GRUPO HORUS

Asunción, 17 de abril 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 2 "Resultado GAP ANALISIS" 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 2: 1(un) Gap Análisis: que contiene el estado actual de madurez con respecto a ciberseguridad de la infraestructura de Ministerio de Educación y Cultura. Basados en los controles críticos de ciberseguridad v7.1. Estándar de controles de ciberseguridad para todas las instituciones gubernamentales, aprobado mediante la **Resolución MITIC Nº 277/2020**.*

Aprovechamos la oportunidad para saludarlos muy atentamente.

George Temperley Ovalle
Representante Legal
GRUPO HORUS S.A.

GRUPO HORUS
GRUPO HORUS S.A.

U.E.P.P. MEC
ENT. Nº: 3511
Lic.
HORA
17 ABR 2023 14:40

Avda. Brasilia 228 • CP 1208 • Asunción, Paraguay
+595 21 606 320
www.grupohorus.com.py
info@horustek.com

Contenido Programático Controles Críticos de Ciberseguridad

Código	MEC_001
Versión	Versión Enviada para Aprobación MEC
Fecha de la versión	17.04.2023
Creado por equipo de consultores	Grupo Horus
Aprobado por	
Nivel de confidencialidad	**SENSIBLE**

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Tabla de contenido

Introducción 2

Metodología CIS 3

Actividades 6

El Ministerio de Educación y Cultura (MEC) 7

1- GAP Análisis: 8

2- Establecer una priorización de controles 9

Implemente un plan para: 10

4- Establecer un alcance priorizado 11

CIS 1 | Inventario de dispositivos autorizados y no autorizados. 12

CIS 2 | Inventario de Software autorizados y no autorizados. 14

CIS 3 | Gestión continua de vulnerabilidades 16

CIS 4 | Uso controlado de privilegios administrativos 18

CIS 5 | Configuración segura para hardware y software en dispositivos móviles,computadoras portátiles, estaciones de trabajo y servidores 20

CIS 6 | Mantenimiento, monitoreo y análisis de logs de auditoría. 22

ANEXO 24

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Introducción

El continuo avance de las tecnologías ha propiciado que los agentes responsables de las amenazas hayan incrementado la sofisticación de sus ataques y sus herramientas, dando lugar a un ciberespacio cada vez más hostil, que obliga a las organizaciones a disponer de los medios técnicos más novedosos para poder hacer frente a los ataques y a sus posibles impactos, así como adoptar políticas de seguridad proactiva para mitigarlos.

En la actualidad este enfoque está evolucionando hacia la gestión de los riesgos del ciberespacio (Information Assurance), donde la ciberseguridad consiste en un proceso continuo de análisis y gestión de los riesgos asociados al ciberespacio.

Las amenazas más importantes relacionadas con el ciberespacio se pueden clasificar en dos grupos: **amenazas contra la información**, y amenazas contra la infraestructura. Las amenazas contra la información son aquellas que provocan una pérdida o un **uso indebido de la información**, el espionaje, el fraude, el robo de identidad, entre otras muchas. Por otro lado, las amenazas contra la infraestructura son aquellas que pueden provocar la interrupción parcial o total de los sistemas, como la infección de malware, ataques contra redes, sistemas, etc.

Todos los cambios que se han producido en estos últimos años, han puesto a prueba los servicios ofrecidos por la Institución y han hecho necesaria su revisión, de forma que esta asimile la evolución que se está produciendo en las soluciones de seguridad y pueda hacer frente con garantías al futuro inmediato de un mercado en constante cambio.

Sus comienzos se remontan al año 2008, la Oficina del Secretario de Defensa solicitó ayuda a la Agencia de Seguridad Nacional (**NSA**) para priorizar la búsqueda de controles de seguridad disponibles para la ciberseguridad. La solicitud fue realizada a la NSA porque ésta "**comprendió mejor cómo funcionaban los ataques cibernéticos y qué ataques se usaban con mayor frecuencia**". Esta solicitud llegó en un momento en que la frase "**la ofensa debe informar a la defensa**" se había convertido en un mantra de la Casa Blanca para la ciberseguridad.
El mandato del Departamento de Defensa (**DoD**) de USA para los **20 CIS** fue descrito de la siguiente manera por Tom Donahue de la CIA:

"**Primero arregle los males conocidos**". Eso significa que ningún control debe ser una prioridad a menos que se pueda demostrar que detiene o mitigar un ataque conocido. Este mandato fue la clave que vino a separar los controles críticos de

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

CIS de la mayoría de las otras listas de controles.

De esta manera comenzó la historia de los **20 controles críticos**, que es el resultado del trabajo de la **NSA, CIA, FBI, SANS** y un par de marcas de ciberseguridad hoy a cargo del CIS (**Center for Internet Security**), el objetivo, implementar los controles que "**realmente mitigan**" los ataques de ciberseguridad actuales, es un estudio vivo que se va actualizando, cambiando el orden y número de los controles, todo basado en cómo van mutando los ataques actuales. Definitivamente, consideramos que es el camino más eficiente para implementar ciberseguridad, ya que al introducir los 20 CIS realmente se están mitigando los ciber ataques actuales

Metodología CIS

Los **Controles CIS** se nutren de información de ataques reales y defensas efectivas y reflejan el conocimiento combinado de expertos de cada parte del ecosistema (**empresas, gobiernos, individuos**); con cada rol (respondedores y analistas de amenazas, tecnólogos, buscadores de vulnerabilidades, fabricantes de herramientas, proveedores de soluciones, defensores, usuarios, responsables de políticas, auditores, etc.); y dentro de muchos sectores (gobierno, poder, defensa, finanzas, transporte, academia, consultoría, seguridad, TI) que se han unido para crear, adoptar y respaldar los Controles.

Los principales expertos de las organizaciones combinaron su extenso conocimiento de primera mano para defenderse de los ciberataques reales y evolucionar la lista de controles consensuados, representando las mejores técnicas defensivas para prevenir o rastrearlos. Esto asegura que los Controles CIS son el conjunto más efectivo y específico de medidas técnicas disponibles para detectar, prevenir, responder y mitigar el daño desde el más común al más avanzado de esos ataques.

En mayo de 2021, se publicó la **versión 8.0**, que pese a no introducir mayores cambios en el contenido de los controles respecto a la 7.1, varía en su agrupación, introduce una novedad en el monitoreo y protección de redes, y manejo de la infraestructura de red. Además, también introduce una nueva categoría sobre la administración de proveedores de servicios. A efectos prácticos y a fin de cumplir con la resolución MITIC No 277/2020 por la cual "Dispone la aplicación de la Guía Aprobada de Controles Críticos de Ciberseguridad en su versión 7.0", esta consultoría evaluará en base a ponderación de la versión 7.0.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

Cada control crítico incluye:

