| | | |
|---|---|---|
| ALCALDÍA DE MANIZALES | **ALCALDÍA DE MANIZALES**<br>**SERVICIOS JURÍDICOS**<br>**INFORME DE SUPERVISIÓN PARA CONTRATOS** | **PSI-SJM--FR-021**<br>**Estado Vigente**<br>**Versión 02** |

| | |
|---|---|
| **ACTA №** | **03** |
| **FECHA** | **Diciembre de 2024** |
| **SECRETARÍA** | **TIC y Competitividad** |
| **PERIODO EVALUADO** | **2 de noviembre de 2024 al 30 de noviembre de 2024** |
| **CONTRATO O CONVENIO №** | **2408260980** |
| **OBJETO** | **"AUNAR ESFUERZOS PARA DESARROLLAR UNA ESTRATEGIA DE FORTALECIMIENTO DE CIBERSEGURIDAD EN LAS EMPRESAS DE MANIZALES"** |
| **CONTRATISTA** | **BIOS "CENTRO DE BIOINFORMÁTICA Y BIOLOGÍA COMPUTACIONAL DE COLOMBIA"** |
| **SUPERVISOR(ES)** | **JUAN PABLO TOBARIA HURTADO** |
| **PLAZO DE EJECUCIÓN** | **Desde la suscripción del acta de inicio, hasta el 30 de noviembre 2024** |
| **VALOR DEL CONTRATO O CONVENIO** | **DOSCIENTOS CATORCE MILLONES DOSCIENTOS OCHENTA Y CINCO MIL SETECIENTOS CATORCE PESOS ($214.285.714)**<br>Aporte del Municipio de Manizales: **CIENTOCINCUENTA MILLONES DE PESOS M/CTE ($150.000.000)**<br>Aporte de la Corporación BIOS: **SESENTA Y CUATRO MILLONES DOSCIENTOS OCHENTA Y CINCO MIL SETECIENTOS CATORCE PESOS M/CTE ($64.285.714)** |
| **PRÓRROGAS** | **No Aplica** |
| **SUSPENSIONES** | **No Aplica** |
| **ADICIONES** | **No Aplica** |

| **VERIFICACIÓN DE OBLIGACIONES** | | | | |
|---|---|---|---|---|
| **№** | **DESCRIPCIÓN DE LA OBLIGACIÓN** | **ACTIVIDADES REALIZADAS** | | **DESCRIPCIÓN DEL CUMPLIMIENTO** |
| | | **CANTIDAD** | **PORCENTAJE** | |
| **1.1** | Plan de acción donde se detalle la estrategia a implementar | **1 plan de acción** | 100% | **Programa integral de fortalecimiento de capacidades de ciberseguridad dirigido específicamente a las MiPymes de Manizales.**<br><br>En la ejecución del programa integral de fortalecimiento de capacidades de ciberseguridad dirigido específicamente a las MiPymes de Manizales, se le proporcionaron a las empresas herramientas y conocimientos prácticos para protegerse contra amenazas cibernéticas. Este programa fomentó una cultura de seguridad cibernética proactiva en el tejido empresarial local, lo que fortaleció la resiliencia de las MiPymes, dotándolas de capacidades y conocimientos necesarios para enfrentar las amenazas digitales. El proyecto no solo benefició a las empresas al proteger sus activos y garantizar su continuidad operativa, sino que también contribuyó al desarrollo económico sostenible y al fortalecimiento del tejido empresarial.<br><br>**Convocatoria**<br>La convocatoria logró la inscripción de 117 MiPymes, a través de una difusión efectiva mediante visitas, reuniones y redes sociales. La capacitación se estructuró en 20 horas teóricas distribuidas en cuatro sesiones, abarcando temas como fundamentos de ciberseguridad, respuesta ante incidentes, malware y prácticas seguras. Además, se desarrolló un laboratorio práctico denominado LightFire, donde los participantes pudieron realizar simulaciones de ataques y pruebas de penetración.<br><br>La evaluación de resultados mostró un alto nivel de participación y satisfacción entre los asistentes, con 78 participantes y 53 MiPymes recibiendo certificados de culminación. En conclusión, la estrategia implementada ha sido efectiva en el fortalecimiento de las capacidades de ciberseguridad de las MiPymes de Manizales, mejorando su preparación |

