere a la aplicación de parches de seguridad, sino también a una cultura organizacional que garantice que todos los empleados comprendan la importancia de mantener los sistemas actualizados y seguros frente a las amenazas cibernéticas, siguiendo las mejores prácticas internacionales para reducir los riesgos en un entorno digital cada vez más complejo. (ISO/IEC, 2022)

Las actualizaciones de software y de componentes deben ser tratadas de manera primordial y es fundamentes que sean Implementadas lo antes posible, es importante monitorear y verificar las actualizaciones. Al hacerlo, una organización puede incrementar su postura de seguridad. La NIST sugiere que "el monitoreo y la verificación de actualizaciones son procesos críticos para asegurar que los sistemas se mantengan protegidos contra vulnerabilidades, verificando que las actualizaciones se apliquen correctamente y evaluando su impacto en la seguridad del sistema". (NIST-National Institute of Standards and Technology, 2007) Implementar un proceso eficiente de actualización de software y componentes de Windows en una empresa que enfrenta dificultades para adoptar buenas prácticas puede resultar en procesos lentos y poco productivos. Por eso, es crucial incorporar marcos de referencia que guíen la gestión de estos procesos, como ITIL V4, que ofrece directrices clave para optimizar la eficiencia. ITIL V4 destaca que la gestión de cambios es el proceso que controla el ciclo de vida de todos los cambios, facilitando sus beneficios y minimizando el riesgo de interrupciones en los servicios. (Axelos, 2022) Seguir este marco ayuda a asegurar que las actualizaciones se realicen de manera ordenada y con el mínimo impacto en la operación de la empresa, mejorando tanto la productividad como la estabilidad del entorno tecnológico.

Dentro del panorama de normas y estándares consultados se concluye que las mencionadas anteriormente son sin duda primordiales, así mismo dentro de la industria existen procedimientos o recomendaciones que se deben tener en cuenta. ECOPETROL al poseer toda su flota de equipos computo bajo el sistema operativo Windows es primordial considerar las guías para la implementación y actualización que expide el fabricante en las cuales hay un común denominador que nos indica que el monitoreo de las actualizaciones y la verificación de su correcta aplicación son esenciales para asegurar que los sistemas reciban los parches necesarios y para mantener la integridad del entorno de TI. (Microsoft Learn - Deploy and Update Windows, 2024)

Las recomendaciones de Microsoft son esenciales para el éxito de la eficiencia de todos los softwares utilitarios que se ejecutan bajo los sistemas operativos de

Windows, siguiendo estas mejores prácticas tenemos la base para diseñar una guía en la cual se busca garantizar que las actualizaciones se apliquen de forma sistemática y eficaz. Sin embargo, los controles CIS sugieren que "una política de actualizaciones debe incluir procedimientos para la evaluación y aplicación de actualizaciones de seguridad, asegurando que se realicen de manera sistemática y conforme a los riesgos y necesidades de la organización" (Center For Internet Secury, 2023)

Los eventos cibernéticos han demostrado la importancia de las actualizaciones, el mantener software utilitario desactualizado es crítico para ECOPETROL y cualquier compañía dado que se exponen a brechas para posibles ataques cibernéticos. Algunos de los ataques más conocidos en la historia de ataques cibernéticos es la del famoso Ransomware WannaCry que se propagó rápidamente a nivel mundial en mayo de 2017. El ataque aprovechó una vulnerabilidad en Microsoft Windows conocida como Eternal Blue. Aunque Microsoft había lanzado un parche para corregir la vulnerabilidad en marzo de 2017, muchas organizaciones no habían actualizado sus sistemas antes del ataque. (IBM, 2024)

Ser víctima de perdida de información e incluso divulgación e información de las compañías como resultado de un ataque cibernético en muchos países puede implicar consecuencias legales. En Colombia no es la excepción y la ley está preparada para este tipo de situaciones. De acuerdo con la Resolución Número 00500 de marzo 10 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones “MinTIC”, en el Artículo 17 se establecen las etapas generales de la gestión de incidentes de seguridad digital. Donde se especifica la necesidad de prevenir, proteger, detectar responder y comunicar de manera continua sobre los posibles incidentes la plataforma tecnológica e infraestructura crítica para así identificar y predecir comportamientos inusuales que puedan evidenciar ataques contra la entidad. (“MinTic,” 2021)

2. Diseño Metodológico

Ecopetrol en sus procesos de mejora continua aplica metodologías que permitan tener un ciclo basado en Planificar-Hacer-Verificar-Actuar (PHVA) el cual oriente la solución de problemas, en este caso la organización se enfrenta a un desafío de ciberseguridad originado por una falla descubierta recientemente en una aplicación. Dicha vulnerabilidad podría afectar potencialmente a 9,584 estaciones de trabajo dentro del parque tecnológico de la compañía.

Por lo cual la investigación se identifica como un modelo exploratorio teniendo en cuenta que en la organización no se tienen antecedentes o se ha estudiado poco la problemática que se tiene hoy en día la cual fue descubierta por el incidente ocurrido en el mes de julio de 2024. En la Figura 2 se presenta las fases del proyecto.