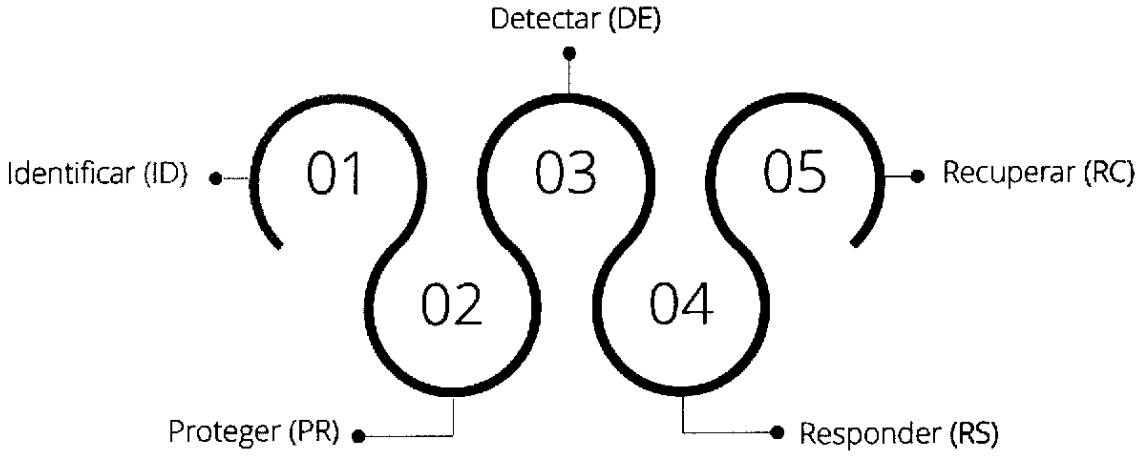
- Una explicación de cómo los atacantes explotan activamente la ausencia de este control.
- Un listado de las acciones específicas que las organizaciones están realizando para implementar, automatizar y medir la efectividad de este control:
    - **Quick wins** que proporcionen una sólida reducción del riesgo sin realizar grandes cambios técnicos, en la arquitectura o a nivel de procedimientos y que proporcionen una reducción sustancial y rápida del riesgo en base a los ataques más comunes que sufren la mayoría de las organizaciones.
    - **Medidas de visibilidad y atribución** que mejoren los procesos, la arquitectura y las capacidades técnicas de la organización para monitorizar las redes y sistemas, detectar intentos de ataques, localizar puntos de entrada, identificar máquinas ya comprometidas, interrumpir las actividades de los atacantes infiltrados y conseguir información sobre las fuentes de los ataques.
    - **Configuración de la seguridad de la información** mejorada para reducir el número o magnitud de las vulnerabilidades de seguridad y mejorar las operaciones de los sistemas informáticos con un enfoque en la protección contra prácticas de seguridad pobres por parte de los administradores de los sistemas y de los usuarios
    - **Sub controles avanzados** que utilizan las nuevas tecnologías para proporcionar una máxima seguridad pero que son difíciles de implementar o son más caros que soluciones de seguridad más estándar.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

Qué es el Cybersecurity Framework de NIST

Este marco ayuda a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos

Núcleo del Marco



El núcleo proporciona cinco funciones continuas, vistas más arriba. Asimismo, también brinda un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación para lograr esos resultados.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

Actividades

1. **GAP Análisis:** evaluación del grado de cumplimiento actual de cada uno de los controles que le apliquen.
2. Establecer una priorización de controles por impacto en la seguridad. Si bien los controles que corresponde al IG1 deberían ser los más prioritarios y los exclusivos al IG3 los menos urgentes, el impacto depende completamente (**quick wins**) de la naturaleza de la institución.
3. Establecer un alcance priorizado para cada control.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

El Ministerio de Educación y Cultura (MEC)

Organigrama MEC

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

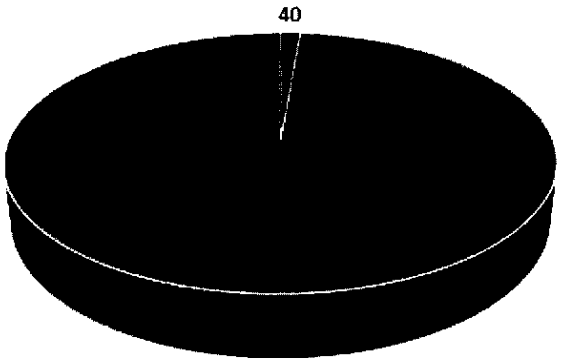
1- GAP Análisis:

Evaluación del grado de cumplimiento actual de cada uno de los controles que le apliquen.

Observación

0 - **Nulo**: el sub-control no existe
1 - **Básico**: el sub-control existe a nivel de procedimiento (escrito o manual) y se cumple parcialmente
2 - **Intermedio**: el sub-control existe de manera más o menos automatizada (mediante una herramienta tecnológica) y se cumple parcialmente
3 - **Avanzado**: el sub-control existe de manera completamente automatizada (mediante una herramienta tecnológica) y se cumple completamente
4 - **Completo**: el sub-control existe de manera completamente automatizada, se cumple completamente y se monitorea regularmente para controlar su funcionamiento correcto

Cumplimiento Controles Criticos de Ciberseguridad v7



1,39 %

	Puntaje	**1,39**
Ponderación Controles	13,0212766	Controles básicos
Ponderación Controles Fundacionales	0,81818182	Controles Fundacionales
Ponderación Controles Organizacionales	1	Controles Organizacionales
Máximo Puntaje	**76,40957447**	Puntaje Máximo alcanzable de los controles

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

2- Establecer una priorización de controles

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.

Framework de Ciberseguridad del NIST

1. **Identificar.**
    a. **Acciones**: Haga una lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.
    b. **Elabore y comparta** una política de ciberseguridad de la compañía que cubra los siguientes puntos: **1.** Funciones y responsabilidades de los empleados, proveedores y todo aquel que tenga acceso a datos delicados. **2.** Pasos a seguir para protegerse contra un ataque y limitar el daño si se produce un ataque.
2. **Proteger.**
    a. Controle quiénes acceden a su red y usan sus computadoras y otros dispositivos.
    b. Use programas de seguridad para proteger los datos.
    c. Codifique los datos delicados, tanto cuando estén almacenados o en tránsito.
    d. Haga copias de seguridad de los datos con regularidad.
    e. Actualice los programas de seguridad con regularidad, en lo posible, automatice estas actualizaciones.
    f. Implemente políticas formales para la eliminación segura de archivos electrónicos y dispositivos en desuso.
    g. Capacite sobre ciberseguridad a todas las personas que usan sus computadoras, dispositivos y redes. Usted puede ayudar a los empleados a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.
3. **Detectar.**
    a. Monitoree sus computadoras para controlar si detecta acceso de personal no autorizado a sus computadoras, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.
    b. Revise su red para controlar si detecta usuarios o conexiones no autorizadas.
    c. Investigue cualquier actividad inusual en su red o por parte de su

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

personal.

4. **Responder.**

   a. Implemente un plan para:
      i. Notificar a los clientes, empleados y otros cuyos datos pudieran estar en riesgo.
      ii. Mantener en funcionamiento las operaciones del negocio.
      iii. Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.
      iv. Investigar y contener un ataque.
      v. Actualizar su política y plan de ciberseguridad con las lecciones aprendidas.
      vi. Prepararse para eventos inadvertidos (como emergencias climáticas) que puedan poner en riesgo los datos.

5. **Recuperar.**

   a. Después de un ataque: Repare y restaure los equipos y las partes de su red que resultaron afectados. Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación.

Quick wins

Acciones que requieren poco esfuerzo pero que dan un resultado relativamente grande..

A continuación, los sub-controles que tienen el impacto más inmediato en la prevención de ataques:

1. **Inventario de Activos**
   a. Registre todos los activos de la organización.
   b. Existen herramientas tanto open source como privadas.
   c. Mantener la lista actualizada.
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)
3. **Uso de estándares, configuraciones seguras**
   a. Establecer configuraciones seguras basadas en estándares de

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

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

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

PLAN DE TRABAJO										
#	Actividad		Esfuerzo TL	Esfuerzo Team	s1	s2	s3	s4	s5	s6
1	Inventario de activos	✓	1	2						
2	Listas blancas de aplicaciones	✓	1	2						
3	Uso de estándares, configuraciones seguras	✓	1	2						
4	Aplicar parches de sistemas	✓	1	2						
5	Uso de privilegios administrativos	✓	1	2						

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE PAMPLEY
GRUPO HORUS
Grupo Horus S.A.