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ante amenazas y contribuyendo aldesarrollo económico sostenible de la región<br><br>Para ampliar la cobertura de la convocatoria, BIOS incluyó durante sus presentaciones en las visitas pedagógicas e institucionales la invitación a participar en el programa de ciberseguridad promovido por la Alcaldía, destacando la importancia de fortalecer las capacidades digitales. Adicionalmente, se desarrollaron reuniones con entidades e instituciones aliadas como FENALCO, ACOPI y la Universidad de Caldas. Durante todo el mes de septiembre, la convocatoria se mantuvo activa en las redes sociales de BIOS, y se produjeron videos invitando a las MiPymes a sumarse al programa de capacitación con el objetivo de mejorar la gestión y protección de su información. También se enviaron más de 16.000 correos desde BIOS a todas las MiPymes de Manizales para animarlas a participar<br>en este eje de formación.<br><br>
<table>
<tr><th>Temario</th><th>Experto</th><th>Fechas (G1, G2, G3, G4)</th><th>% Planeado</th><th>% Ejecutado</th></tr>
<tr><td>Kick Off</td><td>John César Arango/Alejandro Loaiza</td><td>27 de septiembre 2:00 a 3:00pm</td><td>100%</td><td>100%</td></tr>
<tr><td>Fundamentación en Ciberseguridad</td><td>Efren Arcesio Sánchez Javela</td><td>01, 02, 03, 04 de octubre 2:00-7:00 pm</td><td>25%</td><td>25%</td></tr>
<tr><td>Respuesta y Acciones ante Infiltraciones Cibernéticas</td><td>James Montaño</td><td>08, 09, 10, 11 de octubre 2:00-7:00 pm</td><td>0%</td><td>0%</td></tr>
<tr><td>Malware y Amenazas de Nueva Generación</td><td>Andrés Orozco</td><td>15, 16, 17, 18 de octubre 2:00-7:00 pm</td><td>0%</td><td>0%</td></tr>
<tr><td>Prácticas saludables para trabajar en entornos seguros</td><td>John César Arango/Alejandro Loaiza</td><td>22, 23, 24,/ 25 de octubre 2:00-7:00 pm</td><td>0%</td><td>0%</td></tr>
<tr><td>Workshop</td><td>Equipo BIOS Academy y Grupo de Expertos</td><td>11, 25 de octubre 12:00 - 1:00 pm</td><td>0%</td><td>0%</td></tr>
<tr><td>LithgFire (Laboratorio de ciberseguridad)</td><td>Equipo BIOS Academy y Grupo de Expertos</td><td>10 y 11 de Noviembre 2:00-7:00 pm</td><td>0%</td><td>0%</td></tr>
</table>
<br>Se estableció la siguiente agenda académica:<br>
1. Fundamentación en Ciberseguridad<br>
2. Respuesta y Acciones ante Infiltraciones Cibernéticas<br>
• Principios y Estrategias<br>
• Estrategia de comunicación durante Infiltraciones<br>
• Análisis Forense y Recopilación de Evidencias<br>
• Recuperación y Continuidad<br>
3. Malware y Amenazas de Nueva Generación<br>
• Fundamentos e identificación<br>
• Técnicas de Ofuscación y Evasión<br>
• Técnicas de Ingeniería Inversa<br>
• Promoción y Prevención<br>
• Inteligencia de Amenazas<br>
• Detección y Respuestas a Incidentes<br>
4. Prácticas saludables para trabajar en entornos seguros<br><br>
CIBER LAB<br>
LithgFire (Laboratorio de ciberseguridad): Se establecerá un laboratorio de ciberseguridad donde las empresas podrán poner en práctica los conocimientos adquiridos durante la capacitación. Este laboratorio proporcionará un entorno seguro y controlado donde los participantes podrán simular ataques cibernéticos, realizar pruebas de penetración, evaluar la seguridad de sistemas y aplicaciones, y aprender a responder adecuadamente ante incidentes de seguridad. La duración del laboratorio será de diez (10) horas y estará dirigido por un experto en ciberseguridad que brindará asistencia y orientación a los participantes. Se programarán dos (2) sesiones de workshops virtuales que facilitarán la respuesta a dudas e inquietudes relacionadas con los light fires programados en el laboratorio.<br>
Lo anterior evidencia el cumplimiento de las actividades planeadas de acuerdo con la agenda establecida en el plan de trabajo conjunto entre la Alcaldía de Manizales y BIOS.</td>
</tr>
<tr>
<td>2.1</td>
<td>Informe final de capacitación,</td>
<td>1 informe</td>
<td>100%</td>
<td>En este informe detalla el desarrollo de la capacitación teórica dirigida a las MIPYMES, la cual se llevó a cabo en cuatro módulos, orientados por</td>
</tr>
</table>

| | | | | |
|---|---|---|---|---|
| | incluyendo la lista de asistencia, resultados de evaluaciones, y retroalimentación de los participantes. | | | docentes en los siguientes temas:<br><br>**Fundamentación en Ciberseguridad**: Se introdujeron los conceptos básicos de la ciberseguridad, resaltando la importancia de proteger la información y los activos digitales de las empresas.<br><br><br><br><br><br><br><br>**Respuesta y Acciones ante Infiltraciones Cibernéticas:** Este módulo se centró en las estrategias y protocolos a seguir en caso de un ataque cibernético, enfatizando la necesidad de tener un plan de respuesta efectivo. |







**Malware y Amenazas de Nueva Generación**: Se exploraron los diferentes tipos de malware y las amenazas emergentes que enfrentan las empresas hoy en día, así como las mejores prácticas para mitigarla