Figura 2 Fases del proyecto

2.1 Fase 1: Diagnostico

2.1.1 Inventario

A la fecha del 25 de septiembre de 2024, el parque tecnológico de Ecopetrol se compone de un total de 9,584 equipos de cómputo, de los cuales 9,537 están en asignación “En el Parque” y 47 se encuentran en asignación como “respaldo”. Esta infraestructura tecnológica está estratégicamente dividida en cinco zonas operativas: Zona Central, Zona Santanderes, Zona Llanos, Zona Caribe y Zona Sur. Distribución y estado de los equipos, se puede consultar el **¡Error! No se encuentra el origen de la referencia.**

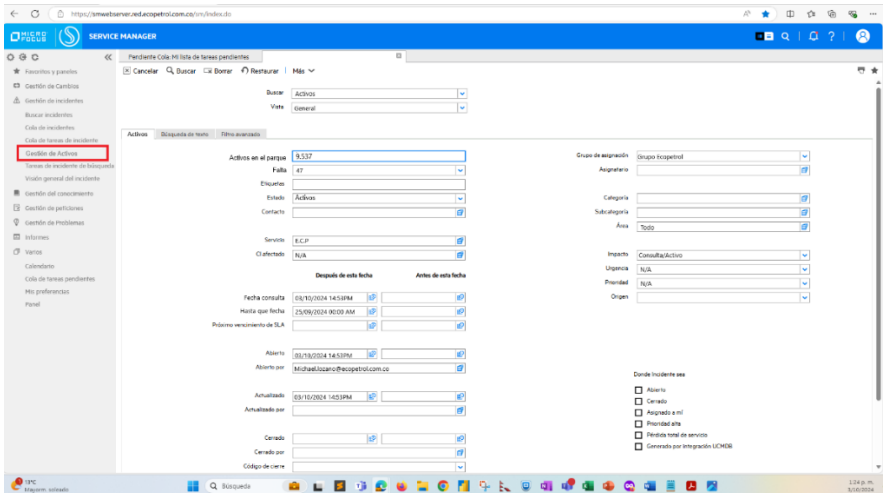


Figura 3 Asset Manager - gestión de activos
Herramienta IT para la gestión y control de activos

En la Figura 3 Asset Manager - gestión de activos Se llevó a cabo un análisis de vulnerabilidades de una muestra de 2000 equipos. Este análisis reveló el siguiente escenario: ver Anexo 2

2.1.2 Informe Escaneo De Vulnerabilidades

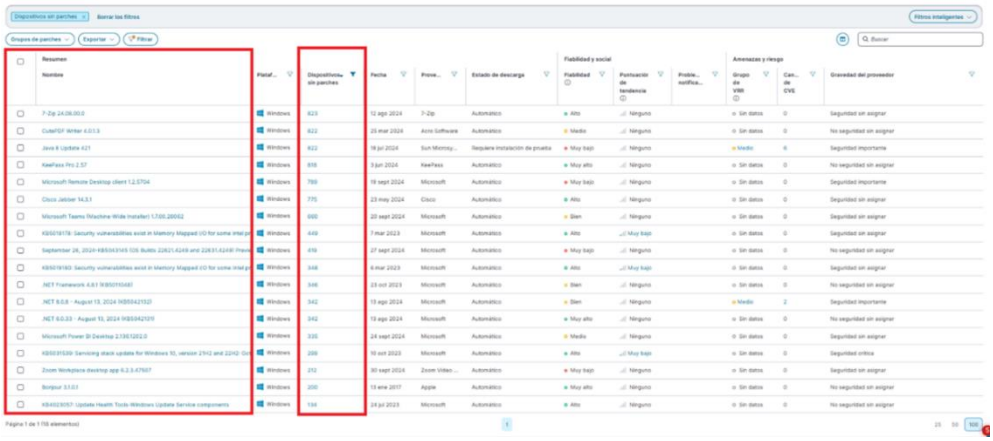


Figura 4 Ivanti - patch Intelligence

Herramienta de Saas para el control de dispositivos

El análisis reciente de la plataforma de administración de actualizaciones reveló que 900/2000 endpoints no han recibido diferentes actualizaciones de software terceros y componentes de Windows como se ve en la Figura 4, Esta situación compromete la seguridad y el rendimiento de los equipos afectados, incrementando el riesgo de exposición a vulnerabilidades cibernéticas y fallos de sistema.

2.2 Fase 2: Planificación

2.2.1 Análisis de impacto en la organización

Se estableció que, mediante una toma de muestras del inventario realizado en el parque tecnológico, se identificó el impacto en la seguridad, basándose en la cantidad de vulnerabilidades encontradas. Esto permitió priorizar y clasificar la criticidad de las vulnerabilidades a las que está expuesta la compañía, por lo cual es de alta importancia la implementación de un proceso para las actualizaciones de software utilitario en los equipos de cómputo de usuario final, y así garantizar la confidencialidad, integridad y disponibilidad, logrando fortalecer la postura

de ciberseguridad de la compañía, encaminado a la correcta protección y tratamiento de los datos personales.(CONGRESO DE COLOMBIA, 2012)

2.2.2 Validación de estándares y marcos normativos de seguridad

Se realizó la validación de los estándares y los marcos normativos de seguridad digital, donde se validó cual se adapta a la compañía con el fin de implementar las mejores prácticas minimizando brechas de seguridad, los estándares y marcos normativos de seguridad reconocidos como ISO/IEC 27001, NIST y las directrices de OWASP, los cuales buscan mitigar riesgos y asegurar la integridad de la información. Este enfoque no solo implicó identificar y evaluar las vulnerabilidades existentes, sino también establecer criterios claros para la validación de prácticas seguras. Con estas herramientas, a través del análisis, se pudo identificar áreas de mejora y desarrollo del plan de acción que incluyó medidas correctivas. A continuación, se relaciona, un cuadro comparativo con los estándares y marcos normativos mencionados.

Tabla 1.