4- Establecer un alcance priorizado

Para cada control. Implementar CIS Basicos. Identificar las herramientas existentes que puedan ser reutilizadas o utilizadas mejor, nuevas herramientas a adquirir, procesos a mejorar y habilidades a desarrollar mediante formación.

- **CIS 1 | Inventario de dispositivos autorizados y no autorizados.**

Control 1 se enfoca en administrar activamente (inventariar, rastrear y corregir) todos los dispositivos de hardware en la red para que solo los dispositivos autorizados tengan acceso y los dispositivos no autorizados o no administrados se encuentren y se bloqueen para que no obtengan acceso.

Este control se divide en 6 secciones enfocadas relacionadas con el control de acceso a la red, la automatización y la gestión de activos. El control se centra específicamente en la necesidad de conocer qué está conectado a tu red. También prioriza la gestión de inventario interno y la automatización de la gestión.

La implementación del control de inventario no es la forma más atractiva de mejorar tu programa de seguridad, sin embargo, es un control de seguridad fundamental que es un requisito previo para los 19 controles de seguridad adicionales.

¿Por qué es importante este control?

CIS Control 1 es fundamental porque los malos actores en línea buscan sistemas nuevos y desprotegidos y están particularmente interesados en los dispositivos que entran y salen de la red. Por ejemplo, traiga sus propios dispositivos (BYOD), dispositivos móviles y dispositivos IoT.

Estos dispositivos no solo corren el riesgo de no estar sincronizados con las actualizaciones de seguridad, sino que, lo que es peor, ya podrían estar comprometidos.

Incluso los dispositivos que no son visibles desde Internet pueden ser utilizados por malos actores que ya han obtenido acceso interno.

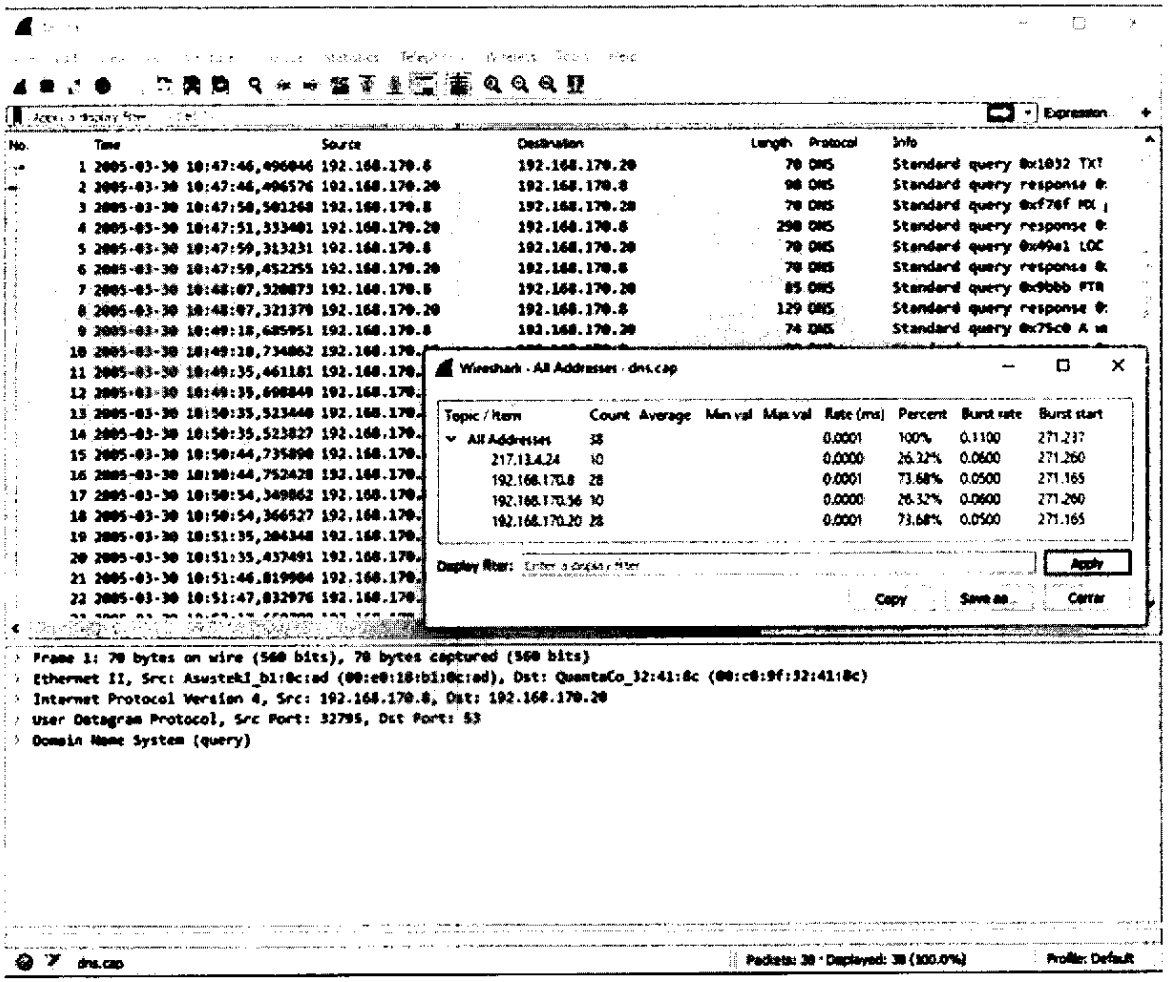
Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (MEC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento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

IMPLEMENTACIÓN

Dentro de las herramientas que se pueden utilizar para la realización de un inventariado de activos se distinguen principalmente dos tipos: las herramientas gratuitas (open source y libres) y las herramientas propietarias o comerciales. Las herramientas open source son aquellas que se pueden utilizar de manera gratuita y cuyo código fuente se encuentra disponible para todo el mundo.

- Wireshark

Es una herramienta de código libre desarrollada para el análisis de protocolos de red, que permite la realización de un inventario mediante la identificación de los equipos implicados en las comunicaciones de forma pasiva gracias a la captura de tráfico de red.



Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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 2 | Inventario de Software autorizados y no autorizados.**

CIS Control 2 se enfoca en administrar activamente (inventariar, rastrear, corregir) todo el software en la red para que solo el software autorizado esté instalado y pueda ejecutarse. Del mismo modo, todo el software no autorizado y no administrado se encuentra y se bloquea su instalación y ejecución.

Básicamente, CIS Control 2 te pide que sepas qué software hay en tu sistema, quién lo instaló y qué hace. El control se centra en la necesidad de saber qué se está ejecutando en tus sistemas y red en todo momento. También se centra en la necesidad de una gestión de inventario interna. De esa manera, si algo sucediera, tu equipo podría identificar y eliminar fácilmente el software que no está en su lista de inventario.

Cuando se hace correctamente, reduce las amenazas internas y los riesgos de pérdida, limpia tu entorno de TI y proporciona una mayor visibilidad y organización a tu red.

¿Por qué es importante este control?

Los atacantes se dirigen continuamente a organizaciones que ejecutan versiones vulnerables de software porque es fácil de explotar de forma remota.

