GRUPO HORUS

Asunción, 03 de julio de 2023

Señor
Richard Fabian Baddouh Berni, Coordinador TIC de la Unidad Ejecutora de Programas y Proyectos del Ministerio de Educación y Ciencias
Ministerio de Educación y Ciencias (MEC)

REF.: Entrega del Producto 4 "Informe Final de la Consultoría de síntesis de recomendaciones y entrega Técnica" conforme Orden de Inicio de Servicios en el marco del contrato N°07-22 CD – Contratación Directa Nº 01/2022 "CONSULTORIA PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC (HACKING ETICO) - SEGUNDO LLAMADO"ID: 416.862.

Presente

De nuestra mayor consideración,

Tenemos el agrado de dirigirnos a Usted en el marco del *contrato N°07-22 CD – Contratación Directa Nº 01/2022 "CONSULTORIA PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC (HACKING ETICO) - SEGUNDO LLAMADO"ID: 416.862. Para realizar la entrega del siguiente Producto:*

- Producto 4: 1(un) Informe Final de la Consultoría de síntesis de recomendaciones y entrega Técnica.

Aprovechamos la oportunidad para saludarlos muy atentamente.

Daniel Aranda Acosta
Gerente Administrativo y Financiero
GRUPO HORUS S.A.

GRUPO HORUS
GRUPO HORUS S.A.

U.E.P.P. MEC
Exp. Nº: 7076
Recibido por:

DIA	MES	AÑO	HORA
03	JUL	2023	16:07

Avda. Brasilia 228 • CP 1208 • Asunción, Paraguay
www.grupohorus.com.py

INFORME FINAL - *CONSULTORÍA PARA EL DIAGNÓSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC" (HACKING ÉTICO)*

3 Julio 2023

ROBERTO INSFRAN

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución al Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

Histórico de Versiones

Fecha	Versión	Modificación	Realizado por
	1.0	Versión Inicial Remitida al MEC	Equipo Grupo Horus

Tabla de contenido

1 Antecedentes 4
2 Metodología de trabajo 4
3 Resumen de Actividades y Entregables 5
3.1 Producto 2: Estado de Madurez con Respecto a la Ciberseguridad GAP Análisis CIS Control 5
3.1.1 Beneficios Controles Críticos de Ciberseguridad 7
3.1.2 Principales Resultados 8
3.2 Producto 3: Informe de Seguridad hallazgos y evidencias de los Sistemas Transaccionales de Gestión e Información del MEC 14
3.2.1 Análisis de Vulnerabilidades – Sistemas Externos 14
3.2.2 Análisis de Vulnerabilidades – Sistemas Internos 16
4 Recomendaciones Generales 20
5 Conclusiones 22
6 ANEXO 1 – Vulnerabilidades Sitos Externos – Recomendaciones 24
6.1 SISTEMA "A" 24
6.2 SISTEMA B 26
6.3 Sistema C 28
6.4 Sistema D 29
6.5 Sistema E 30
6.6 Sistema F 31
6.7 Sistema G 32
6.8 Sistema H 33
6.9 Sistema I 34
6.10 Sistema J 34

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

JOSE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

6.11 Sistema K 35

6.11.1 1. Default Tomcat User and Password (apache-tomcat-default-password) 37

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

ROBERTO INSFRAN

GRUPO HORUS

GRUPO HORUS S.A.

1 Antecedentes

La Consultoría fue realizada por un equipo de profesionales multidisciplinarios, quienes poseen conocimiento, entrenamiento y experiencia probadas en el ámbito de las TIC.

El objetivo del **GAP ANÁLISIS de Controles Críticos de Ciberseguridad** es evaluar la madurez de los sistemas con respecto a las buenas prácticas en materias de ciberseguridad.

Ante la aprobación del cronograma propuesto por parte de HORUS S.A., se procedió a clasificar los mejores perfiles para llevar adelante el trabajo. A modo de lograr los objetivos propuestos.

La presente documentación con sus anexos, abarca no sólo el análisis de la situación actual de la institución desde sus distintos ámbitos, sino también el análisis y diseño de soluciones tecnológicas previendo el soporte y la operativa en base a las nuevas normativas que rigen RESOLUCIÓN MITIC Nº 277-2020, para el cumplimiento de sus funciones.

Poniendo énfasis en que no es objeto de la presente consultoría la estimación de tiempos, costos ni esfuerzos para la implementación de las propuestas y en que, al momento de la eventual aplicación de las recomendaciones dadas en los documentos técnicos:

1. **PRODUCTO 2 GAP ANÁLISIS** – Gap Análisis.
2. **MEC ANALISIS_EXTERNO_002** – Análisis de Vulnerabilidades Externas.
3. **MEC ANALISIS_INTERNO_003** – Análisis de Vulnerabilidades Internas.

El **Ministerio de Educación y Ciencias** (MEC) deberá indefectiblemente realizar los ajustes que considere necesarios de acuerdo con las normas y funciones que se encuentren vigentes.

2 Metodología de trabajo

El equipo de trabajo optó por realizar los trabajos de forma híbrida (presencial y remoto), procedió a relevar y analizar documentación y comprobar información de acceso Público sobre el Ministerio de Educación y Ciencia (MEC).

Se identificaron y coordinaron reuniones de trabajo con personal clave del Ministerio de Educación y Ciencias (MEC) del área de TI.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.

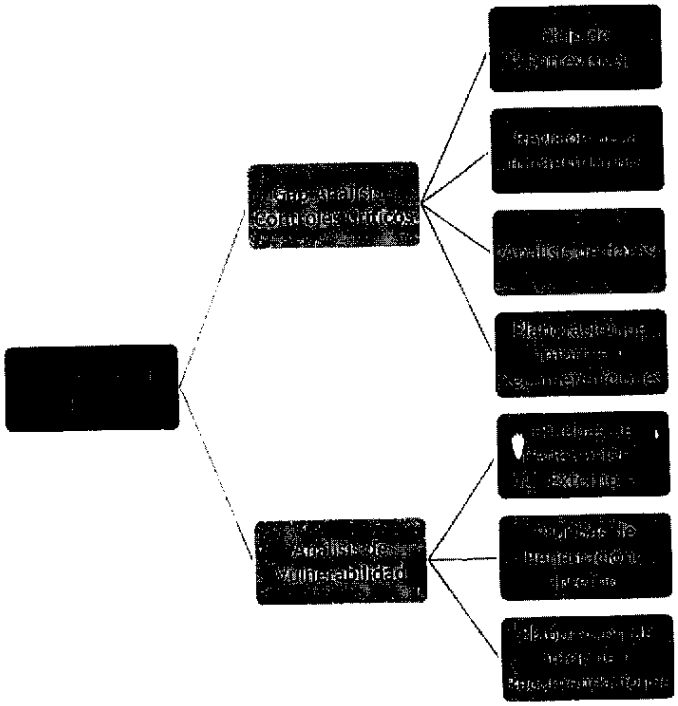


Ilustración 1 - Metodología de Trabajo

Se procedió a realizar una reunión de exposición de descubrimientos y avances documentales al director, donde se validaron aspectos del trabajo y se ajustaron los detalles a considerar dentro del informe final.

Por último, el equipo de consultores sugiere a modo de recomendaciones técnicas los aspectos a ser tenidos en cuenta por el Ministerio de Educación y Ciencia (MEC) en los componentes de infraestructura de redes, sistemas, seguridad y de recursos humanos técnicos especializados en caso de considerar la implementación de estas.