Comparativa entre ISO/IEC 27001, NIST y OWASP

Característica	ISO/IEC 27001	NIST	OWASP
Objetivo	Establecer un sistema de gestión de seguridad de información (SGSI).	Proveer un marco flexible para gestionar riesgos de ciberseguridad.	Mejorar la seguridad de aplicaciones Web.
Enfoque	Gestión de la seguridad de la información en toda la organización.	Identificación, protección, detención, respuesta y recuperación de incidentes.	Mejores prácticas y herramientas para el desarrollo seguro de software.
Estructura	Requiere auditorías internas y	Basado en un ciclo de mejora continua, no	Basado en principios de diseño seguro

Característica	ISO/IEC 27001	NIST	OWASP
	revisiones periódicas.	requiere certificación formal.	y pruebas de seguridad.
Requisitos de documentación	Extensa documentación sobre políticas, procedimientos y controles.	Documentación flexible, puede adaptarse a la necesidad de la organización.	Documentación sobre riesgos y recomendaciones de seguridad para aplicaciones.
Ámbito de aplicación	Aplicable a cualquier organización, independientemente de su tamaño o sector.	Enfocado en organizaciones de todos los sectores, con énfasis en el sector público.	Principalmente enfocado en el desarrollo de software y aplicaciones web.
Implementación	Requiere un enfoque sistemático y continuo para la gestión de la seguridad.	Puede implementarse en fases y adaptarse a las capacidades de la organización.	Proporciona guías y herramientas prácticas para desarrolladores y equipos de seguridad.
Enfoque en formación	Fomenta la capacitación del personal en temas de seguridad.	Promueve la concienciación y formación sobre ciberseguridad.	Proporciona recursos y documentación para educar a los desarrolladores sobre seguridad.

Una de las grandes diferencias identificadas entre los marcos normativos es que NIST se centra en controles técnicos y estándares específicos, la ISO 27001 se enfoca en la gestión y mejora continua del sistema de gestión de la seguridad informática, esto significa que el NIST es más detallado y técnico mientras que la ISO 27001 es más holística y flexible en su enfoque, por otro lado, el OWASP nos ofrece guías prácticas para la mejora de la seguridad de la información y mitigar riesgos.

2.3 Fase 3: Desarrollo

2.3.1 Desarrollo de la propuesta

Se elaboró la propuesta de un proceso con el objetivo de Gestionar software de utilitarios y/o componentes de Windows en equipos de cómputo de usuarios finales en ECOPETROL a través de la instalación de actualizaciones con el fin de garantizar su operación. Definiendo un alcance el cual inicia con la elaboración del cronograma para la instalación mensual de actualizaciones software de utilitarios y/o componentes de Windows en equipos de cómputo de usuarios finales, con la exploración de nuevas actualizaciones, despliegue en pruebas y despliegue general al parque tecnológico finalizando con la gestión del cierre de la actividad. Anexo 3.

En la Figura 5 se puede evidenciar el proceso de la propuesta que incluye las cuatro fases de la metodología PHVA con sus respectivas actividades, adicionalmente o en el Anexo 3 Procedimiento se detallan los roles, descripción y registro de finalización de cada actividad.



Figura 5 Diagrama de flujo de procedimientoAnexo 3

2.3.2 Desarrollo de propuesta de cronograma de despliegue de actualizaciones.

Con el objetivo de mantener los equipos actualizados y seguros, se ha diseñado un cronograma para el despliegue mensual de actualizaciones de software utilitario y componentes de Windows en los equipos de cómputo de los usuarios finales.

Este cronograma contempla la implementación de actualizaciones de todas las aplicaciones utilizadas en la compañía, en sincronía con las versiones disponibles en el mercado. El despliegue se realizará a través de herramientas como Intune, System Center, Lenovo Patch e Ivanti Neurons. En caso de que, después de una semana, algunos equipos no se hayan actualizado de forma automática, se activará un modelo de atención on-site para asegurar que el 100% de los dispositivos cumplan con los estándares de actualización establecidos. Anexo 4

3. Resultados esperados

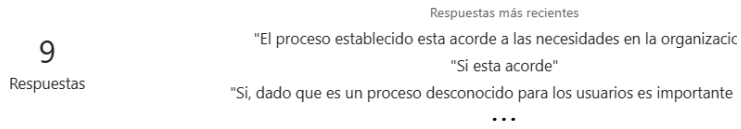
Después de realizar la propuesta del proceso de actualizaciones y la propuesta de cronograma se presentaron a los colaboradores de la organización con el objetivo de recibir retroalimentación, para esto se realizó una encuesta (ver Anexo 5), se obtuvieron los siguientes resultados:

- 56% de los 9 encuestados desconocen si existe un proceso actualmente en la compañía para llevar a cabo las actualizaciones.
- Se validó la frecuencia en la que los usuarios reciben notificaciones sobre las actualizaciones en los equipos de cómputo obteniendo un 56% mediana y un 44% baja.

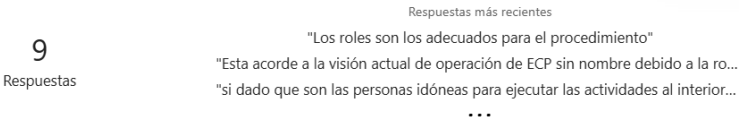
- Se consultó a los usuarios si tenía conocimiento si la compañía adelanta actualizaciones de software utilitario y componentes de Windows donde el 88% lo desconoce



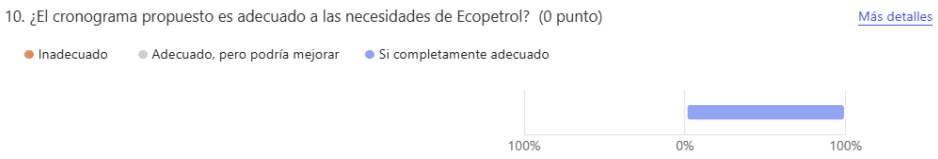
En cuanto a la propuesta indicaron que se adapta a las necesidades de la compañía como se puede verificar en el documento de respuestas de la encuesta Anexo 5 Encuesta



Adicionalmente, los usuarios encuestados estuvieron de acuerdo con los roles establecidos para las actividades, sin embargo, recomiendan incluir un backup para el ejecutor de la actividad, por lo mismo es que se indican cargos y no personas para que siempre el flujo se encuentre activo con sus ejecutores.