Además, algunos atacantes también distribuyen documentos, archivos multimedia, páginas web hostiles y otro contenido malicioso a través de sus propias páginas web o sitios de terceros confiables. Si los usuarios desprevenidos acceden a este contenido con un navegador vulnerable, los ataques pueden comprometer tus máquinas. Luego, los atacantes a menudo instalan programas de puerta trasera y bots que les brindan un control del sistema a largo plazo y sin ser detectados.

Una vez que un atacante explota una sola máquina, a menudo la usa para recopilar información confidencial sobre la corporación, el sistema comprometido y cualquier otro sistema conectado a ella.

Por lo tanto, sin un conocimiento o control completo del software implementado en una organización, los defensores no pueden proteger adecuadamente sus activos o identificar el software que no debería estar allí. O peor aún, puede que ya esté allí y sea malicioso.

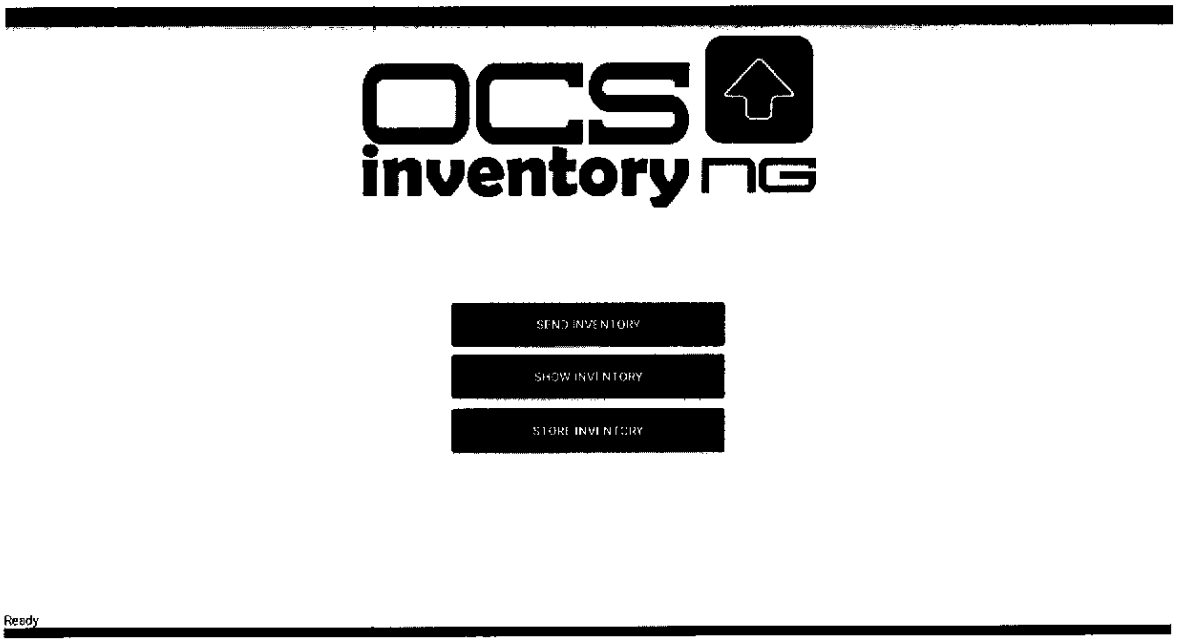
El control administrado de todo el software también juega un papel fundamental en la planificación y ejecución del respaldo del sistema, la respuesta a incidentes y la recuperación. Como resultado, CIS Control 2 fortalece múltiples aspectos de su postura de seguridad cibernética y vale la pena implementarlo para tu equipo.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

IMPLEMENTACIÓN

- OCS inventory

Es una herramienta de código libre desarrollada para mantener una lista de inventario automatizado.



Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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 3 | Gestión continua de vulnerabilidades**

CIS Control 3 se centra en la necesidad de adquirir, evaluar y actuar continuamente sobre nueva información para identificar nuevas vulnerabilidades, remediar y minimizar la oportunidad para los atacantes.

Las organizaciones operan en un flujo constante de nueva información de seguridad: amenazas en evolución, actualizaciones de software, parches, avisos de seguridad, etc.

Básicamente, CIS Control 3 te pide que comprendas y administres continuamente estas vulnerabilidades.

El control consta de 8 secciones diferentes relacionadas con la concienciación y la gestión de la vulnerabilidad.

¿Por qué es importante este control?

Comprender y administrar las vulnerabilidades a un ritmo constante requiere tiempo, atención y recursos. En la mayoría de los casos, los atacantes tienen acceso a la misma información y pueden aprovechar las brechas entre la aparición de nuevos conocimientos y la corrección.

Por ejemplo, los investigadores que informan sobre nuevas vulnerabilidades pueden provocar una carrera entre varias partes: atacantes (que intentan convertir la vulnerabilidad en armas y explotarla), proveedores (que intentan implementar parches y actualizaciones para proteger a los usuarios) y defensores (que intentan evaluar el riesgo y proteger sus sistemas).

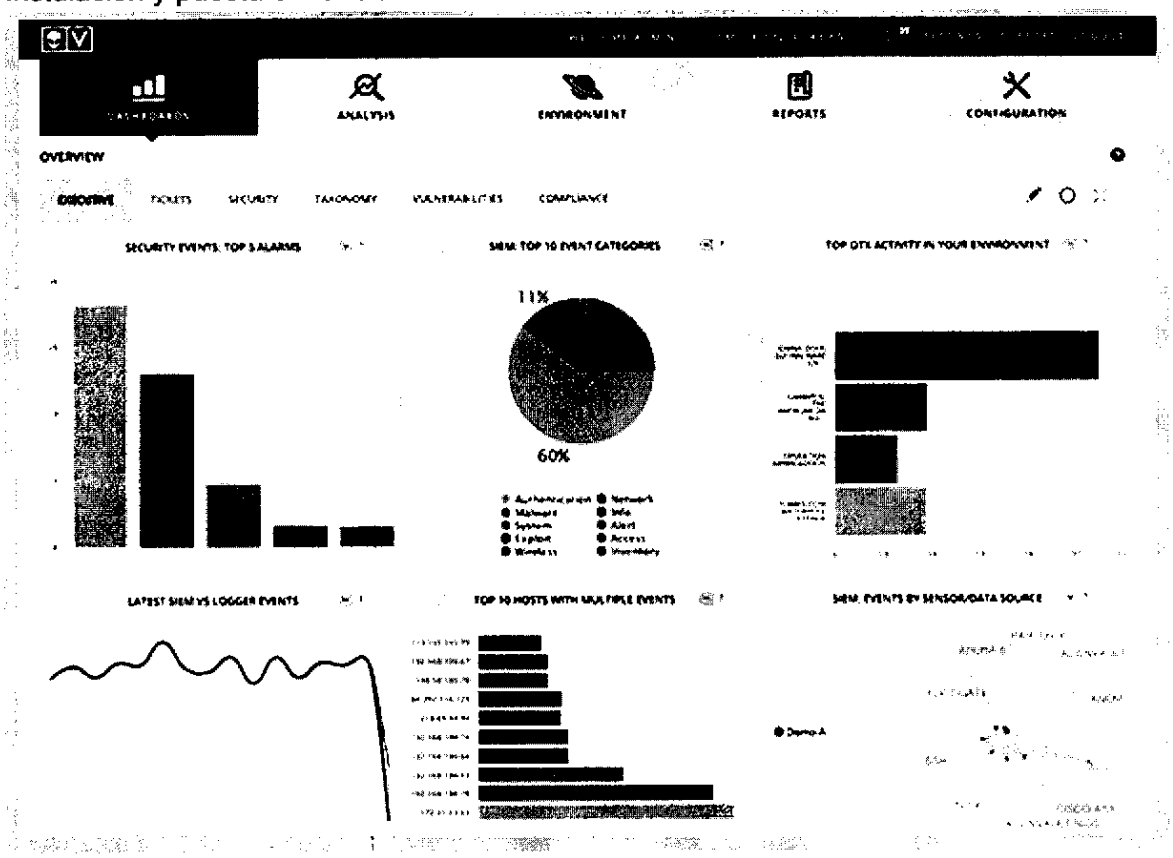
Las organizaciones que no escanean en busca de vulnerabilidades o abordan de manera proactiva las vulnerabilidades descubiertas aumentan la probabilidad de exploits y ataques.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

IMPLEMENTACIÓN

- Instalación y puesta en funcionamiento de SIEM OSSIM



Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

- **CIS 4 | Uso controlado de privilegios administrativos**

CIS Control 4 se centra en controlar el uso de privilegios administrativos.