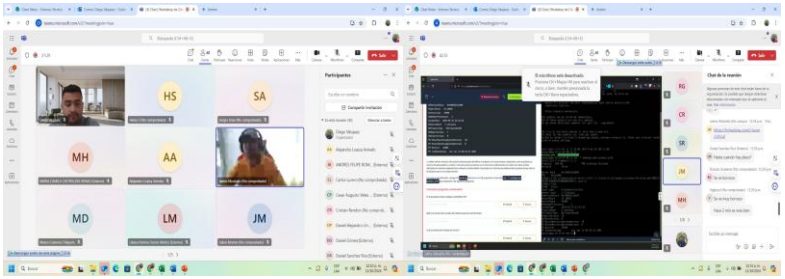
**Prácticas Saludables para Trabajar en Entornos Seguros:** Se discutieron hábitos y prácticas que los empleados deben adoptar para garantizar un entorno de trabajo seguro, tanto físico como digital.

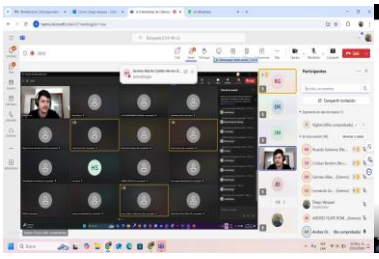






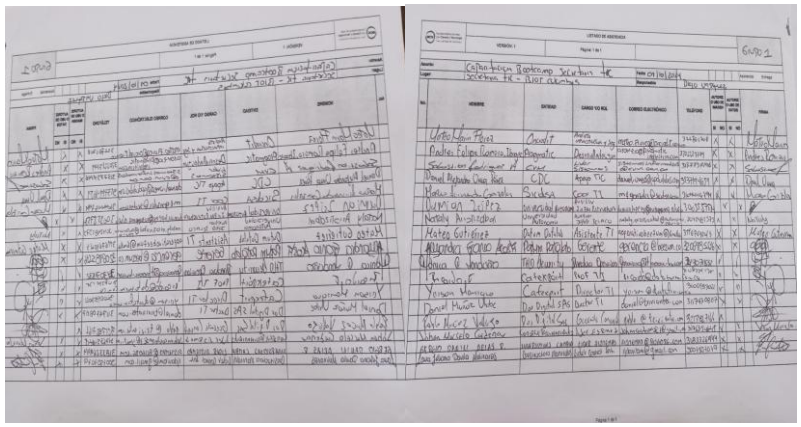
Además de los módulos teóricos, se llevaron a cabo dos workshops interactivos que tuvieron una excelente recepción por parte de los participantes. Durante estos talleres, se despejaron dudas, se realizaron encuestas para evaluar la satisfacción y se llevaron a cabo pequeñas demostraciones de laboratorios en ciberseguridad. Estas actividades prácticas permitieron a los participantes aplicar los conocimientos adquiridos y experimentar de primera mano las herramientas y técnicas discutidas.