3 Resumen de Actividades y Entregables

3.1 Producto 2: Estado de Madurez con Respecto a la Ciberseguridad GAP Análisis CIS Control

La actividad de Controles Críticos de Ciberseguridad nos permitió identificar las brechas y debilidades en la gestión de la seguridad de la información de la MEC, respecto al cumplimiento de normas estándares de seguridad de la información.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

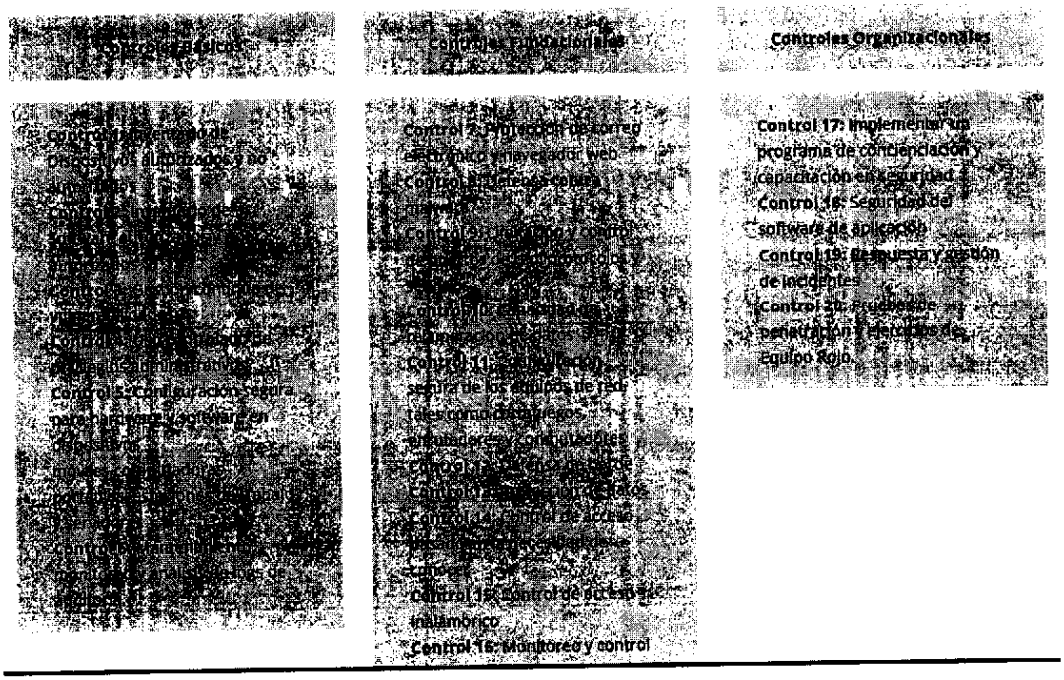
GRUPO HORUS
GRUPO HORUS S.A.

La implementación de medidas preventivas de seguridad, suponen que las organizaciones deben ejecutar acciones claras para la protección de sus datos. Se debe recordar que la información es uno de los activos a proteger de todas sus formas.

El trabajo realizado se basó principalmente en los siguientes estándares:

- Resolución MITIC N 277/-2020 siguiendo la Estrategia del Plan Nacional de Ciberseguridad.
- **Controles |Criticos de Ciberseguridad "CIS Critical Security Controls V7.1".** Los controles CIS son un conjunto recomendado de acciones de ciberseguridad que brindan acciones específicas para prevenir los ataques más conocidos.

Siguiendo la metodología CIS Control en su versión v7.1. Se procedió a realizar la evaluación según el Estándar de Controles Críticos de Ciberseguridad. En este estándar los controles de Ciberseguridad se agrupan en 3 dominios principales.

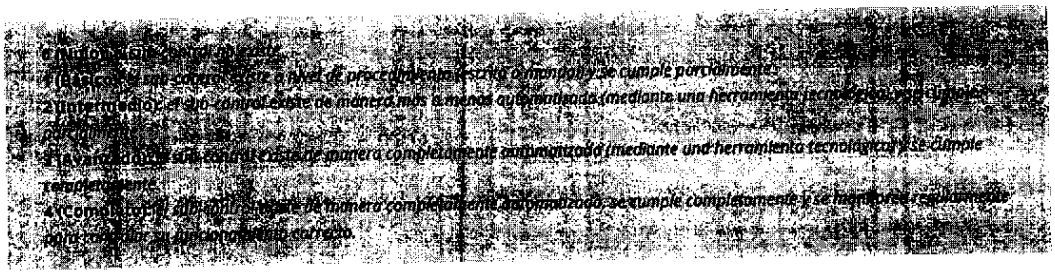


En el marco de la Evaluación se procedió a identificar de manera cualitativa el grado de implementación de cada subcontrol según la siguiente escala:

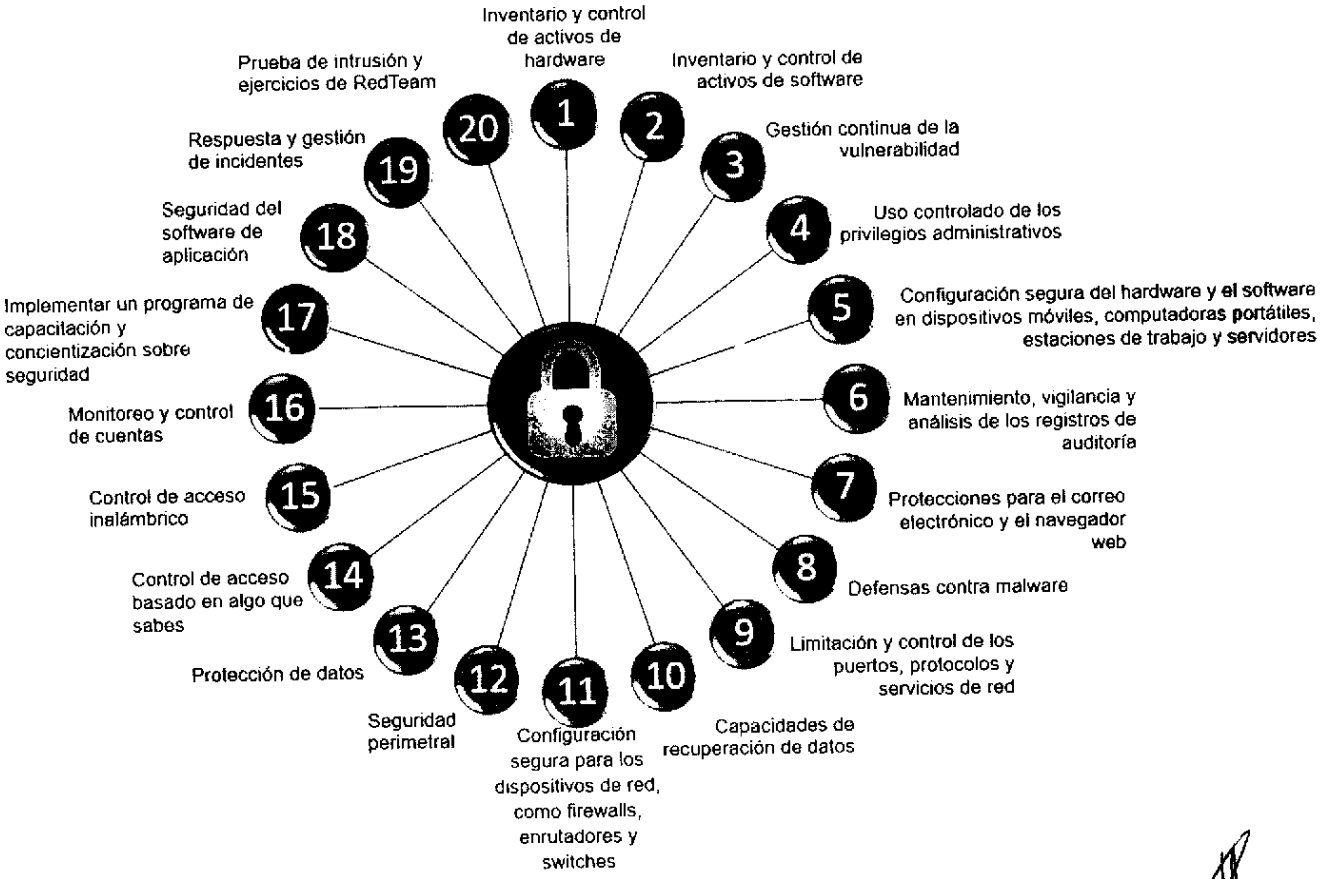
ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.