Finalmente, en cuanto al cronograma propuesto los usuarios indicaron que están totalmente de acuerdo y que se adapta a la necesidad de la organización.



3.1 Conclusiones

- Una vez socializada la propuesta del proceso para la instalación de las actualizaciones de software utilitarios y/o componentes de Windows para equipos de usuario final y su correspondiente cronograma con algunos colaboradores de Ecopetrol del área de operaciones, se determinó que estos se ajustan a las necesidades actuales de la compañía y mitiga las vulnerabilidades ya detectadas en los equipos y futuras que se puedan desprender de no tener una correcta aplicación de actualizaciones.
- El diagnóstico del estado actual de los equipos de usuarios finales en la compañía, realizado con herramientas internas de Ecopetrol, permitió obtener un inventario detallado y un análisis preciso de las vulnerabilidades presentes. Se identificaron las vulnerabilidades críticas que requieren atención, proporcionando una visión clara sobre el estado de seguridad de los dispositivos.
- Se elaboró y presentó la propuesta del cronograma para la instalación de actualizaciones de software utilitarios y componentes de Windows en equipos de usuario final. Esta propuesta fue validada por los usuarios de la compañía, quienes expresaron que el enfoque satisface las necesidades actuales de Ecopetrol. La propuesta de cronograma fue bien recibida por los colaboradores, ya que proporciona un marco claro y estructurado para asegurar la actualización oportuna de los equipos.
- Una vez socializada la propuesta del procedimiento para la instalación de actualizaciones de software utilitarios y componentes de Windows en equipos de usuario final con colaboradores del área de operaciones de Ecopetrol, se ha determinado que la propuesta se alinea con las necesidades actuales de la organización. Este enfoque no solo responde a los requerimientos operativos, sino que también contribuye significativamente a la mitigación de vulnerabilidades previamente identificadas en los equipos, así como a la prevención de futuras brechas de seguridad derivadas de la falta de actualizaciones oportunas.

3.2 Recomendaciones

Es importante que desde la alta gerencia de la compañía respalde e impulse este tipo de iniciativas para que sean adoptadas y aplicadas al interior de la compañía con el fin de cerrar brechas de seguridad.

Es necesario que la propuesta del proceso incluyendo su cronograma sean revisados y actualizados de manera periódica con el fin de ir adaptándola a las necesidades que se presenten al interior de la compañía y a los cambios que surjan en el mercado.

Desarrollar planes de capacitación continúa dirigido a los usuarios finales y al personal de TI, enfocado en la importancia de las actualizaciones y las mejores prácticas de seguridad, contribuyendo a fomentar una cultura de ciberseguridad en todos los niveles de la organización y a reducir riesgos asociados a la falta de actualización de software y componentes

Bibliografía

Axelos. (2022). *ITIL 4* . https://www.axelos.com/certifications/itil-service-management/itil-4-foundation

Buatista Garcia, F. M. G. L. “TicTac”; F. A. M. “Fortinet”; "CrowdStrike. (2022). TENDENCIAS DEL CIBERCRIME 2021-2022. *Cámara Colombiana de Informática y Telecomunicaciones*.

Center For Internet Secury. (2023). *CIS Critical Security Controls*. https://www.cisecurity.org/controls

CONGRESO DE COLOMBIA. (2012). *Ley 1581 de 2012-Protección de Datos*.

IBM. (2024). *¿Qué es el ransomware?* https://www.ibm.com/es-es/topics/ransomware

ISO/IEC. (2022). *ISO-27001-2022*. *3*.

Microsoft Learn - Deploy and Update Windows. (2024). *Windows deployment documentation*. https://learn.microsoft.com/en-us/windows/deployment/

“MinTic.” (2021). *MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES*. https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

NIST-National Institute of Standards and Technology. (2007). *Guide to Storage Encryption Technologies for End User Devices*. https://doi.org/10.6028/NIST.SP.800-111

OEA - Organización de los Estados Americanos. (2019). *DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA*.