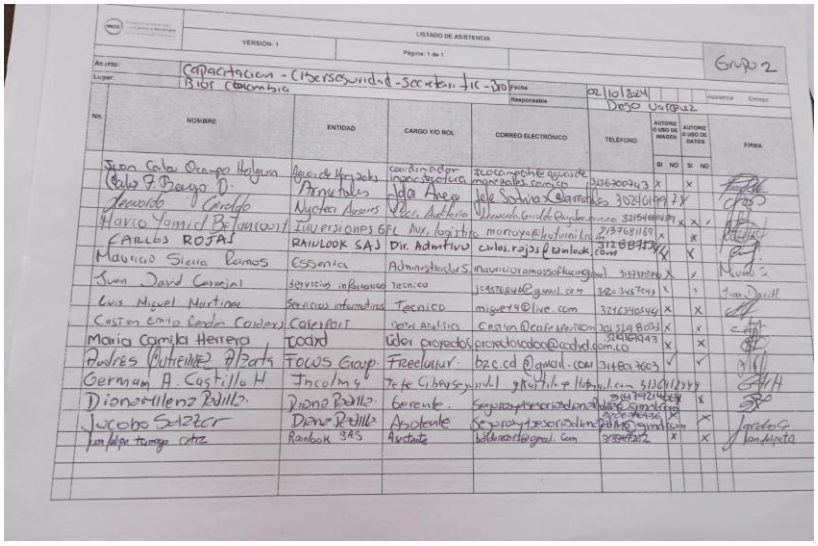


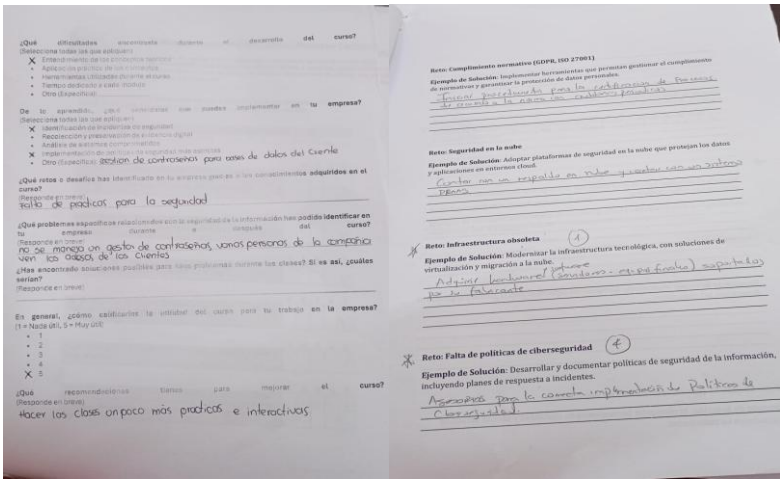


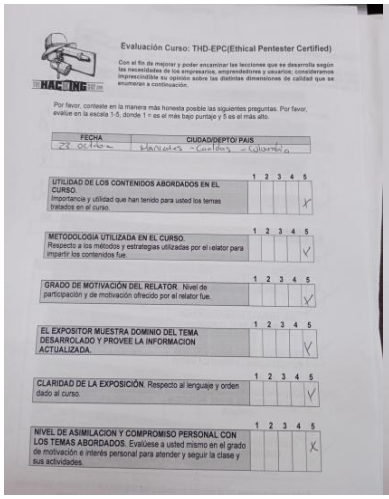
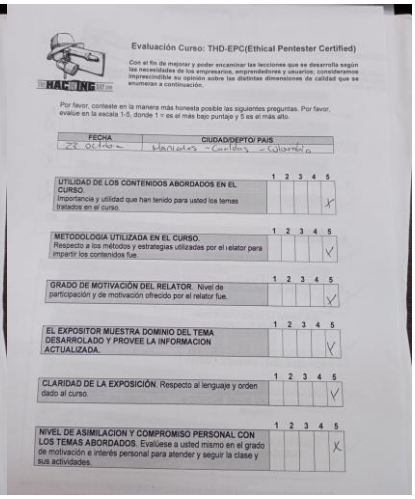
Se recogieron listas de asistencia tanto físicas como virtuales para asegurar un seguimiento adecuado de la participación en las actividades.

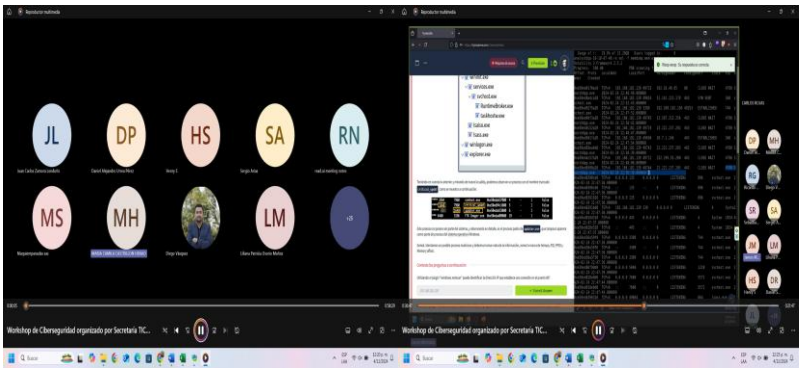




Se realizaron encuestas de satisfacción, tanto en formato físico como virtual, con el fin de obtener retroalimentación valiosa de los participantes sobre su experiencia y el impacto de las capacitaciones.



| | | | | |
|---|---|---|---|---|
| | | | |  <br><br><br>El siguiente paso en este proceso formativo fue los laboratorios virtuales programados para los días 12 y 13 de noviembre. Estos laboratorios permitieron a los participantes profundizar en los temas tratados y practicar habilidades específicas en un entorno controlado. La clausura del programa estuvo prevista para el 21 de noviembre, donde se realizó una evaluación final y se entregaron los certificados de participación.<br><br>Los resultados de las evaluaciones realizadas al finalizar cada módulo reflejaron un alto nivel de comprensión y satisfacción entre los participantes. La mayoría de ellos expresó que se sentía más preparado para enfrentar los desafíos en ciberseguridad y aplicar lo aprendido en sus respectivos entornos laborales. Además, se llevaron a cabo encuestas de satisfacción dirigidas a los docentes, donde obtuvimos una buena recepción por parte de los participantes. Estos calificaron de manera muy positiva los objetivos de nuestra área de ciberseguridad. |
| **2.2** | Certificados de participación emitidos a los empresarios capacitados. | **100%** | 100% | La entrega de certificados se llevó a cabo el 21 de noviembre de manera presencial. Este evento se realizó en la Secretaría TIC de Manizales.<br>Durante la jornada, se certificaron un total de 78 personas participantes, así como 53 empresas MiPYME que formaron parte de esta iniciativa. La participación activa de todos los asistentes ha sido fundamental para el éxito del curso.<br>  |