En el marco del entregable 2 se procedió a la entrega detallada del informe que contiene el resultado encontrado según la metodología de los Controles Críticos de Ciberseguridad. Se ha realizado la evaluación en los 20 controles definidos según la metodología.



3.1.1 Beneficios Controles Críticos de Ciberseguridad

Los análisis GAP suponen una importante inversión, pero a su vez, son una

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.

herramienta muy poderosa para conocer el estado de la Seguridad o identificar sus puntos débiles. Algunas de las ventajas que ofrecen son las siguientes:

- Permite evaluar la situación actual de la organización y detectar aquellos fallos o deficiencias que impiden llegar al estado objetivo o deseado.
- Identifica los riesgos asociados a los procesos realizados en la organización.
- Determina las necesidades de la organización para subsanar sus deficiencias y adaptarse a los estándares que marcan las normativas o estándares de seguridad.
- Crea una base sólida que permite iniciar una planificación eficiente para alcanzar las metas propuestas.

3.1.2 Principales Resultados

En líneas generales se observa un nivel de cumplimiento que requiere de atención a nivel de equipo técnico del MEC en función del bajo cumplimiento obtenido. De un total de 2880 ítems de control y subcontroles, el MEC a logrado tener algún nivel de cumplimiento en 40 de ellos. Esto significa que el nivel de cumplimiento según los Controles Críticos de Ciberseguridad en el MEC llega a 1,39%.

Se observa un nivel de madurez **BAJO** con respecto a ciberseguridad en la Institución.

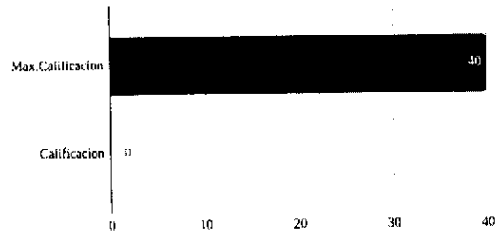
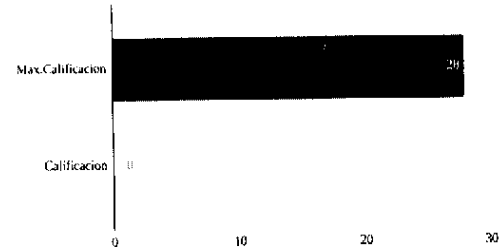
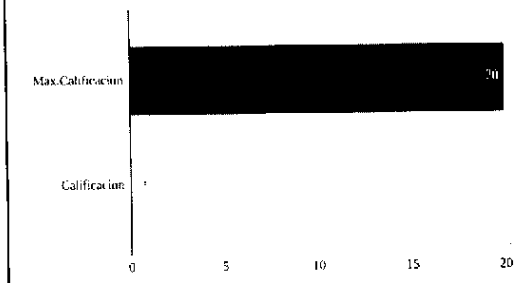
En esta sección detallaremos el estado de las medidas de seguridad aplicadas a la Institución. Si bien lo indicado representa el estado en que se encontró, algunos puntos se han tomado medidas por parte de la Dirección.

A continuación, un resumen de los resultados por los 20 controles evaluados:

Control Realizado	Nivel de Cumplimiento

ROBERTO INSFRAN

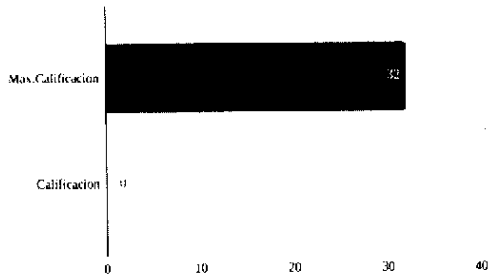
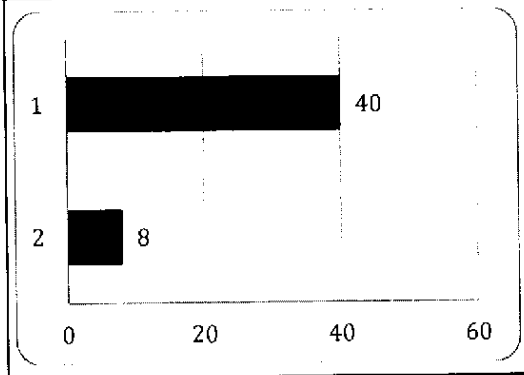
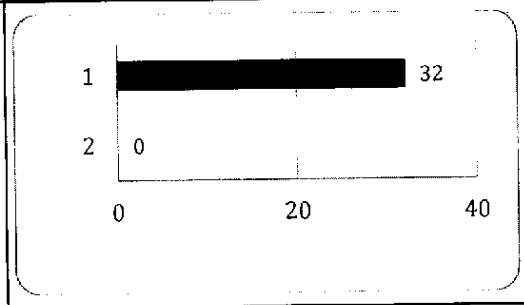
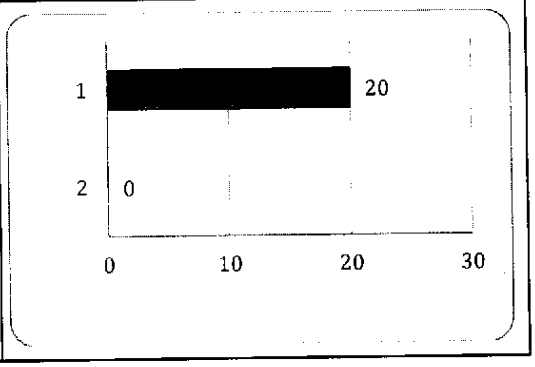
Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

CIS 1 | Inventario de dispositivos autorizados y no autorizados.	
CIS 2 | Inventario de Software autorizados y no autorizados.	
CIS 3 | Gestión continua de vulnerabilidades.	
CIS 4 | Uso controlado de privilegios administrativos.	
CIS 5 | Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores.	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

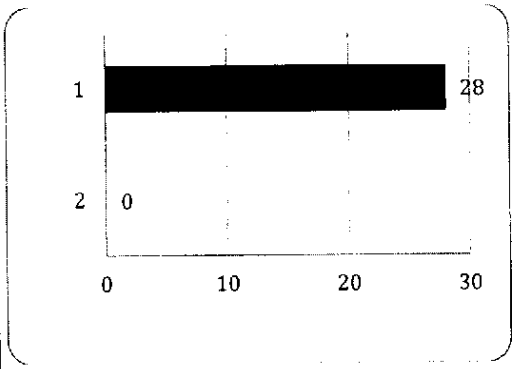
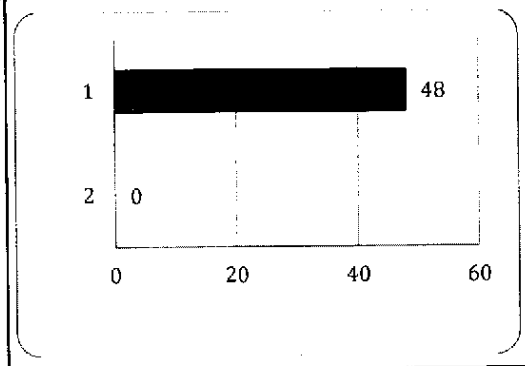
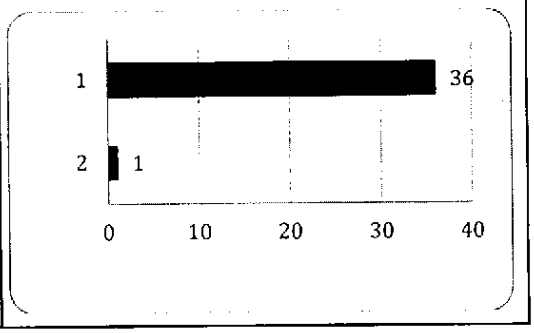
GRUPO HORUS
GRUPO HORUS S.A.