Específicamente, este control se enfoca en reducir el privilegio administrativo y restringirlo solo a los usuarios que lo requieran para desempeñar sus funciones laborales. En la mayoría de los casos, la mayoría de los usuarios no requieren privilegios de administrador para realizar las tareas diarias. Sin embargo, muchas empresas otorgan privilegios administrativos a todos los usuarios, independientemente de su función laboral.

CIS Control 4 se enfoca en el uso de procesos y herramientas para rastrear, controlar, prevenir y corregir el uso, asignación y configuración de privilegios administrativos en computadoras, redes y aplicaciones.

¿Por qué es importante este control?

CIS Control 4 es fundamental porque los piratas informáticos están constantemente en busca de organizaciones que no controlen / restrinjan a su administrador.

El uso indebido de privilegios es un método cada vez más popular entre los atacantes para aterrizar y expandirse dentro de las redes.

Por ejemplo, dos ataques comunes que dependen de privilegios administrativos para ejecutarse son los siguientes:

En primer lugar, un atacante manipula a un usuario que se ejecuta con privilegios administrativos para que abra un archivo PDF o adjunto malicioso.

O bien, un usuario se infecta con malware después de visitar un sitio que lo carga silenciosamente en segundo plano.

Las cuentas privilegiadas hacen que estos ataques sean específicamente rápidos y peligrosos de llevar a cabo. Las máquinas de los usuarios pueden controlarse instantáneamente, tener instalado el registro de teclas y pueden ocurrir otras actividades maliciosas, todo fuera de la vista.

Cuando esto se ejecuta en un dispositivo con privilegios administrativos, el atacante puede apoderarse completamente de la máquina de la víctima e infectar otros sistemas en la red.

El segundo ataque común se conoce como un ataque de elevación de privilegios al adivinar o descifrar una contraseña establecida para un usuario administrativo con el fin de obtener acceso a una máquina objetivo. Si los privilegios administrativos se otorgan libremente, o si se utilizan contraseñas idénticas (o similares) en sistemas menos críticos,

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE KEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

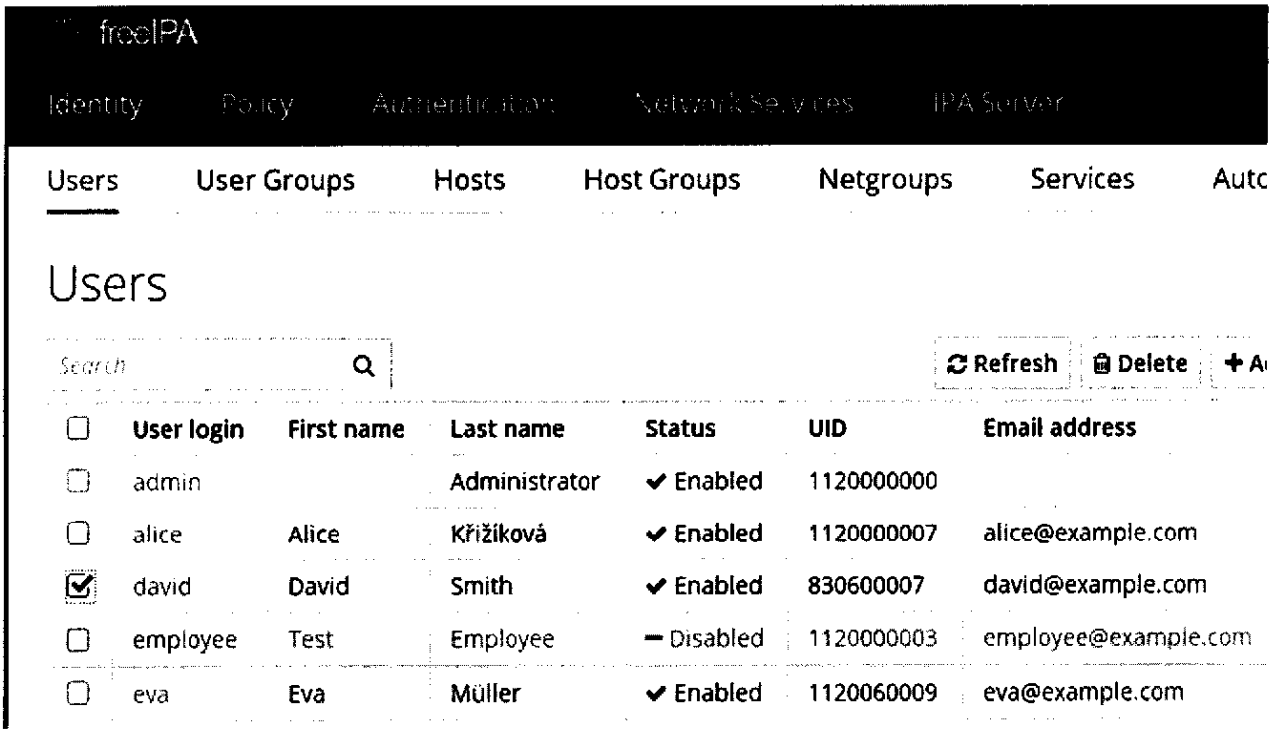
el atacante puede obtener fácilmente el control total de tus sistemas.

Como resultado, restringir el acceso a los datos por función laboral es una de las formas más efectivas de reducir su riesgo.

IMPLEMENTACIÓN

- FreeIPA

FreeIPA es una solución integrada de identidad y autenticación para entornos de red Linux / UNIX. Un servidor FreeIPA proporciona información centralizada de autenticación, autorización y cuenta al almacenar datos sobre usuarios, grupos, hosts y otros objetos necesarios para administrar los aspectos de seguridad de una red de computadoras.



Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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 5 | Configuración segura para hardware y software en dispositivos móviles,computadoras portátiles, estaciones de trabajo y servidores**

CIS Control 5 se centra en la configuración segura de hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores.

Específicamente, este control se enfoca en establecer, implementar y luego administrar activamente la configuración de seguridad de los dispositivos utilizando una administración de configuración rigurosa y procesos de control de cambios para evitar que los piratas informáticos exploten los servicios y configuraciones vulnerables.

¿Por qué es importante este control?

CIS Control 5 es fundamental porque las configuraciones predeterminadas para los sistemas operativos y las aplicaciones están orientadas principalmente a la facilidad de uso y no a la seguridad. Como resultado, los controles básicos, los servicios y puertos abiertos, las cuentas o contraseñas predeterminadas, los protocolos más antiguos y la preinstalación de software innecesario pueden ser fáciles de explotar en su estado predeterminado.