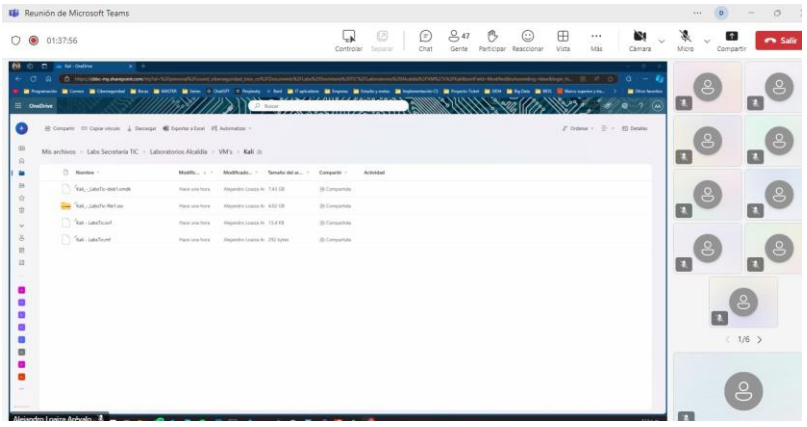
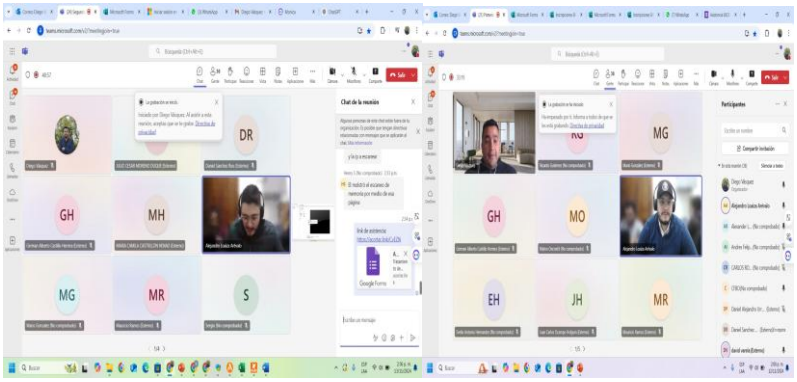
| | | | | |
|---|---|---|---|---|
| | | | |  |
| **3.1** | Grabaciones de las dos sesiones workshop | **2 grabaciones** | 100% | Se llevaron a cabo las grabaciones de las dos sesiones del workshop realizadas el 11 y el 25 de octubre de 2024. También se tomaron fotografías y se elaboraron listas de asistencia para ambas sesiones virtuales. Durante los talleres, se despejaron dudas y se cumplió con calidad en ambos workshops. La retroalimentación de los participantes fue muy positiva, destacando la claridad de las explicaciones y la relevancia de los temas tratados. Este esfuerzo contribuyó a fortalecer las habilidades de los asistentes y potenció su confianza en la aplicación de lo aprendido.<br><br><br><br> |
| **3.2** | Informe de las preguntas y respuestas abordadas durante las sesiones. | **1 informe** | 100% | Se ha cumplido con el objetivo del curso diseñado para fortalecer las capacidades de los empresarios de Manizales a través de capacitación en ciberseguridad. A lo largo de las sesiones, los participantes adquirieron conocimientos teóricos y prácticos que les permitirán implementar medidas efectivas de seguridad en sus empresas, protegiendo así su información y activos digitales.<br><br>1.Pregunta: ¿Cuáles son las amenazas cibernéticas más comunes que enfrentan las empresas hoy en día? |