Anexos

Anexo 1 equipos en el parque_25.09.2024_Univer

Modificado el	Naturaleza	Submodelo de	Tipo PC	Serial	Marca	Modelo	Asignación	Ubicacion	Zona	Fecha entrada a operacion
9/25/2024 7:48:31 AM	Computador	PORTATIL	PORTATIL ME	PF2RTL2N	LENOVO	THINKPAD T14 5000	En el parque	CENTRO DE ATENCION LOCAL NEIVA		19/09/2024
9/25/2024 12:26:24 AM	Computador	ESCRITORIO	WORKSTATION	MJDGJMEN	LENOVO	THINKSTATION P720	En el parque	ICP - EDF 9	Zona Santanderes	18/09/2024
9/25/2024 12:22:57 AM	Computador	PORTATIL	PORTATIL ME	PF35HM4N	LENOVO	THINKPAD T14 5000	En el parque	CENTRO COMERCIAL PRIMAVERA URBANA		19/09/2024
9/24/2024 2:11:14 PM	Computador	PORTATIL	PORTATIL HI	PF31A8DY	LENOVO	THINKPAD T14 5000	En el parque	CAMPO DINA GDH	Zona Santanderes	1/08/2024
9/24/2024 12:03:13 AM	Computador	PORTATIL	PORTATIL ME	PF30SDKW	LENOVO	THINKPAD T14 5000	En el parque	CAMPO ORITO GPY	Zona Sur	18/09/2024
9/23/2024 11:52:34 PM	Computador	PORTATIL	PORTATIL ME	PF2RQHT5	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	19/09/2024
9/23/2024 11:40:56 PM	Computador	ESCRITORIO	WORKSTATION	MJDGJMED	LENOVO	THINKSTATION P720	En el parque	REFINERIA BARRANCABERMEJA	Zona Santanderes	19/09/2024
9/23/2024 4:33:44 PM	Computador	PORTATIL	PORTATIL HI	PF31A58V	LENOVO	THINKPAD T14 5000	En el parque	REFINERIA CARTAGENA	Zona Caribe	11/09/2024
9/23/2024 4:31:31 PM	Computador	PORTATIL	PORTATIL HI	PF258SNV	LENOVO	THINKPAD T14 5000	En el parque	CENTRO COMERCIAL PRIMAVERA URBANA		11/09/2024
9/23/2024 4:05:55 PM	Computador	PORTATIL	PORTATIL ME	PF30VJGW	LENOVO	THINKPAD T14 5000	En el parque	CENTRO COMERCIAL PRIMAVERA URBANA		11/09/2024
9/23/2024 3:59:29 PM	Computador	ESCRITORIO	COMPUTADOR DE ESCRITORIO	MJDG9VLM	LENOVO	THINKCENTRE M75Q	En el parque	ICP	Zona Santanderes	11/09/2024
9/23/2024 3:53:29 PM	Computador	ESCRITORIO	COMPUTADOR DE ESCRITORIO	MJDGE2KS	LENOVO	THINKCENTRE M75Q	En el parque	ICP	Zona Santanderes	11/09/2024
9/23/2024 3:50:14 PM	Computador	PORTATIL	PORTATIL ME	PF30XSLW	LENOVO	THINKPAD T14 5000	En el parque	REFINERIA BARRANCABERMEJA	Zona Santanderes	11/09/2024
9/23/2024 2:54:56 PM	Computador	PORTATIL	PORTATIL HI	PF3MM4JD	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO TELUSACA		10/09/2024
9/23/2024 2:47:05 PM	Computador	PORTATIL	PORTATIL ME	PF256D74	LENOVO	THINKPAD T14 5000	En el parque	CENTRO COMERCIAL PRIMAVERA URBANA		10/09/2024
9/23/2024 2:44:03 PM	Computador	PORTATIL	PORTATIL HI	PF25BV26	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO TELUSACA		10/09/2024
9/23/2024 11:48:45 AM	Computador	PORTATIL	PORTATIL ME	PF3NXYJX	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	10/09/2024
9/23/2024 11:11:39 AM	Computador	ESCRITORIO	COMPUTADOR DE ESCRITORIO	MJDGE3Z3	LENOVO	THINKCENTRE M75Q	En el parque	POLICLINICA ECOPETROL	Zona Caribe	9/09/2024
9/23/2024 11:04:14 AM	Computador	PORTATIL	PORTATIL HI	PF3MSDHW	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	9/09/2024
9/23/2024 8:28:58 AM	Computador	PORTATIL	PORTATIL ME	PF30QLHQ	LENOVO	THINKPAD T14 5000	En el parque	CAMPO EL CENTRO - PTA 6	Zona Santanderes	4/09/2024
9/23/2024 8:13:08 AM	Computador	PORTATIL	PORTATIL ME	PF32AYMD	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO TELUSACA		4/09/2024
9/23/2024 7:47:57 AM	Computador	PORTATIL	PORTATIL ME	PF2S91CD	LENOVO	THINKPAD T14 5000	En el parque	REFINERIA CARTAGENA	Zona Caribe	19/09/2024
9/23/2024 12:09:43 AM	Computador	PORTATIL	PORTATIL ME	PF258RT6	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	18/09/2024
9/23/2024 12:03:47 AM	Computador	PORTATIL	PORTATIL ME	PF25XG2P	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	19/09/2024
9/22/2024 11:59:49 PM	Computador	PORTATIL	PORTATIL ME	PF30W682	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	19/09/2024
9/20/2024 10:52:55 PM	Computador	PORTATIL	PORTATIL ME	PF2R9WG3	LENOVO	THINKPAD T14 5000	En el parque	CAMPO CASABE	Zona Santanderes	17/09/2024
9/20/2024 4:07:28 PM	Computador	ESCRITORIO	COMPUTADOR DE ESCRITORIO TORRE	GM0CBCSY	LENOVO	THINKCENTRE M75T	En el parque	TIBU	Zona Santanderes	23/02/2024
9/19/2024 9:09:42 PM	Computador	PORTATIL	PORTATIL HI	PF3MQZH8	LENOVO	THINKPAD T14 5000	En el parque	REFINERIA BARRANCABERMEJA - 25 DE AGOSTO - BLOQUE 8 - SEG FISICA	Zona Santanderes	9/11/2022
9/19/2024 9:09:41 PM	Computador	PORTATIL	PORTATIL ME	PF2RPEWD	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	2/09/2021
9/19/2024 9:09:41 PM	Computador	PORTATIL	PORTATIL ME	PF30QLKV	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	11/10/2021
9/19/2024 9:09:41 PM	Computador	PORTATIL	PORTATIL ME	PF2S63K3	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	5/10/2021
9/19/2024 9:09:40 PM	Computador	PORTATIL	PORTATIL HI	PF3MLPKW	LENOVO	THINKPAD T14 5000	En el parque	REFINERIA BARRANCABERMEJA - 25 DE AGOSTO - BLOQUE 8 - SEG FISICA	Zona Santanderes	4/10/2022
9/19/2024 9:09:39 PM	Computador	PORTATIL	PORTATIL ME	PF30SFMA	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	25/10/2021
9/19/2024 9:09:31 PM	Computador	PORTATIL	PORTATIL ME	PF30RY3D	LENOVO	THINKPAD T14 5000	En el parque	EDIFICIO PRINCIPAL ECOPETROL	Zona Central	3/11/2021