Por lo tanto, es importante desarrollar opciones de configuración con propiedades de seguridad sofisticadas. Sin embargo, esta puede ser una tarea compleja más allá de la capacidad de los usuarios individuales. De hecho, puede requerir el análisis de cientos o miles de opciones para tomar las decisiones correctas.

Por ejemplo, incluso si se desarrolla e instala una configuración inicial sólida, debe administrarse continuamente para evitar la degradación de la seguridad a medida que el software se actualiza o parchea, se informan nuevas vulnerabilidades de seguridad y se modifican las configuraciones. En la mayoría de los casos, las configuraciones se modifican para permitir la instalación de nuevo software o para admitir nuevos requisitos operativos.

Si no es así, los atacantes encontrarán oportunidades para explotar tanto los servicios accesibles a la red como el software del cliente.

Como resultado, es fundamental desarrollar e implementar una configuración segura de tus dispositivos.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

IMPLEMENTACIÓN DE LAS GUÍAS

Guías

A continuación, se referencian una serie de sitios web con documentación general relacionada con configuración segura:

- ➔ Políticas de Uso de manejo de correo institucional
- ➔ Política de manejo de credenciales
- ➔ Política de uso de accesos administrativos
- ➔ Políticas de seguridad en entornos corporativos

OBS: Pendientes de socializar por medio de resoluciones internas.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

- **CIS 6 | Mantenimiento, monitoreo y análisis de logs de auditoría.**

CIS Control 6 se enfoca en recopilar, administrar y analizar registros de auditoría de eventos que podrían ayudar a tu equipo a detectar, comprender y recuperarse de un ataque.

Específicamente, este control se enfoca en establecer, implementar y luego administrar activamente el proceso mediante el cual se monitorizan y analizan tus registros.

Procedimiento
• Activación de los registros de auditoría • Configuración de los datos a ser registrados • Protección de los registros de eventos • Revisión periódica de los registros de eventos • Planificación e implementación de una infraestructura de registro de eventos

¿Por qué es importante este control?

CIS Control 6 es fundamental porque las deficiencias en el registro y análisis de seguridad pueden permitir a los atacantes ocultar su ubicación, software malicioso y actividades en las máquinas de las víctimas. Cuanto más tiempo esté un atacante en tu dispositivo sin ser detectado, más daño será capaz de infligir. Además, incluso si las víctimas están al tanto de un atacante en tu sistema, sin registros protegidos y completos, pueden no ver los detalles del ataque.

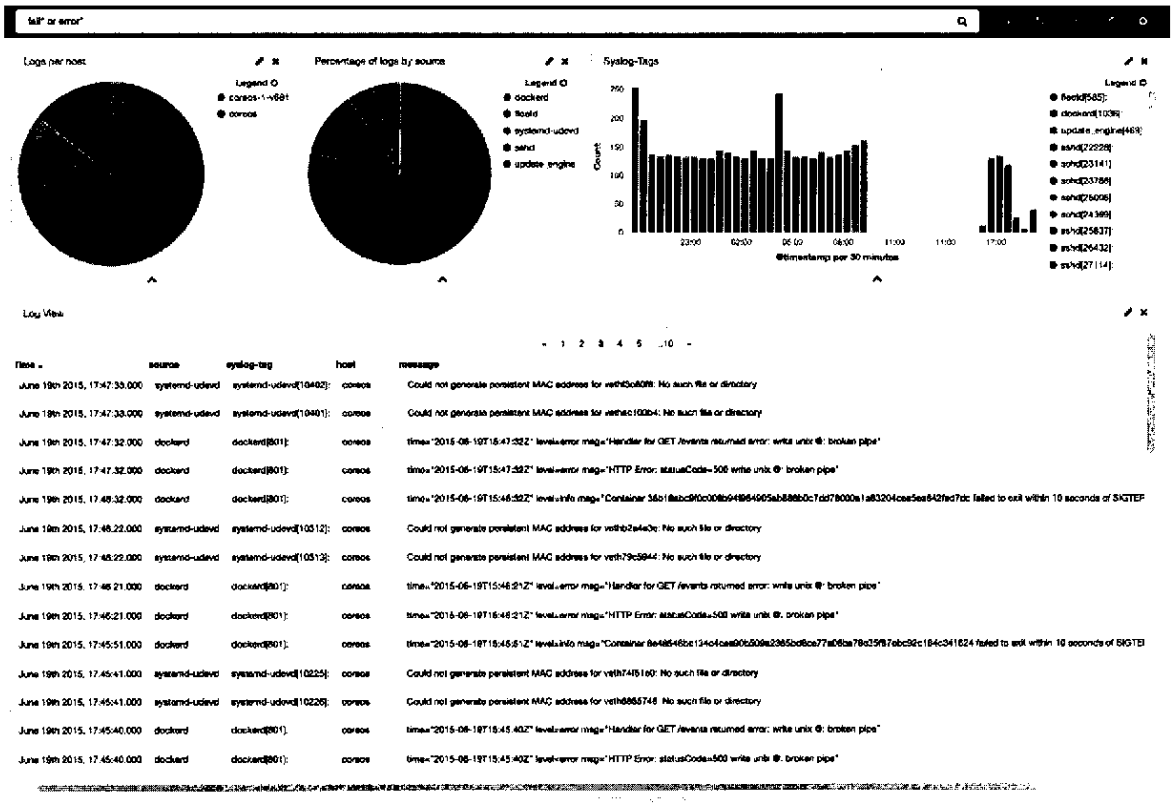
Sin registros de auditoría sólidos, un ataque puede pasar desapercibido indefinidamente y el daño causado puede ser irreversible.

IMPLEMENTACIÓN

- Instalación de ELK

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.



Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

ANEXO

1. Adjunto **ListadeAplicacionesPermitidas.xlsx**
2. Adjunto **PlanilladeEvaluacionCIS-MEC-v2.xlsx**

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Educación y Cultura (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.

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

GAP ANÁLISIS DE CIBERSEGURIDAD

Controles Críticos de Ciberseguridad

CIS v8

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A

Código	MEC_001
Versión	**V1**
Fecha de la versión	
Creado	Grupo Horus
Aprobado por	
Nivel de confidencialidad	CONFIDENCIAL

Histórico de Versiones

Fecha	Versión	Modificación	Realizado por
17-04-23	1.0	Versión Enviada para Aprobación	Grupo Horus

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

ÍNDICE

Introducción	4
Metodología CIS	5
Mapa de Calor MEC	14
Glosario	14
Actividades	16
1.1. Inventario y control de activos corporativos	17
2.1. Inventario y control de activos de software	18
4.1 Configuración segura de activos y software corporativos	20
5.1 Gestión de cuentas	21
6.1 Gestión de Control de Acceso	23
7.1 Gestión Continua de Vulnerabilidades	23
8.1 Gestión de Registros de Auditoría	24
9.1 Protecciones de Correo Electrónico y Navegador Web	26
10.1 Defensas Contra Malware	26
11.1 Recuperación de Datos	27
12.1 Gestión de Infraestructura de Red	28
13.1 Monitoreo y Defensa de la Red	29
14.1 Concientización sobre Seguridad y Capacitación en Habilidades	31
15.1 Gestión de Proveedores de Servicios	32
16.1 Seguridad de la Aplicación	33
17.1 Gestión de Respuesta a Incidentes	34
18.1 Pruebas de Penetración	35
Anexo A: Plan de Acción	37
Anexo B: Respuestas de la Organización	49

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Introducción

Este documento tiene como objetivo presentar, en una perspectiva empresarial, los resultados obtenidos durante el proyecto **"CONSULTORIA PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC" (HACKING ETICO)** realizado en el entorno del MEC. Estos resultados se refieren al conjunto de posibilidades de mejora encontradas por la consultoría durante la evaluación técnica.