| | | | | |
|---|---|---|---|---|
| | | | | Respuesta: Las amenazas más comunes incluyen el phishing, que es un intento de obtener información sensible como contraseñas y datos bancarios a través de correos electrónicos engañosos. El malware es otro riesgo, que puede infectar sistemas y robar datos. El ransomware cifra la información y exige un rescate para liberarla, lo cual puede paralizar las operaciones de una empresa. Además, los ataques de denegación de servicio (DDoS) buscan saturar la red, haciendo que los servicios sean inaccesibles. Es crucial estar informado y preparado para estas amenazas mediante la implementación de medidas de seguridad adecuadas.<br><br>2. Pregunta: ¿Qué medidas básicas de seguridad puedo implementar de inmediato en mi empresa?<br>Respuesta: Algunas medidas básicas incluyen el uso de contraseñas fuertes, que deben combinar letras, números y caracteres especiales. La implementación de autenticación de dos factores añade una capa extra de seguridad, ya que requiere un segundo método de verificación. Mantener el software actualizado es vital, ya que muchas actualizaciones incluyen parches de seguridad. También es importante capacitar a los empleados sobre prácticas seguras, como identificar correos electrónicos sospechosos y evitar hacer clic en enlaces desconocidos.<br><br>3. Pregunta: ¿Cómo puedo asegurarme de que mis datos están protegidos en la nube?<br>Respuesta: Asegúrate de utilizar proveedores de servicios en la nube que ofrezcan cifrado de datos tanto en tránsito como en reposo, lo que significa que la información está protegida mientras se envía y mientras se almacena. La autenticación robusta, como la autenticación multifactor, es esencial para proteger el acceso a tus datos. También es importante revisarlas políticas de privacidad del proveedor y asegurarte de que cumplan con las regulaciones pertinentes. Además, realiza copias de seguridad regulares y verifica que puedas restaurar tus datos en caso de pérdida.<br><br>4. Pregunta: ¿Qué debo hacer si sospecho que mi empresa ha sido víctima de un ciberataque?<br>Respuesta: Si sospechas que tu empresa ha sido víctima de un ciberataque, lo primero que debes hacer es aislar los sistemas afectados para evitar que el ataque se propague. Cambia las contraseñas de acceso y notifica a tu equipo de IT inmediatamente. Es recomendable informar a las autoridades competentes para que puedan investigar el incidente. Realiza un análisis forense para entender el alcance del ataque y determinar qué datos fueron comprometidos. Finalmente, revisa y mejora tus medidas de seguridad para prevenir futuros incidentes.<br><br>5. Pregunta: ¿Es necesario contar con un plan de respuesta ante incidentes?<br>Respuesta: Sí, es fundamental tener un plan de respuesta ante incidentes. Este plan debe incluir protocolos claros sobre cómo identificar, contener y erradicar un ataque. Tener un equipo designado para manejar incidentes de seguridad cibernética es crucial para actuar rápidamente y de manera efectiva. Además, el plan debe ser revisado y actualizado regularmente para adaptarse a nuevas amenazas y cambios en la infraestructura de la empresa. Esto no solo minimiza el daño potencial, sino que también ayuda a restaurar las operaciones normales lo más rápido posible.<br><br>6. Pregunta: ¿Qué papel juega la capacitación continua en la ciberseguridad?<br>Respuesta: La capacitación continua es esencial en ciberseguridad, ya que las amenazas cibernéticas están en constante evolución. Mantener a los empleados informados sobre las últimas tendencias y técnicas utilizadas por los atacantes es fundamental para prevenir incidentes. La capacitación regular ayuda a crear una cultura de seguridad en la empresa, donde todos los empleados son conscientes de su papel en la protección de la información. Además, fomenta el uso de buenas prácticas, como la identificación de correos electrónicos de phishing y la gestión segura de contraseñas.<br><br>7.Pregunta: ¿Qué herramientas recomendarías para proteger nuestra red? |

| | | | | |
|---|---|---|---|---|
| | | | | Respuesta: Recomiendo utilizar firewalls para controlar el tráfico entrante y saliente de la red y protegerla de accesos no autorizados. El software antivirus es fundamental para detectar y eliminar malware antes de que cause daño. Los sistemas de detección de intrusiones (IDS) monitorean la red en busca de actividades sospechosas y pueden alertar a los administradores sobre posibles amenazas. Además, considera implementar soluciones de gestión de información y eventos de seguridad (SIEM) para recopilar y analizar datos de seguridad en tiempo real.<br><br>8. Pregunta: ¿Cómo puedo evaluar la efectividad de nuestras medidas de ciberseguridad?<br>Respuesta: Puedes realizar auditorías de seguridad periódicas para evaluar la efectividad de tus medidas de ciberseguridad. Las pruebas de penetración simulan ataques reales para identificar vulnerabilidades en tu sistema. Las simulaciones de ataques, como ejercicios de phishing, pueden ayudar a evaluar la preparación de tus empleados. También es importante revisar los registros de seguridad y los informes de incidentes para identificar patrones y áreas de mejora. Estas evaluaciones te ayudarán a identificar vulnerabilidades y mejorar tus defensas, asegurando que tu empresa esté mejor preparada para enfrentar amenazas futuras |
| **4.1** | Informe que detalle el desarrollo del laboratorio, incluyendo la asistencia, los temas cubiertos, la evaluación de los participantes, y las recomendaciones para futuras actividades de capacitación. | **1 informe** | 100% | En este informe detalla el desarrollo del laboratorio programado para el 12 y 13 de noviembre, dirigido a los integrantes de las MIPYMES. Se abordarán diversos temas relevantes en el ámbito de la ciberseguridad, y se llevará a cabo la recolección de asistencias y las preguntas realizadas por los participantes.<br><br>Se registro la asistencia de todos los participantes durante los dos días de laboratorio, asegurando que cada integrante esté presente y pueda beneficiarse de las actividades programadas.<br><br>**Resumen Ejecutivo del Laboratorio 1:**<br><br>**Objetivo del laboratorio:** El Laboratorio 1 se enfocó en la detección, análisis y explotación de vulnerabilidades en un entorno práctico basado en contenedores Docker. Los participantes trabajaron con sistemas simulados vulnerables para practicar técnicas de análisis forense y escalada de privilegios, utilizando herramientas modernas de seguridad informática.<br><br>**Aspectos clave:**<br>•Despliegue del entorno:<br>o Configuración del contenedor vulnerable "chocolatelovers" utilizando Docker.<br>o Validación de conectividad y exploración de puertos con herramientas como Nmap.<br>•Exploración y explotación:<br>o Descubrimiento de la plataforma web "Nibbleblog" a través de análisis de directorios y contenido web.<br>o Explotación de la vulnerabilidad CVE-2015-6967 utilizando Metasploit, tras identificar credenciales predeterminadas (admin/admin) y un complemento vulnerable ("My Images").<br>• Escalada de privilegios:<br>o Uso de una reverse shell para interactuar con el sistema comprometido.<br>o Identificación del usuario con privilegios administrativos ("chocolate") y explotación de permisos mediante PHP para obtener control total sobre el sistema.<br><br>**Conclusión del laboratorio:**<br><br>o Ejecución de un script PHP modificado para ganar acceso como usuario root.<br>o Éxito en la simulación de un ataque desde la exploración inicial hasta la obtención de privilegios de superusuario.<br><br>**Logros del laboratorio:** El laboratorio proporcionó una experiencia integral en el manejo de herramientas y técnicas de seguridad informática, desde el |