Anexo 2 IvantiNeurons.Notifications.NotificationsExport

Id	Nombre	Plataforma	Proveedor	Cantidad de CVE	mplazado pa	emas notific	Fecha	sitivos sin pa	Fiabilidad	ıación de fiab	Amenaza	Mi fiabilidad	uación de fia	Gravedad del proveedor	Nombre del dispositivo	Nombre del dominio	Dirección IP	ombre de SA	ersión de SC	Tendencia	CVSS	ado de desca
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF3NXRDMC	red.ecopetrol.com.cc	169.254.99.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30E20XC	red.ecopetrol.com.cc	192.168.1.3(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2S8EZ5C	red.ecopetrol.com.cc	10.176.15.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30EYMGC	red.ecopetrol.com.cc	10.165.48.2(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF32AZ4VC	red.ecopetrol.com.cc	192.168.0.4	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30AMVYC	red.ecopetrol.com.cc	10.176.35.2(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BUALF2S8KB1C	red.ecopetrol.com.cc	192.168.10.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2S92FLC	red.ecopetrol.com.cc	10.176.32.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF32AZEXC	red.ecopetrol.com.cc	10.167.128.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF35LAY1C	red.ecopetrol.com.cc	10.176.15.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30A76WC	red.ecopetrol.com.cc	192.168.0.9	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2Q28HDC	red.ecopetrol.com.cc	192.168.0.1(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2R9NCQC	red.ecopetrol.com.cc	192.168.20.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	CAALF30C4MMC	red.ecopetrol.com.cc	10.176.34.2(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RAHHNC	red.ecopetrol.com.cc	10.5.5.215	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RV005C	red.ecopetrol.com.cc	192.168.1.2(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30AWJZC	red.ecopetrol.com.cc	10.176.33.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RV6KQC	red.ecopetrol.com.cc	10.5.4.159	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30BP33C	red.ecopetrol.com.cc	10.165.5.58	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30SFEAC	red.ecopetrol.com.cc	192.168.20.(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RTW23C	red.ecopetrol.com.cc	10.176.15.3(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30WMMCC	red.ecopetrol.com.cc	10.162.36.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RBSCYC	red.ecopetrol.com.cc	192.168.10.(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF36GPDZC	red.ecopetrol.com.cc	192.168.1.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30ERYJC	red.ecopetrol.com.cc	192.168.1.9	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RV7HHC	red.ecopetrol.com.cc	192.168.1.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2S8DJYC	red.ecopetrol.com.cc	192.168.0.2(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF36EAY0C	red.ecopetrol.com.cc	10.176.15.7(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RTZ8GC	red.ecopetrol.com.cc	10.176.15.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RAZQ6C	red.ecopetrol.com.cc	10.137.5.15(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BJALF2S8LNJC	red.ecopetrol.com.cc	10.176.32.1(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	CAALF30WND0C	red.ecopetrol.com.cc	##########	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RPEWDC	red.ecopetrol.com.cc	169.254.12.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30BG7TC	red.ecopetrol.com.cc	10.165.5.15(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30QNJ1C	red.ecopetrol.com.cc	192.168.80.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RPVAKC	red.ecopetrol.com.cc	169.254.46.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF30EV1TC	red.ecopetrol.com.cc	192.168.11.(	Windows 1(	Windows 1(	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RBRE2C	red.ecopetrol.com.cc	192.168.1.6	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RBQWJC	red.ecopetrol.com.cc	10.136.39.2	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RTK2DC	red.ecopetrol.com.cc	192.168.20.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RNQE4C	red.ecopetrol.com.cc	169.254.98.(	Microsoft W	10.0	Ninguno	Sin datos	Automático
KEEP-240603	KeePass Pro 2.57	Windows	KeePass	0	FALSE	0	2-jun-24	818	Muy alto	##########	Sin datos	Excelente	10	No seguridad sin asignar	BOALF2RBTF9C	red.ecopetrol.com.cc	192.168.20.(	Microsoft W	10.0	Ninguno	Sin datos	Automático

Anexo 3 Procedimiento

OBJETIVO	**Gestionar software de utilitarios y/o componentes de Windows en equipos de cómputo de usuarios finales en ECOPETROL a través de la instalación de actualizaciones con el fin de garantizar su operación.**	
ALCANCE	Inicia con la elaboración del cronograma para la instalación mensual de actualizaciones software de utilitarios y/o componentes de Windows en equipos de cómputo de usuarios finales, con la exploración de nuevas actualizaciones, despliegue en pruebas y despliegue general al parque tecnológico finalizando con la gestión del cierre de la actividad.	
ÁMBITO DE APLICACIÓN	Aplica para todos los equipos de cómputo asignados a los usuarios finales pertenecientes al parque tecnológico de la compañía.	
LÍDER	Líder Funcional de Plataformas.	
	ACTUALIZACIONES: En informática, una actualización de sistema operativo consta de cambios que se aplican al mismo, para corregir errores, subsanar fallas de seguridad, o falencias de aplicaciones. **ROLL BACK:** Actividad que devuelve la aplicación o componente a su estado previo. **PUNTO DE RECUPERACION:** También conocidos como copias instantáneas, son una tecnología utilizada para proteger y gestionar datos en sistemas de alta disponibilidad. Se trata de imágenes congeladas del estado de los datos en un momento determinado,	**SERVICIO GESTIONADO POR EL PROVEEDOR :** Modalidad de entrega de los Servicios de despliegue en el parque tecnológico mediante el aprovisionamiento y configuración de los recursos y herramientas contratadas por la Compañía, el proveedor deberá tener en cuenta todos los recursos necesarios para realizar el aprovisionamiento, configuración, instalación, despliegue, ajustes, monitoreo, seguimiento, elaboración y presentación de reportes, elaboración y presentación de informes y administración relacionadas con todos los servicios adquiridos por la Compañía.