CIS 6 | Mantenimiento, monitoreo y análisis de logs de auditoría.	
CIS 7 | Protecciones de correo electrónico y navegador web.	
CIS 8 | Defensa contra malware	
CIS 9 | Limitación y control de puertos de red, protocolos y servicios	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

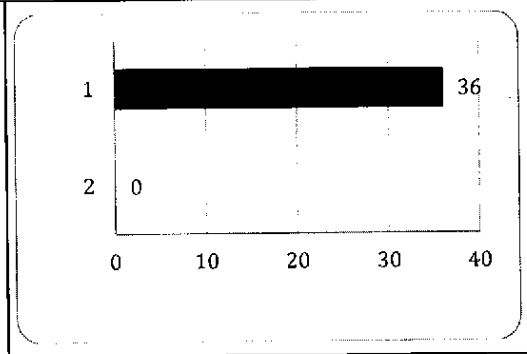
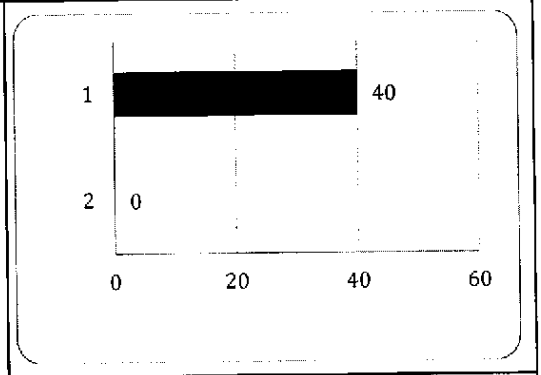
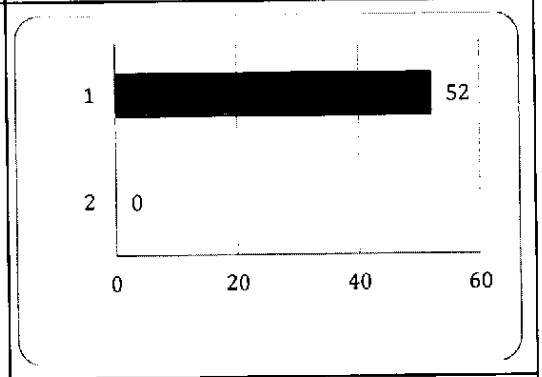
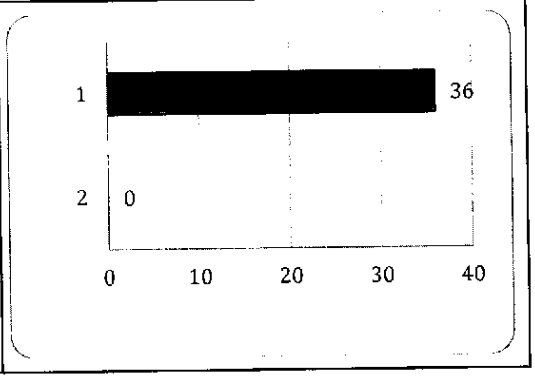
GRUPO HORUS
GRUPO HORUS S.A.

CIS 10 | Capacidad de recuperación de datos	
CIS 11 | Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	
CIS 12 | Defensa de borde	
CIS 13 | Protección de datos	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizado por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

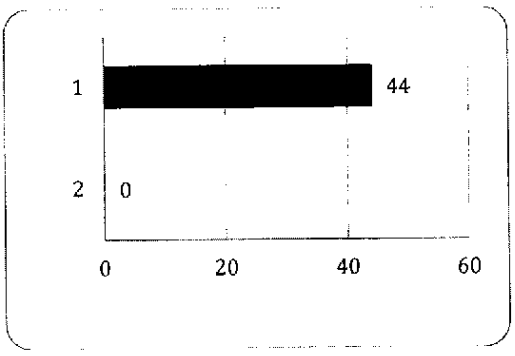
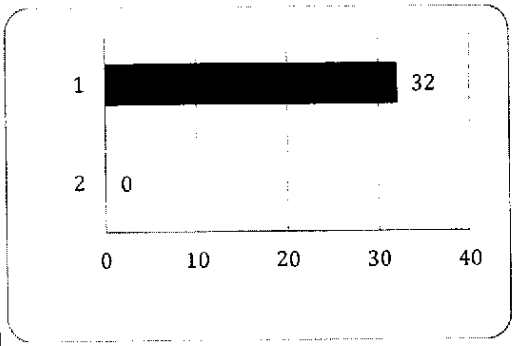
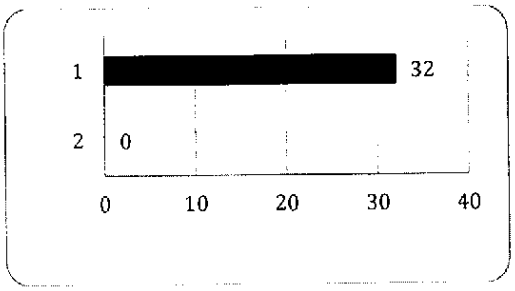
GRUPO HORUS
GRUPO HORUS S.A.

CIS 14 | Control de acceso basado en la necesidad de conocer	
CIS 15 | Control de acceso inalámbrico	
CIS 16 | Monitoreo y control de cuentas	
CIS 17 | Implementar un programa de concienciación y entrenamiento de seguridad	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizado por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.

CIS 18 | Seguridad del software de aplicación	
CIS 19 | Respuesta y manejo de incidentes	
CIS 20 | Pruebas de penetración y ejercicios de equipo rojo	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
13
GRUPO HORUS S.A.

3.2 Producto 3: Informe de Seguridad hallazgos y evidencias de los Sistemas Transaccionales de Gestión e Información del MEC

3.2.1 Análisis de Vulnerabilidades – Sistemas Externos

Se han realizado consultas y análisis para identificación de brechas de seguridad de la información sobre los dominios:

1. https://rue.mec.gov.py/
2. https://intramec.mec.gov.py/
3. https://intramec.mec.gov.py/sies
4. https://tramites.mec.gov.py/
5. https://sigmec.mec.gov.py/
6. https://atenea.mec.gov.py/
7. https://datos.mec.gov.py/
8. https://mapaescolar.mec.gov.py/
9. https://tapmec.mec.gov.py/
10. https://aprendizaje.mec.edu.py/

La modalidad utilizada para la realización de las pruebas fue del tipo *caja negra.*

Adicionalmente se realizaron pruebas de identificación de brechas de manera interna, desde la red interna del.

El detalle técnico se encuentra en el documento **MEC ANALISIS_EXTERNO_002.**

En base a la cantidad de vulnerabilidades encontradas, sólo se enumeran las que fueron posibles sus pruebas de concepto (PoC).
Para catalogar las vulnerabilidades se ha utilizado catálogos de vulnerabilidades como CVE (Common Vulnerabilities Enumeration) y CWE (Common Weakness Enumeration) para tener un análisis más acabado de la situación ya que CVE trata los síntomas mientras que el CWE trata una causa. Si el CWE clasifica los tipos de vulnerabilidades de software, el CVE es simplemente una lista de problemas conocidos actualmente con respecto a sistemas y productos específicos.

El presente cuadro refleja las vulnerabilidades encontradas con su correspondiente descripción, tipo y severidad de vulnerabilidades encontradas.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución del Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

ROBERTO INSFRAN

GRUPO HORUS
GRUPO HORUS S.A.