| | | | | |
|---|---|---|---|---|
| | | | | reconocimiento inicial hasta la explotación de vulnerabilidades críticas y la escalada de privilegios en un entorno controlado.<br><br>**Resumen Ejecutivo del Laboratorio 2:**<br><br>El Laboratorio 2 se centró en la seguridad informática mediante la exploración de vulnerabilidades, técnicas de explotación y análisis forense digital en sistemas Windows XP, Windows 7 y contenedores Linux en Docker. Los participantes llevaron a cabo actividades prácticas que incluyeron despliegue, exploración de vulnerabilidades y explotación, utilizando herramientas como SQLmap, Burp Suite, Gobuster y John the Ripper para descubrir debilidades y obtener accesos no autorizados.<br><br>**Aspectos principales del laboratorio:**<br>• Despliegue del entorno:<br>o Configuración de contenedores Docker, actualización de sistemas, instalación de dependencias y carga de imágenes para simular entornos vulnerables.<br>o Exploración inicial y pruebas de conectividad, como escaneos de puertos con Nmap.<br><br>• Explotación de vulnerabilidades:<br>o Pruebas de inyección SQL en un sistema web para obtener acceso no autorizado y extraer datos sensibles como credenciales de usuarios.<br>o Uso de herramientas como SQLmap para enumerar bases de datos, tablas y datos almacenados.<br><br>• Análisis de archivos protegidos:<br>o Descompresión de archivos protegidos con contraseñas mediante extracción de hashes y rompimiento de claves con herramientas como John the Ripper.<br>o Acceso a directorios ocultos y recuperación de información sensible.<br><br>• Escalada de privilegios:<br>o Uso de herramientas como BusyBox para sortear restricciones del sistema y acceder a archivos protegidos.<br>o Obtención de privilegios de root mediante el uso de claves privadas SSH extraídas del sistema comprometido.<br><br>El laboratorio concluyó con éxito, destacando las técnicas y metodologías necesarias para detectar, analizar y responder a incidentes de seguridad. Además, se resaltaron las diferencias entre la seguridad de sistemas Windows y Linux, ofreciendo una experiencia integral y práctica en entornos controlados.<br><br>**Resumen Ejecutivo del Laboratorio 3**<br><br>**Objetivo:** El laboratorio 3 se centró en la identificación y explotación de vulnerabilidades en el sistema web MyBB, utilizando técnicas de fuerza bruta, ejecución remota de código (RCE) y escalada de privilegios. Los participantes adquirieron experiencia práctica al comprometer un sistema configurado en un entorno Docker.<br><br>**Aspectos principales:**<br><br>• Despliegue del entorno:<br>o Configuración de un contenedor Docker con MyBB y validación de conectividad mediante escaneos de puertos.<br>o Edición del archivo /etc/hosts para resolver el dominio local del contenedor.<br>• Análisis y explotación de vulnerabilidades:<br>o Identificación de la versión vulnerable de MyBB (1.8.35), la cual contiene la vulnerabilidad CVE-2023-41362. |