DEFINICIONES	capturando tanto los archivos como los metadatos asociados. **SD: (Service Request)** es una solicitud formal que un usuario realiza para recibir asistencia o servicios de TI. Puede abarcar desde solicitudes de acceso a aplicaciones, creación de cuentas de usuario, hasta la configuración de hardware o software. Cada SD tiene un ciclo de vida, que incluye la creación, gestión y resolución.	**SOLICITUD DE CAMBIOS, RFC:** La solicitud de cambio **(Request for Change, RFC)**, consiste en un documento formal que contiene una propuesta para realizar modificaciones que afecten la configuración estándar de una aplicación o servicio. **FTE: Full-Time Equivalent (FTE)** asignado a la Gerencia de Operaciones tiene como objetivo proporcionar apoyo estratégico a todas las áreas bajo su jurisdicción, asegurando una distribución eficiente de su tiempo dentro de las horas laborales permitidas. Su enfoque está dirigido a la asistencia en proyectos de corta y larga duración, garantizando la ejecución exitosa de iniciativas clave, sin involucrarse directamente en las operaciones diarias

POLÍTICAS DE OPERACIÓN:

1. El desarrollo de las actividades por parte del Líder Funcional de Plataformas debe atender lo dispuesto en las funciones asignadas a su rol.
2. La aplicación de este procedimiento debe atender los requisitos establecidos en la Norma Técnica ISO/IEC 27001.
3. Políticas generales:
    - Las actualizaciones de sistema operativo a instalar en los equipos de usuario final serán las liberadas por el fabricante durante el transcurso del mes (generalmente son liberadas en la segunda semana de cada mes), atendiendo las recomendaciones de este.

- Los equipos de usuario final deben ser reiniciados las veces que se requiera según la recomendación del fabricante, una vez se hayan aplicado o instalado las actualizaciones.

- Los usuarios deben realizar las validaciones en sus aplicativos durante las 24 horas siguientes a la instalación de las actualizaciones.

4. Políticas para aplicación de actualizaciones de sistema operativo en ambiente de pruebas

   - La actualización se debe llevar a cabo dentro de la semana siguiente de la liberación realizada por el fabricante.
   - La ventana de tiempo para la realización de la actividad será de aproximadamente 12 horas, preferiblemente en horario nocturno.

5. Políticas para aplicación de actualizaciones en los equipos de usuario final que hacen parte del parque tecnológico:

   - La actualización se debe llevar a cabo dentro de la semana siguiente a la actualización realizada en el ambiente de pruebas.

6. Aplicar los lineamientos institucionales dados en la Política de Administración de Riesgos Institucionales y la Guía para la administración integral de riesgos en los procesos para la ejecución de este procedimiento.

DESCRIPCIÓN DEL PROCEDIMIENTO						
No	**ACTIVIDAD/TAREA**	**DESCRIPCIÓN**	**PHVA**	**PUNTO DE CONTROL**	**RESPONSABLE**	**REGISTRO**
AMBIENTE DE PRUEBAS Y PRODUCCIÓN						
1	Elaborar y enviar cronograma de trabajo al proveedor del servicio de plataformas para la instalación de actualizaciones en los equipos de cómputo	El Líder funcional de plataformas elabora mensualmente el cronograma y envía al proveedor de servicios de plataformas, para la instalación de las actualizaciones en equipos de	Planear		Líder funcional de plataformas	Creación de SD

	asignados a usuarios finales.	cómputo asignados a usuarios finales y registra en la herramienta establecida por la compañía (# de Ticket). Nota: en el correo se debe mencionar las políticas generales establecidas en el presente procedimiento.				
2	Enviar cronograma de trabajo de instalación de actualizaciones de software utilitario y componentes de Windows en los equipos de cómputo de la compañía asignados a los usuarios finales.	El Líder Funcional de Plataformas enviará el cronograma para la instalación de las actualizaciones de software utilitario y componentes de Windows en los equipos de cómputo de la compañía asignados a los usuarios finales. ¿Hay objeciones? Si: Se reajusta el cronograma y continúa con la actividad 1 No: Continúa en actividad 3 NOTA: Los usuarios cuenta con un (1) día hábil para informar si tiene objeciones.	Planear	El Líder Funcional de Plataformas deberá revisar si existen objeciones para ejecutar la actividad.	El Líder Funcional de Plataformas	Actualización de la SD
3	Enviar RFC por parte del FTE asignado a la operación	El FTE notifica al Líder Funcional de Plataformas las actualizaciones a realizar, mediante la creación del SD donde relaciona: • El listado de actualizaciones	Planear	Líder Funcional de Plataformas	FTE	Actualización de la SD