El trabajo realizado se basó principalmente en los **Controles Críticos de Ciberseguridad** (CIS) y en segundo lugar en el Marco de Ciberseguridad del NIST. Los controles CIS son un conjunto recomendado de acciones de ciberseguridad que brindan acciones específicas para prevenir los ataques más conocidos.

El Ministerio de Educación y Ciencias o MEC, es la dependencia estatal del Gobierno Nacional responsable de las políticas públicas, de la gestión y de la calidad de la educación en la República del Paraguay

El Ministerio de Educación y Ciencias (MEC), por su importancia, trascendencia y el volumen y sensibilidad de la información que produce y administra debe actuar siempre sobre la base de una preocupación constante en orden a garantizar la **Integridad, Confidencialidad y Disponibilidad** de sus operaciones y servicios. Así, este documento presenta la situación actual constatada y enumera recomendaciones que apuntan a garantizar un nivel aún mayor de seguridad de la información, los activos y servicios complementarios.

Las Amenazas

El continuo avance de las tecnologías ha propiciado que los agentes responsables de las amenazas hayan incrementado la sofisticación de sus ataques y sus herramientas, dando lugar a un ciberespacio cada vez más hostil, que obliga a las organizaciones a disponer de los medios técnicos más novedosos para poder hacer frente a los ataques y a sus posibles impactos, así como adoptar políticas de seguridad proactivas para mitigarlos.

En la actualidad este enfoque está evolucionando hacia la gestión de los riesgos del ciberespacio (Information Assurance), donde la ciberseguridad consiste en un proceso continuo de análisis y gestión de los riesgos asociados al ciberespacio.

Las amenazas más importantes relacionadas con el ciberespacio se pueden clasificar en dos grupos: **amenazas contra la información**, y amenazas contra la infraestructura. Las amenazas contra la información son aquellas que provocan una

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

pérdida o un **uso indebido de la información**, el espionaje, el fraude, el robo de identidad, entre otras muchas. Por otro lado, las amenazas contra la infraestructura son aquellas que pueden provocar la interrupción parcial o total de los sistemas, como la infección de malware, ataques contra redes, sistemas, etc.

Metodología CIS

Los **Controles CIS** se nutren de información de ataques reales y defensas efectivas y reflejan el conocimiento combinado de expertos de cada parte del ecosistema (**empresas, gobiernos, individuos**); con cada rol (respondedores y analistas de amenazas, tecnólogos, buscadores de vulnerabilidades, fabricantes de herramientas, proveedores de soluciones, defensores, usuarios, responsables de políticas, auditores, etc.); y dentro de muchos sectores (gobierno, defensa, finanzas, transporte, academia, consultoría, seguridad, TI) que se han unido para crear, adoptar y respaldar los Controles.

En mayo de 2021, se publicó la **versión 8.0,** que pese a no introducir mayores cambios en el contenido de los controles respecto a la 7.1, varía en su agrupación, introduce una novedad en el **monitoreo y protección de la información**, **y manejo de la infraestructura de red.** Además, introduce una nueva categoría sobre la administración de proveedores de servicios.

Los expertos responsables de redactar los Controles CIS también reconocen la realidad a la que se enfrentan la mayoría de las organizaciones, donde los recursos suelen ser limitados y las prioridades deben definirse. Como tal, CIS separa los controles, independientemente del tipo de industria, en tres categorías; Básico, Fundamental y Organizativo, los cuales se detallan en el siguiente cuadro:

Básico	Fundamental	Organizativo

GEORGE TEMPERLEY
GRUPO HORUS

CONTROL	CONTROL	CONTROL
Inventory and Control of Enterprise Assets	Inventory and Control of Software Assets	Data Protection
5 SAFEGUARDS IG1 2/5 IG2 2/5 IG3 2/5	7 SAFEGUARDS IG1 3/7 IG2 6/7 IG3 7/7	14 SAFEGUARDS IG1 6/14 IG2 12/14 IG3 14/14
CONTROL	CONTROL	CONTROL
Secure Configuration of Enterprise Assets	Account Management	Access Control Management
12 SAFEGUARDS IG1 7/12 IG2 11/12 IG3 12/12	6 SAFEGUARDS IG1 4/6 IG2 6/6 IG3 6/6	8 SAFEGUARDS IG1 5/8 IG2 7/8 IG3 8/8
CONTROL	CONTROL	CONTROL
Continuous Vulnerability Management	Audit Log Management	Email and Web Browser Protections
7 SAFEGUARDS IG1 4/7 IG2 7/7 IG3 7/7	12 SAFEGUARDS IG1 3/12 IG2 11/12 IG3 12/12	7 SAFEGUARDS IG1 2/7 IG2 6/7 IG3 7/7
CONTROL	CONTROL	CONTROL
Malware Defenses	Data Recovery	Network Infrastructure Management
7 SAFEGUARDS IG1 3/7 IG2 7/7 IG3 7/7	5 SAFEGUARDS IG1 4/5 IG2 5/5 IG3 5/5	8 SAFEGUARDS IG1 1/8 IG2 7/8 IG3 8/8
CONTROL	CONTROL	CONTROL
Network Monitoring and Defense	Security Awareness and Skills Training	Service Provider Management
11 SAFEGUARDS IG1 0/11 IG2 8/11 IG3 11/11	9 SAFEGUARDS IG1 8/9 IG2 8/9 IG3 9/9	7 SAFEGUARDS IG1 1/7 IG2 4/7 IG3 7/7
CONTROL	CONTROL	CONTROL
Applications Software Security	Incident Response Manager	Penetration Testing
14 SAFEGUARDS IG1 0/14 IG2 11/14 IG3 14/14	9 SAFEGUARDS IG1 3/9 IG2 8/9 IG3 9/9	5 SAFEGUARDS IG1 0/5 IG2 3/5 IG3 5/5

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

Qué es el Cybersecurity Framework de NIST

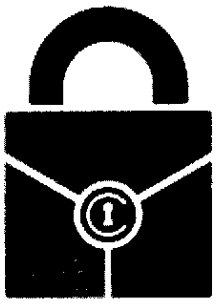
Este marco ayuda a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos

El núcleo proporciona cinco funciones continuas, vistas más arriba. Asimismo, también brinda un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación para lograr esos resultados.

GEORGE TEMPERLEY

GRUPO HORUS
GRUPO HORUS S.A.

Grupos de Implementación



Uno de los aspectos más relevantes de la estructura de la guía de controles CIS es la clasificación y priorización de la implementación de los 18 controles y las 153 salvaguardas tomando en consideración el tamaño, perfil de riesgo y recursos disponibles en la organización para implementar una estrategia de ciberseguridad. CIS define y clasifica sus salvaguardas considerando 3 grupos de implementación que se describen a continuación, conforme a la descripción se podrá identificar de mejor manera qué controles y prácticas de ciberseguridad son apropiadas para la organización.