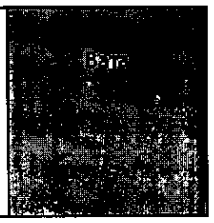
Nota : Por cuestiones de seguridad de la información y confidencialidad, la información detallada del servicio afectado, IP, evidencias no se incorporan en el presente informe. No obstante, los mismos fueron proveídos al equipo técnico del MEC definido como punto focal para el proyecto.

Clasificación	Descripción de la Vulnerabilidad	CVE/s-CWE/s	Severidad Identificada
Denegación de Servicio	Se aprovecha una vulnerabilidad identificada como Buffer Overflow en servicios de apache HTTP Server. Mediante el envío de cuerpos de respuesta mediante la técnica del "slowloris". Se envían peticiones POST con la cabecera HTTP completa e incluyendo un "Content-Length" con el tamaño en bytes del POST DATA a enviar. Provocando que la pila de peticiones de conexión sea llenada evitando que peticiones validas sean concretadas.	**Apache HTTP Server Buffer Overflow Vulnerability (CVE-2021-44790)**	Alta
Seguridad de la Información	Cross-site scripting (XSS) es un ataque en el que un atacante inyecta scripts ejecutables maliciosos en el código de una aplicación o sitio web de confianza. Los atacantes a menudo inician un ataque XSS enviando un enlace malicioso a un usuario e incitándolo a hacer clic en él. Si la aplicación o el sitio web carecen de una desinfección de datos adecuada, el enlace malicioso ejecuta el código elegido por el atacante en el sistema del usuario. Como resultado, el atacante puede robar la cookie de sesión activa del usuario.	**Cross-Site Scripting**	[redacted]
Servicio Obsoleto	La aplicación web utiliza una biblioteca de JavaScript que se sabe que contiene al menos una vulnerabilidad.	**Use of JavaScript Library with Known Vulnerability**	[redacted]
Seguridad de la Información	La acción predeterminada del formulario de inicio de sesión contiene un enlace que no se envía a través de HTTPS (HTTP sobre SSL).	**Login Form Is Not Submitted Via HTTPS**	[redacted]
Daño Corporativo	Con el secuestro de clics, un atacante puede engañar a un usuario víctima para que haga clic en un marco invisible en la página web, lo que hace que la víctima realice una acción que no tenía intención de realizar.	**Clickjacking - Framable Page**	[redacted]
Seguridad de la Información	La cookie de sesión configurada a través de una conexión que no es HTTPS puede provocar un ataque Man in the Middle y los datos de la cookie pueden ser robados.	**Session Cookie Set over Non-HTTPS Connection**	[redacted]

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
15
GRUPO HORUS S.A.

ROBERTO INSFRAN

Seguridad de la Información	La presencia de un directorio navegable no implica necesariamente una vulnerabilidad. Determine si la lista del directorio está destinada a mostrarse. Verifique que ningún archivo en el directorio contenga contenido que la aplicación web no deba servir.	**Path Disclosure** **Directory Listing**	

En el ANEXO 1 – se presentan las recomendaciones por tipo de vulnerabilidad.

3.2.2 Análisis de Vulnerabilidades – Sistemas Internos

Para catalogar las vulnerabilidades se ha utilizado catálogos de medidas de Riesgo según indica CVE (Common Vulnerabilities Enumeration)

Se clasifican los tipos de vulnerabilidades según puntuación de RIESGO de 1 a 1.000, siendo 1.000 el riesgo más elevado.

En la metodología de análisis de vulnerabilidad se ha procedido a realizar un análisis de la red interna en los cuales se identificaron 767 servicios: Conforme tabla a continuación:

Tipo de Servicio	Cantidad de Nodos
SSH	317
HTTP	308
HTTPS	254
portmapper	223
Estado	102
NFS lockd	82
mDNS	61
SNMP	49
Postgres	44
DCE RPC	43

En base a los servicios encontrados se procedió el análisis de vulnerabilidades el cual arrojo más 7.000 potenciales vulnerabilidades. La modalidad utilizada para la realización de las pruebas fue del tipo *caja negra*.

Se procedió a realizar la valoración del riesgo asociado a cada vulnerabilidad y a partir de la misma se obtuvo la lista de las 10 principales vulnerabilidades que representan un mayor riesgo a efectos de ciberseguridad. La lista detalla de

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

JORGE TOMPERLEY
GRUPO HORUS
GRUPO HORUS S.R.

vulnerabilidades se hizo entrega conjuntamente con el informe 3. Y a continuación se lista las 10 principales vulnerabilidades identificadas y las recomendaciones pertinentes para su tratamiento.

Nota: A efectos de mejor identificación en lo repositorio de ciberseguridad (CVE – CWE, Bugtrack, etc) se mantiene el titulo de la vulnerabilidad en inglés.

Nota 2: Por cuestiones de seguridad de la información, la información detallada del servicio afectado, IP, evidencias no se incorporan en el presente informe. No obstante, los mismos fueron disponibilizados al equipo técnico del MEC definido como punto focal para el proyecto.

1. Default Tomcat User and Password (apache-tomcat-default-password)

Nodo Afectados: 1	Información Adicional: Existencia de Exploit	Estado ACTIVO

Cambie la contraseña de la cuenta del administrador del servicio de Tomcat.

El servicio Tomcat tiene una cuenta de administrador establecida en una configuración predeterminada. Esto se puede cambiar en conf/tomcat-users.xml

Esto solucionará el siguiente problema: usuario y contraseña predeterminados de Tomcat (apache-tomcat-default-password).

2. Postgres default account: postgres/no password

Nodo Afectados: 7	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Establezca una contraseña para la cuenta 'postgres'. Esto generalmente se hace editando el archivo 'pg_hba.conf'

Esto solucionará el siguiente problema: Cuenta predeterminada de Postgres: postgres/sin contraseña (postgres-default-account-postgres-nopassword).

Restringir el acceso a la base de datos

Configure el servidor de la base de datos para que solo permita el acceso a sistemas de confianza. Por ejemplo, el estándar PCI DSS requiere que coloque la base de datos en una zona de red interna, separada de la DMZ

Esto solucionará el siguiente problema: Acceso abierto a la base de datos (acceso abierto a la base de datos).

3. Samba RPC unauthenticated remote code execution (CVE-2012-1182)

Nodo Afectados: 2	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Estas vulnerabilidades se pueden resolver realizando los siguientes 3 pasos.

1. Actualizar a la última versión de Samba
2. Alternativamente, los parches pueden estar disponibles en http://www.samba.org/samba/history/security.html.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
17
GRUPO HORUS S.A.

3. Se recomienda que utilice el administrador de paquetes de su sistema operativo para actualizar si es posible.

Adicionalmente configurar la firma SMB para Samba

Configure Samba para habilitar o requerir la firma SMB según corresponda. Para habilitar la firma SMB, coloque lo siguiente en Samba

archivo de configuración, la configuración default se encuentra en smb.conf, en la sección global:

firma del servidor = auto

Para solicitar la firma SMB, cambiel:

firma del servidor = obligatorio

4. PHP Vulnerability: CVE-2015-0235

Nodo Afectados: 50	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Estas vulnerabilidades se pueden resolver realizando los siguientes pasos.

Actualice a la última versión de PHP

Descargue y aplique la actualización desde: http://www.php.net/downloads.php
La última versión de PHP es 8.2.3
Esto indirectamente resolverá 1,136 problemas:

5. Apache Tomcat: Important: Remote Code Execution on Windows (CVE-2019-0232)

Nodo Afectados: 12	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Actualice a la última versión de Apache Tomcat

Descargue y aplique la actualización desde: http://archive.apache.org/dist/tomcat/tomcat-10/v10.1.9/

La última versión de Apache Tomcat es 10.1

Esto indirectamente resolverá 71 problemas:

6. Webmin: Unauthenticated Remote Code Execution

Nodo Afectados: 21	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Actualizar a la última versión de Webmin

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
18
GRUPO HORUS S.A.