| | | | | |
|---|---|---|---|---|
| | | | | ○ Uso de herramientas como Gobuster y WhatWeb para descubrir directorios y tecnologías implementadas.<br>○ Ataque de fuerza bruta con Hydra para descubrir credenciales válidas del administrador (admin/babygirl).<br>○ Ejecución de un exploit RCE para obtener acceso al sistema.<br>• Escalada de privilegios:<br>○ Utilización del usuario alice, que puede ejecutar scripts Ruby con permisos de root, para crear y ejecutar un script que otorga acceso completo al sistema.<br>○ Acceso continuo al sistema mediante una reverse shell configurada con Netcat.<br><br>**Conclusión:**<br><br>• Este laboratorio demostró vulnerabilidades críticas como políticas de contraseñas débiles, falta de actualizaciones en el software, y configuraciones permisivas en la ejecución de scripts.<br>• Los participantes lograron comprometer el sistema de forma completa, desde el acceso inicial hasta la obtención de privilegios de root.<br>• Lecciones aprendidas: La actividad resaltó la importancia de implementar medidas de seguridad como:<br>○ Políticas estrictas de contraseñas.<br>○ Actualización constante del software.<br>○ Restricciones en la ejecución de scripts y configuraciones de permisos mínimos.<br><br>El laboratorio proporcionó una visión práctica y completa de los riesgos y desafíos en la seguridad informática.<br><br>**Resumen Ejecutivo del Laboratorio 4**<br><br>Resumen Ejecutivo: Explotación de la Vulnerabilidad EternalBlue (CVE-2017-0143)<br><br>Este laboratorio presenta un análisis práctico de la explotación de la vulnerabilidad EternalBlue en un sistema Windows 7, utilizando herramientas avanzadas como Metasploit. El propósito es demostrar las etapas clave de un ataque controlado y resaltar las implicaciones de las fallas de seguridad.<br><br>**Objetivos**<br>• Simular un ataque controlado para acceder de forma no autorizada a un sistema.<br>• Mostrar cómo identificar vulnerabilidades, explotarlas y extraer credenciales de usuarios.<br><br>Pasos Clave<br>Reconocimiento y Análisis: Se identificaron dispositivos y configuraciones de red mediante herramientas como ping y nbtscan.<br><br>Identificación de Vulnerabilidades: Se exploró el protocolo SMB en el puerto 445 utilizando crackmapexec. Se confirmó que el sistema era vulnerable al exploit EternalBlue.<br><br>Explotación: Se empleó el módulo MS17-010 de Metasploit para ejecutar el exploit. Se configuró un reverse shell para obtener acceso remoto al sistema comprometido.<br><br>Extracción de Información: Se localizaron archivos sensibles, como un archivo password.txt. Las credenciales encontradas fueron descifradas con hashcat, demostrando la exposición de datos críticos.<br><br>Resultados<br>Acceso Exitoso: Se obtuvo acceso remoto al sistema, demostrando la explotación efectiva de la vulnerabilidad EternalBlue. |

| | | | | |
|---|---|---|---|---|
| | | | | Extracción de Datos Sensibles: Se recuperaron y descifraron contraseñas de usuarios, confirmando el impacto crítico de esta vulnerabilidad.<br>Conclusión<br><br>El laboratorio demuestra de forma práctica cómo las vulnerabilidades mal gestionadas pueden ser explotadas, poniendo en riesgo la seguridad de los sistemas. Este ejercicio destaca la importancia de aplicar parches de seguridad y realizar evaluaciones regulares para mitigar posibles amenazas.<br><br><br><br><br> |
| **5.1** | Informe final, presentará un análisis detallado de la estrategia implementada para el fortalecimiento de las capacidades de ciberseguridad en las MiPymes de Manizales. | **1 informe** | 100% | Se cumplió con toda la estrategia establecida para la transferencia de conocimiento en ciberseguridad, realizando la planeación y estructuración académica diseñada para el ecosistema empresarial invitado. Se inició la ejecución del Programa Integral de Fortalecimiento de Capacidades en Ciberseguridad, dirigido específicamente a las MiPymes de Manizales. Este programa proporcionó a las empresas herramientas y conocimientos prácticos para protegerse contra amenazas cibernéticas, al tiempo que fomentó una cultura de seguridad cibernética proactiva en el tejido empresarial local. Esto fortaleció la resiliencia de las MiPymes de Manizales, dotándolas de capacidades y conocimiento para enfrentar las amenazas digitales. El proyecto no solo benefició a las empresas al proteger sus activos y garantizar su continuidad operativa, sino que también contribuyó al desarrollo económico sostenible y al fortalecimiento del tejido empresarial de la región.<br><br>Además, se llevaron a cabo talleres y capacitaciones que permitieron a los participantes aplicar lo aprendido en situaciones reales, mejorando su capacidad de respuesta ante incidentes de seguridad. Las empresas participantes reportaron un aumento en la conciencia sobre la importancia de la ciberseguridad y la implementación de medidas preventivas.<br><br>Anexo1 informe Final |
| **1** | Aportar los recursos en efectivo pactados para la ejecución del Convenio en las | **1 informe** | 100% | El conviniente aporto los recursos pactados.<br><br>Anexo 2-Informe Financiero. |

| | | | | |
|---|---|---|---|---|
| | condiciones descritas, por valor de SESENTA Y CUATRO MILLONES DOSCIENTOS OCHENTA Y CINCO MIL SETECIENTOS CATORCE PESOS ($64.285.714) equivalentes al 30% del valor total del mismo. | | | |

El Supervisor certifica que el contratista está ejecutando las obligaciones y el objeto contractual, de conformidad con lo pactado asegurando que no ha omitido información y la consignada es veraz.



**FIRMA**
**NOMBRE: JUAN PABLO TOBARIA HURTADO**
**C.C. 1097388823**
**SUPERVISOR**