		• Solicitud de cambio (Request for Change, RFC) diligenciada, con la programación de las actualizaciones a realizar				
4	Aprobar la solicitud de Cambio (RFC) para la instalación de las actualizaciones	Una vez validado que la información cumpla con las políticas generales solicitadas en la actividad No. 1 se aprueba el RFC para la instalación de las actualizaciones.	Planear		Líder Funcional de Plataformas	Aprobación del SD.
5	Generar GPO de punto de restauración en los equipos de cómputo de usuario final	El proveedor del servicio de plataformas, por seguridad genera un punto de restauración a todos los equipos de cómputo de usuarios final por medio de una GPO, con el fin de asegurar la información en caso de que las actualizaciones generen fallas y se haga necesario aplicar roll back.	Hacer	Número de SD	Administrador de Tecnología - MECM	Log de Windows
6	Instalar actualizaciones en los equipos de cómputo de usuario final	El Proveedor de servicios de plataformas aplica las actualizaciones en los equipos de cómputo de usuario final de acuerdo con el RFC. Una vez finaliza esta actividad debe enviar el informe respectivo,	Hacer		Administrador de Tecnología - MECM	Informe con las actualizaciones instaladas.

		el cual debe mostrar las actualizaciones que fueron instaladas.				
7	Verificar que se hayan hecho todas las actualizaciones.	Profesional del Líder Funcional de Plataformas, verifica que el informe contemple las actualizaciones solicitadas. ¿Hay objeciones? Si: Se regresa el informe con observaciones Regresa a la actividad 6 No: Continúa en actividad 8	Verificar		Líder Funcional de Plataformas	Respuesta de SD
8	Verificar el funcionamiento de los equipos de computo	Una vez instaladas las actualizaciones en los equipos de cómputo de usuario final, el FTE revisara los incidentes sobre el correcto funcionamiento de los equipos, software base, cadenas de conexión, tareas programadas, sistema operativo y entre otros.	Verificar		FTE y usuarios finales	Casos SD
9	Ejecutar Roll back	El FTE solicitara en caso de que las pruebas no sean éxitos que se ejecute el Roll back al personal OnSite.	Actuar	FTE	FTE / personal OnSite.	Punto de Restauración
10	Cerrar el RFC	Proveedor de servicios de plataformas realiza el cierre del RFC	Actuar		Profesional del proveedor de plataformas	Estado de SD cerrado

Anexo 4 CRONOGRAMA REVISION Y ACTUALIZACION DE APLICACIONES

ACTIVIDAD	NOVIEMBRE				DICIEMBRE				2025	ENERO				FECRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4		SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4
APLICACIONES																																																							
Adobe Acrobat (64-bit) 23.001.20174																																																						
Adobe Refresh Manager_1.8.0																																																					
Stand-alone																																																					
KeePass Pro																																																					
64 Bit HP CIO Components Installer_22.2.1																																																					
7-Zip 21.00 alpha (x64)_21.00 alpha																																																					
Aplicaciones de Microsoft 365 para empresas - es-es_16.0.16227.20318																																																					
Bonjour_3.0.0.10																																																					
Check Point Endpoint Security_87.20.0139																																																					
Cisco Jabber_14.1.4.57561																																																					
ClearPass OnGuard 6.9.5.131053_6.9.5.131053																																																					
ConfigMgr Client Setup Bootstrap_5.00.9040.1000																																																					
Configuration Manager Client_5.00.9088.1000																																																					
APP REVO VDP																																																					
BWISE																																																						
PI GRB-GRC																																																					
SALESFORCE																																																					
RIS GRB-GRC																																																					
SILAB GRB																																																					
PROYECTA																																																					
KADME																																																					
SCHLUMBERGER AVOCET																																																					
HALLIBURTON OPENWELLS																																																					
WELLMEETING																																																					
SMARTPLANT GRB																																																					

Parámetros de implementación	
	EXPLORATORIO- REVISION DE ACTUALIZACIONES PENDIENTES
	PRUEBAS- DESPLIEGUE A 5 MAQUINAS DE PRUEBAS
	DESPLIEGUE-ACTUALIZACION AL PARQUE TECNOLOGICO

Anexo 5 Encuesta

Encuesta Propuesta proceso de actualización de software utilitario y componentes Windows

Encuesta proceso de actualización de software utilitario y componentes de Windows en máquinas cliente - Seminario de grado

1. Nombre

2. Cargo

3. ¿Sabe si Ecopetrol tiene algún proceso de actualizaciones de los equipos de cómputo?

- ◯ Si
- ◯ No

4. ¿Conque frecuencia recibe notificaciones de actualizaciones en el equipo de cómputo asignado por Ecopetrol?

- ◯ Alta
- ◯ Mediana
- ◯ Baja

5. ¿Sabe si Ecopetrol realiza actualización del software utilitario y componentes de Windows en equipos de cómputo de usuario final?

   ◯ Si

   ◯ No

6. Después de leer la propuesta presentada para la actualización del software utilitario y componentes de Windows en equipos de cómputo a usuarios finales con los procesos de Ecopetrol. ¿Considera que la propuesta se adapta a las necesidades actuales de la organización?

7. ¿Considera que los roles establecidos para el proceso son los adecuados para ejecutar las actividades para ejecutar las actividades?

8. ¿Considera que las actividades propuestas en el procedimiento de instalación de actualizaciones en los equipos de cómputo de usuario final son los adecuados?

   Inadecuado ◯ Adecuado, pero podría mejorar ◯

9. ¿Tiene observaciones sobre la propuesta presentada, cuáles?

10. ¿El cronograma propuesto es adecuado a las necesidades de Ecopetrol?

    Inadecuado ◯ Adecuado, pero podría mejorar ◯