Descargue y aplique la actualización desde: https://sourceforge.net/projects/webadmin/files/webmin/

Actualice a la última versión de Webmin.
Esto solucionará el siguiente problema: CVE-2019-15107: Webmin: Ejecución de código remoto no autenticado (http-webmin-cve-2019-15107).

7. PostgreSQL class A vulnerability in core server: CVE-2013-1899

Nodo Afectados: 21	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Estas vulnerabilidades se pueden resolver con un solo paso.

Actualice a la última versión de PostgreSQL

Descargue y aplique la actualización desde: http://www.postgresql.org/download/

8. HTTP TRACE Method Enabled

Nodo Afectados: 104	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Deshabilitar el método HTTP TRACE para Apache
Apache HTTPD, Apache Tomcat
Las versiones más recientes de Apache (1.3.34 y 2.0.55 y posteriores) proporcionan una directiva de configuración llamada TraceEnable. Para denegar solicitudes, agregue la siguiente línea a la configuración del servidor:

```
TraceEnable off
```

Para versiones anteriores del servidor web Apache, use el módulo mod_rewrite para denegar las solicitudes TRACE:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

En Apache Tomcat, HTTP Trace se puede deshabilitar agregando restricciones de seguridad en la especificación de Java Servlet dentro del archivo de configuración web.xml y estableciendo el atributo allowTrace="False" en el conector HTTP en server.xml.

9. Apache Tomcat: Important: Remote Code Execution (CVE-2017-12617)

Nodo Afectados: 104	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

Actualice a la última versión de Apache Tomcat

Descargue y aplique la actualización desde: http://archive.apache.org/dist/tomcat/tomcat-10/v10.1.9/

La última versión de Apache Tomcat es 10.1.9

10. Default SSH password: admin password "admin"

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
19
GRUPO HORUS S.A.

Nodo Afectados: 5	Informacion Adicional: Existencia de Exploit	Estado ACTIVO

El detalle técnico se encuentra en el documento **MEC ANALISIS_INTERNO_003.**

4 Recomendaciones Generales

En base a los resultados del Producto 2 y Proucto 3, se presentan las siguientes recomendaciones Generales. Es importante observar que las recomendaciones específicas y detalladas se presentan en cada produto. A continuación, se presentan los "Quick Wins":

Recomendación 1 – Organización y Estructura del Equipo

En base a las entrevistas, cantidad de activos y tamaño de la red, se observa una necesidad de reforzar la organización del equipo, principalmente en lo que respecta a la cantidad de personas que actúan en actividades de soporte de infraestructura, sistemas y ciberseguridad.

En tal sentido, se recomienda la designación de una persona que tenga responsabilidad de gestión en lo que respecta a la Seguridad de la Información. Por lo general, se recomienda que el director general de TIC también desempeñe el rol de Responsable de Ciberseguridad. Para tal efecto, existen orientaciones por parte del CERT-PY y el MITIC en lo que respecta al rol que deberá desempeñar este cargo.

Recomendación 2 – Actualización de los Servidores WEB - Apache

Las principales incidencias de vulnerabildiades de aplicaciones externas están dadas en función del versiones desatendidas de software. En este sentido, se recomienda como una recomendación imporatne la actualización de versión a la última estable disponible y el ajuste de parámetros de los servidores web en conjunto con su sistema operativo, a fin de lograr mejoras en cuanto a rendimiento y seguridad.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
20
GRUPO HORUS S.A.

Recomendación 3 – Implementar un sistema de Inventario de Activos:

1. **Inventario de Activos**
    a. Registre todos los activos de la organización.
    b. Existen herramientas tanto opensource como privadas.
    c. Mantener la lista actualizada.

Recomendación 4 – Implementación de Lista Blanca de Aplicaciones Confiables.

2. **Listas blancas de aplicaciones**
    a. La lista blanca de aplicaciones consiste en crear una lista de aplicaciones confiables y permitir que solo esas aplicaciones se ejecuten en los dispositivos gestionados.
    b. Existen herramientas tanto open source como privadas.
    c. Acciones establecer políticas y herramientas dentro de la MEC.
    d. Controles (acta de recepción del equipo, aceptación de uso)

Recomendación 5 – Utilización de Estándares de Seguridad para Configuraciones Seguras

3. **Uso de estándares, configuraciones seguras**
    a. Establecer configuraciones seguras basadas en estándares de seguridad.
    b. Mantenga estándares de configuración de seguridad estándar documentados para todos los sistemas operativos y software autorizados.
    c. Guia y manuales https://ncp.nist.gov/repository
    d. Se recomienda principal atención a los siguientes puntos:
        i. Implementación de Active Directory
        ii. Segmentación y Unificación de Redes Corporativas
        iii. Hardening de Sistemas Operaciones de Producción

Recomendación 6 – Automatización y Gestión de Parches de Seguridad

4. **Aplicar parches** dentro de 48 horas en el software del sistema.
    a. Implementar herramientas de gestión automatizada de parches del sistema operativo WSUS o Windows Server Update Services es una función más dentro del catálogo de roles disponible en Windows Server 2008 o superior.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

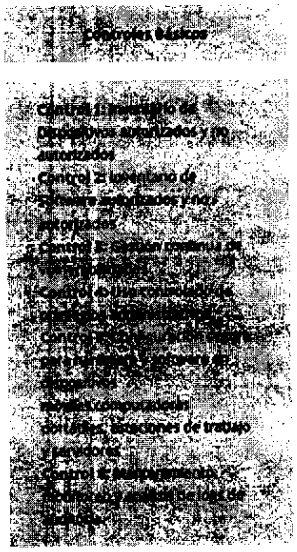
Recomendación 7 – Limitar Usuarios con Privilegios Administrativos

5. **Número reducido de usuarios con privilegios administrativos**
    a. Asegurar el uso de cuentas administrativas dedicadas
    b. Implemente herramientas

5 Conclusiones

Los trabajos se llevaron a cabo de forma satisfactoria. Con la autorización por parte de MEC se pudieron ejecutar los trabajos de escaneos y pruebas controladas para la recolección de datos que sirvieron de insumo para generar los entregables correspondientes.

En líneas generales, se observa un nivel de madurez en lo que respecta a Seguridad de la Información del tipo incipiente: en la cual aún se necesitan implementar el dominio conocido como "Controles Básicos" de Ciberseguridad. Mediante la implementación de los Controles Básicos se podrá obtener un aumento en el nivel de exposición y mejoría del nivel de ciberseguridad de manera considerable:



La implementación de los controles básicos no necesariamente implican en un aumento en la inversión o mayores costos en lo que respecta a software o

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

infraestructura teniendo en cuenta que una gran cantidad de mejorías se puede dar mediante la actualización de versiones de software, la implementación de herramientas del tipo "Open Source" de costo gratuito o la definición e implementación de políticas de seguridad a nivel institucional.

En lo que respecta a la exposición de los sistemas del MEC a ataques, se observa un nivel de exposición externo moderado. Desde ataques originados de sitios externos (internet) se observa como principal vulnerabilidad existente en la red los ataques del tipo denegación de servicio (o sea, indisponibilización del servicio) ya que fueron identificadas vulnerabilidades en los servicios que poseen este tipo de vulnerabilidades activas.

En lo que respecta a vulnerabilidades que puedan ser exploradas desde la red interna del MEC, se observa un riesgo de exposición a vulnerabilidades de ALTO a CRÍTICO. Esto se debe a que se identificaron vulnerabilidades en la red interna que traen riesgos a la red del tipo:

- Acceso con permisos privilegiados de administrador a Bases de Datos
- Usuarios y Contraseñas por defecto a servicios del TIPO SSH y servidores de aplicaciones.
- Vulnerabilidades en los servicios que permiten la exploración de vulnerabilidades como: Escalación de Privilegios, ejecución de código remoto.

Esto conlleva a que, exista un riesgo inminente a la exploración de vulnerabilidades en la red interna que conlleven a situaciones como:

- Robo y Secuestro de Información
- Instalación y ejecución de "Ransonware"
- *Defacement* o adulteración de Sitios o Páginas WEB

Roberto Insfrán
Especialistas en Ciberseguridad

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

6 ANEXO 1 – Vulnerabilidades Sitos Externos – Recomendaciones

Nota : Por cuestiones de seguridad de la información y confidencialidad, la información detallada del servicio afectado, IP, evidencias no se incorporan en el presente informe. No obstante, los mismos fueron proveídos al equipo técnico del MEC definido como punto focal para el proyecto.

6.1 SISTEMA "A"

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. DENY, que prohíbe mostrar la página dentro de un marco SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	
2. Vulnerabilidad	**Web Server Information Disclosure:** La aplicación de destino revela la versión del software del servidor web a través del token "Servidor:" enviado en el encabezado de respuesta HTTP.
Recomendaciones	
Content Security Policy	Los contenidos activos en páginas web, como por ejemplo JavaScript, CSS o ActiveX, plantean riesgos de seguridad para los usuarios de Internet y los gestores de páginas web y pueden manipularse. Para que las páginas de Internet puedan utilizarse sin

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

	preocupaciones, existe lo que se conoce como Content Security Policy (CSP), cuyo papel consiste en proteger a las páginas frente a ataques perjudiciales y es compatible con la mayoría de navegadores web.
Ejemplos de CSP: 1. script-src "https://example.com:443" – Solo se permiten scripts de este dominio por HTTPS. 2. script-src 'none' – No se pueden cargar scripts. 3. script-src 'self' – Solo pueden cargarse scripts que tengan el mismo origen que la página actual, pero no el de los subdominios. 4. script-src https: – Se pueden cargar scripts de cualquier dominio siempre que empiecen por HTTPS. 5. script-src example.com – Se pueden cargar scripts de este dominio. 6. script-src *.example.com – Se permiten scripts de este y de todos los dominios. 7. img-src data: – Pueden cargarse imágenes por medio de enlaces de datos.	
3. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (version actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar Actualizar apache server	
4. Vulnerabilidad	**Use of JavaScript Library with Known Vulnerability:** La aplicación web utiliza una biblioteca de JavaScript que se sabe que contiene al menos una vulnerabilidad.
Recomendaciones	
Update Librerías	Se recomienda la actualización de las dependencias y librerías instaladas.
Debe existir un proceso de administración de parches para: • Eliminar las dependencias no utilizadas, las funciones, los componentes, los archivos y la documentación innecesarios.	

ROBERTO MISFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

- Haga un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, marcos, bibliotecas) y sus dependencias utilizando herramientas como versiones, OWASP Dependency Check, retire.js, etc. Monitoree continuamente fuentes como Common Vulnerability and Exposures (CVE) y National Vulnerability Database (NVD) para detectar vulnerabilidades en los componentes.
- Solo obtenga componentes de fuentes oficiales a través de enlaces seguros. Prefiera los paquetes firmados para reducir la posibilidad de incluir un componente malicioso modificado.
- Supervise las bibliotecas y los componentes que no reciben mantenimiento o que no crean parches de seguridad para versiones anteriores. Si no es posible aplicar parches, considere implementar un parche virtual para monitorear, detectar o proteger contra el problema descubierto.
- Cada organización debe garantizar un plan continuo para monitorear, clasificar y aplicar actualizaciones o cambios de configuración durante la vida útil de la aplicación o cartera.

6.2 SISTEMA B

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. DENY, que prohíbe mostrar la página dentro de un marco SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

2. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:

Deshabilitar el informe de errores:

error_reporting(0);

Ocultar mensajes de error:

display_errors(0);

3. Vulnerabilidad	**Use of JavaScript Library with Known Vulnerability:** La aplicación web utiliza una biblioteca de JavaScript que se sabe que contiene al menos una vulnerabilidad.
Recomendaciones	
Update Librerías	Se recomienda la actualización de las dependencias y librerías instaladas.

Debe existir un proceso de administración de parches para:

- Eliminar las dependencias no utilizadas, las funciones, los componentes, los archivos y la documentación innecesarios.
- Haga un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, marcos, bibliotecas) y sus dependencias utilizando herramientas como versiones, OWASP Dependency Check, retire.js, etc. Monitoree continuamente fuentes como Common Vulnerability and Exposures (CVE) y National Vulnerability Database (NVD) para detectar vulnerabilidades en los componentes.
- Solo obtenga componentes de fuentes oficiales a través de enlaces seguros. Prefiera los paquetes firmados para reducir la posibilidad de incluir un componente malicioso modificado.
- Supervise las bibliotecas y los componentes que no reciben mantenimiento o que no crean parches de seguridad para versiones anteriores. Si no es posible aplicar parches, considere implementar un parche virtual para monitorear, detectar o proteger contra el problema descubierto.
- Cada organización debe garantizar un plan continuo para monitorear, clasificar y aplicar actualizaciones o cambios de configuración durante la vida útil de la aplicación o cartera.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

6.3 Sistema C

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. DENY, que prohíbe mostrar la página dentro de un marco SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	
2. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.
La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para: Deshabilitar el informe de errores:	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

error_reporting(0);
Ocultar mensajes de error:
display_errors(0);

6.4 Sistema D

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

6.5 Sistema E

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
30
GRUPO HORUS S.A.

Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

6.6 Sistema F

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. DENY, que prohíbe mostrar la página dentro de un marco SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	
2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

	En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

6.7 Sistema G

1. Vulnerabilidad	**Cross-Site Scripting**: la aplicación web refleja caracteres potencialmente peligrosos, como comillas simples, comillas dobles y corchetes angulares. Estos caracteres se usan comúnmente para ataques de inyección de HTML, como secuencias de comandos entre sitios (XSS).
Recomendaciones	
Content Security Policy	Los contenidos activos en páginas web, como por ejemplo JavaScript, CSS o ActiveX, plantean riesgos de seguridad para los usuarios de Internet y los gestores de páginas web y pueden manipularse. Para que las páginas de Internet puedan utilizarse sin preocupaciones, existe lo que se conoce como Content Security Policy (CSP), cuyo papel consiste en proteger a las páginas frente a ataques perjudiciales y es compatible con la mayoría de navegadores web.
Ejemplos de CSP: 1. script-src "https://example.com:443" – Solo se permiten scripts de este dominio por HTTPS. 2. script-src 'none' – No se pueden cargar scripts. 3. script-src 'self' – Solo pueden cargarse scripts que tengan el mismo origen que la página actual, pero no el de los subdominios. 4. script-src https: – Se pueden cargar scripts de cualquier dominio siempre que empiecen por HTTPS. 5. script-src example.com – Se pueden cargar scripts de este dominio. 6. script-src *.example.com – Se permiten scripts de este y de todos los dominios. 7. img-src data: – Pueden cargarse imágenes por medio de enlaces de datos.	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.R.

2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

6.8 Sistema H

1. Vulnerabilidad	**Use of JavaScript Library with Known Vulnerability:** La aplicación web utiliza una biblioteca de JavaScript que se sabe que contiene al menos una vulnerabilidad.
Recomendaciones	
Update Librerías	Se recomienda la actualización de las dependencias y librerías instaladas.
Debe existir un proceso de administración de parches para: • Eliminar las dependencias no utilizadas, las funciones, los componentes, los archivos y la documentación innecesarios. • Haga un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, marcos, bibliotecas) y sus dependencias utilizando herramientas como versiones, OWASP Dependency Check, retire.js, etc. Monitoree continuamente fuentes como Common Vulnerability and Exposures (CVE) y National Vulnerability Database (NVD) para detectar vulnerabilidades en los componentes. • Solo obtenga componentes de fuentes oficiales a través de enlaces seguros. Prefiera los paquetes firmados para reducir la posibilidad de incluir un componente malicioso modificado. • Supervise las bibliotecas y los componentes que no reciben mantenimiento o que no crean parches de seguridad para versiones anteriores. Si no es posible aplicar parches, considere implementar un parche virtual para monitorear, detectar o proteger contra el problema descubierto. • Cada organización debe garantizar un plan continuo para monitorear, clasificar y aplicar actualizaciones o cambios de configuración durante la vida útil de la aplicación o cartera.	

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HOPUS S.A.

6.9 Sistema I

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. DENY, que prohíbe mostrar la página dentro de un marco SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	

6.10 Sistema J

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL)

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

	para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

6.11 Sistema K

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

1. Vulnerabilidad	**WordPress XML-RPC Pingback Vulnerability:** XML-RPC es una característica de WordPress que permite que los datos se transmitan, con HTTP actuando como el mecanismo de transporte y XML como el mecanismo de codificación. Dado que WordPress no es un

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
35
GRUPO HORUS S.A.

	sistema encerrado en sí mismo y ocasionalmente necesita comunicarse con otros sistemas, la intención era realizar ese trabajo. Por ejemplo, supongamos que quisieras publicar en tu sitio desde tu dispositivo móvil ya que tu computadora no está cerca. Podrías usar la función de acceso remoto habilitada por xmlrpc.php para hacerlo. Las funciones principales de xmlrpc.php eran permitirte conectarte a tu sitio a través de un teléfono móvil, implementar trackbacks y pingbacks desde otros sitios, y algunas funciones asociadas con el plugin Jetpack.
Recomendaciones	
WordPress XML-RPC	Hay cuatro formas en que un atacante podría abusar de la API XML-RPC de WP (específicamente, el método): pingback.ping • **Recopilación de Intel** : el atacante puede buscar puertos específicos en la red interna del objetivo • **Escaneo de puertos :** el atacante puede escanear puertos de hosts en la red interna • **Ataques DoS** : el atacante puede hacer pingback a través de una gran cantidad de sitios para un ataque DoS • **Hackeo de enrutadores :** el atacante puede reconfigurar un enrutador interno en la red

Si no está utilizando la funcionalidad XML-RPC, puede bloquear la funcionalidad agregando un la configuración en el .htaccess :

```
# protect xmlrpc
<IfModule mod_alias.c>
        RedirectMatch 403 /xmlrpc.php
</IfModule>
```

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

6.11.1 1. Default Tomcat User and Password (apache-tomcat-default-password)

Affected Nodes: 1	Additional Information: Existencia de Exploit	Status ACTIVO

Cambie la contraseña de la cuenta del administrador del servicio de Tomcat.

El servicio Tomcat tiene una cuenta de administrador establecida en una configuración predeterminada. Esto se puede cambiar en conf/tomcat-users.xml

Esto solucionará el siguiente problema: usuario y contraseña predeterminados de Tomcat (apache-tomcat-default-password).

2. Postgres default account: postgres/no password

Affected Nodes: 7	Additional Information: Existencia de Exploit	Status ACTIVO

Establezca una contraseña para la cuenta 'postgres'. Esto generalmente se hace editando el archivo 'pg_hba.conf'

Esto solucionará el siguiente problema: Cuenta predeterminada de Postgres: postgres/sin contraseña (postgres-default-account-postgres-nopassword).

Restringir el acceso a la base de datos

Configure el servidor de la base de datos para que solo permita el acceso a sistemas de confianza. Por ejemplo, el estándar PCI DSS requiere que coloque la base de datos en una zona de red interna, separada de la DMZ

Esto solucionará el siguiente problema: Acceso abierto a la base de datos (acceso abierto a la base de datos).

3. Samba RPC unauthenticated remote code execution (CVE-2012-1182)

Affected Nodes: 2	Additional Information: Existencia de Exploit	Status ACTIVO

Estas vulnerabilidades se pueden resolver realizando los siguientes 3 pasos.

1. Actualizar a la última versión de Samba
2. Alternativamente, los parches pueden estar disponibles en http://www.samba.org/samba/history/security.html.
3. Se recomienda que utilice el administrador de paquetes de su sistema operativo para actualizar si es posible.

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizado por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

Adicionalmente configurar la firma SMB para Samba

Configure Samba para habilitar o requerir la firma SMB según corresponda. Para habilitar la firma SMB, coloque lo siguiente en Samba

archivo de configuración, la configuración default se encuentra en smb.conf, en la sección global:

firma del servidor = auto

Para solicitar la firma SMB, cambiel:

firma del servidor = obligatorio

4. PHP Vulnerability: CVE-2015-0235

Affected Nodes: 50	Additional Information: Existencia de Exploit	Status ACTIVO

Estas vulnerabilidades se pueden resolver realizando los siguientes pasos.

Actualice a la última versión de PHP

Descargue y aplique la actualización desde: http://www.php.net/downloads.php

La última versión de PHP es 8.2.3

Esto indirectamente resolverá 1,136 problemas:

5. Apache Tomcat: Important: Remote Code Execution on Windows (CVE-2019-0232)

Affected Nodes: 12	Additional Information: Existencia de Exploit	Status ACTIVO

Actualice a la última versión de Apache Tomcat

Descargue y aplique la actualización desde: http://archive.apache.org/dist/tomcat/tomcat-10/v10.1.9/

La última versión de Apache Tomcat es 10.1

Esto indirectamente resolverá 71 problemas:

6. Webmin: Unauthenticated Remote Code Execution

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

Affected Nodes: 21	Additional Information: Existencia de Exploit	Status ACTIVO

Actualizar a la última versión de Webmin

Descargue y aplique la actualización desde: https://sourceforge.net/projects/webadmin/files/webmin/

Actualice a la última versión de Webmin.

Esto solucionará el siguiente problema: CVE-2019-15107: Webmin: Ejecución de código remoto no autenticado (http-webmin-cve-2019-15107).

7. PostgreSQL class A vulnerability in core server: CVE-2013-1899

Affected Nodes: 21	Additional Information: Existencia de Exploit	Status ACTIVO

Estas vulnerabilidades se pueden resolver con un solo paso.

Actualice a la última versión de PostgreSQL

Descargue y aplique la actualización desde: http://www.postgresql.org/download/

8. HTTP TRACE Method Enabled

Affected Nodes: 104	Additional Information: Existencia de Exploit	Status ACTIVO

Deshabilitar el método HTTP TRACE para Apache

Apache HTTPD, Apache Tomcat

Las versiones más recientes de Apache (1.3.34 y 2.0.55 y posteriores) proporcionan una directiva de configuración llamada TraceEnable. Para denegar solicitudes, agregue la siguiente línea a la configuración del servidor:

```
TraceEnable off
```

Para versiones anteriores del servidor web Apache, use el módulo mod_rewrite para denegar las solicitudes TRACE:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.

En Apache Tomcat, HTTP Trace se puede deshabilitar agregando restricciones de seguridad en la especificación de Java Servlet dentro del archivo de configuración web.xml y estableciendo el atributo allowTrace="False" en el conector HTTP en server.xml.

9. Apache Tomcat: Important: Remote Code Execution (CVE-2017-12617)		
Affected Nodes: 104	Additional Information: Existencia de Exploit	Status ACTIVO

Actualice a la última versión de Apache Tomcat

Descargue y aplique la actualización desde: http://archive.apache.org/dist/tomcat/tomcat-10/v10.1.9/

La última versión de Apache Tomcat es 10.1.9

10. Default SSH password: admin password "admin"		
Affected Nodes: 5	Additional Information: Existencia de Exploit	Status ACTIVO

ROBERTO INSFRAN

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Ciencias (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS S.A.