Grupo de Implementación	Descripción	Cantidad de Salvaguardas recomendadas
IG1	Una organización **IG1** es una empresa pequeña o mediana con recursos limitados de TI y con expertise mínimo en ciberseguridad para proteger los activos de TI. La principal preocupación de estas organizaciones es mantener el negocio operativo dado que tienen una tolerancia limitada a las interrupciones tecnológicas. La sensibilidad de la información que manejan es baja y está vinculada principalmente con la información de los colaboradores o de carácter financiero Las salvaguardas seleccionadas para este grupo de implementación pueden ser implementadas con un expertise en ciberseguridad limitado y van orientadas a proteger ataques no dirigidos. Estas salvaguardas son las mínimas que toda organización se recomienda implemente para protegerse a los ataques más comunes (Higiene básica de ciberseguridad) Estas salvaguardas van dirigidas también para pequeños negocios o esquemas de teletrabajo (Home office).	56
IG2	Una organización **IG2** contrata posiciones responsables de administrar y proteger la infraestructura de TI. Esta organización soporta a múltiples departamentos con diferentes perfiles de riesgos basado en su función y misión. Algunas unidades de negocio pequeñas pueden tener requerimientos regulatorios a cumplir. Las Organizaciones IG2 con frecuencia almacenan y procesan información sensible de clientes o de la organización y pueden resistir interrupciones cortas a sus servicios.	130

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

	Una preocupación importante es perder la confianza de los clientes derivado de una brecha de seguridad. Las salvaguardas seleccionadas para las organizaciones IG2 dependen del nivel de adopción tecnológico de la compañía y requieren de un mayor nivel expertise y especialización en seguridad para instalarlas y configurarlas.	
IG3	Una organización **IG3** contrata posiciones expertas y especializadas en diferentes facetas de ciberseguridad (Gestión de riesgos, Pentester, seguridad en la información). Los activos y datos de las organizaciones IG3 contienen información sensible o funciones que se encuentran bajo una supervisión de cumplimiento o regulación por parte de terceros/autoridades. Una organización IG3 debe gestionar la disponibilidad de sus servicios de TI y la confidencialidad, integridad de la información sensible. Un ataque exitoso puede generar un daño significativo a la reputación y bienestar en el entorno. Las salvaguardas seleccionadas para una organización IG3 van dirigidas para prevenir un ataque dirigido por parte de un adversario sofisticado y reducir el impacto de ataques de día cero.	153

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Actividades

En la metodología utilizada, cada medida de seguridad tiene un nivel de madurez de acuerdo con su implementación a nivel procedimental, recursos humanos y tecnológicos.

Cada una de estas categorías tiene el mismo peso, ¼ de valor del 100% para cada una de ellas.

Una medida de seguridad se compone de un identificador, resumen para su identificación y su estado. Procedimentales, humanos y tecnológicos.

El siguiente es un ejemplo de una medida de seguridad:

Identificador	Estado de la Medida de Seguridad	Estado		
	Ejemplo	Procedimental	Humano	Tecnológico

De procedimiento: cuenta con una política, norma, proceso o procedimiento operativo, en forma parcial o total, para la ejecución del control

Humano: implementación manual (parcial o total) del control basado en documentación.

Tecnológico: automatización del control (parcial o total).

Color	Prioridad	Clasificación
	1	Básico
	2	Fundamental
	3	Organizativo

Procedimental	Humano	Tecnológico
Buenas Prácticas	Partes Del Proceso	Partes Del Proceso
Parcialmente Escrito	Algunos Sistemas	Algunos Sistemas
Escrito	La Mayoría De Los Sistemas	La Mayoría De Los Sistemas
Escrito y Aprobado	Todos Los Sistemas	Todos Los Sistemas

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Plan De Acción

En el Anexo A: encontramos las recomendaciones técnicas para todas las medidas de seguridad no conformes. El anexo contiene una tabla formada por el ID de la medida de seguridad, el riesgo asociado y las acciones organizativas y técnicas. También vale la pena mencionar que cada ID tiene un color asociado, que representa su grupo de prioridad, como se mencionó anteriormente.

Se recomienda comenzar con los controles IG1 (color verde) ya que son los controles más básicos que debe implementar cualquier empresa sin importar su tamaño. También recomendamos asignar un responsable y plazos de solución para cada medida de seguridad, teniendo así una mejor gestión de las actividades.

Las sugerencias correctivas fueron clasificadas en orden de prioridad por la criticidad del riesgo de no implementación del control. Además, también consideramos el concepto de "**Quick Wins**", ya que reduce la resistencia al cambio y motiva a las personas a apoyar el programa del proyecto correctivo. Se recomienda que la difusión de las mejoras implementadas y sus beneficios para la empresa sea realizada por el área de comunicación interna.

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

Mapa de Calor

El mapa de calor es una representación gráfica cuyos valores se representan mediante colores, que resaltan las necesidades más urgentes para hacer frente a los riesgos de las ciberamenazas. La descripción 'N/A' indica que el artículo no es aplicable a esa clasificación y control. Tras el mapa de calor se encuentran los controles técnicos, así como su cumplimiento identificado durante las entrevistas.

El Mapa Referencial NIST más abajo expuesto es la representación ideal de una implementación para una organización según el NIST.

En el mapa de calor MEC, la imagen "**Estado MEC**" es el resultado de las entrevistas representadas en el mapa de calor.

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

Mapa de Calor Referencial NIST

Prioridad Alta			
Controles	Procesos	Humanos	Tecnologicos
C1	[illegible]	50,00	50,00
C2		[illegible]	
C3	50,00	41,67	45,83
C4	53,57		
C5	[illegible]		
C6	50,00		
C7	[illegible]	56,25	56,25
C8			
C9			
C10			
C11			
C12			
C13	N/A	N/A	N/A
C14	50,00	50,00	50,00
C15			
C16	N/A	N/A	N/A
C17	[illegible]	[illegible]	[illegible]
C18	N/A	N/A	N/A

Prioridad Media			
Controles	Procesos	Humanos	Tecnologicos
C1			50,00
C2		[illegible]	[illegible]
C3		[illegible]	50,00
C4	[illegible]		
C5	[illegible]		
C6	50,00	[illegible]	[illegible]
C7		[illegible]	[illegible]
C8			
C9			
C10			
C11			
C12			
C13	[illegible]	[illegible]	58,33
C14		50,00	
C15		58,33	58,33
C16	[illegible]	43,18	[illegible]
C17	[illegible]	[illegible]	[illegible]
C18	[illegible]	[illegible]	

Prioridad Baja			
Controles	Procesos	Humanos	Tecnologicos
C1	[illegible]	[illegible]	[illegible]
C2	[illegible]	[illegible]	
C3			
C4	[illegible]	50,00	[illegible]
C5	N/A	N/A	N/A
C6	[illegible]	50,00	
C7	N/A	N/A	N/A
C8			
C9			
C10	N/A	N/A	N/A
C11	N/A	N/A	N/A
C12			
C13	45,00	[illegible]	60,00
C14	N/A	N/A	N/A
C15			
C16			
C17			
C18	[illegible]	[illegible]	

Tabla 3 - Largo Plazo

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

Mapa de Calor MEC

Estado MEC			
ntroles	Procesos	Humanos	Tecnologicos
C1			0,0(
C2	0,00	0,00	0,0(
C3			0,0(
C4	0,00	0,00	0,0(
C5	0,00	0,00	0,0(
C6	0,00	0,00	0,0(
C7	0,00	0,00	0,0(
C8	0,00	0,00	0,0(
C9	0,00	0,00	0,0(
C10	0,00	0,00	0,0(
C11			0,0(
C12	0,00	0,00	0,0(
C13			
C14	0,00	0,00	0,0(
C15	0,00	0,00	0,0(
C16			
C17	0,00	0,00	0,0(
C18	0,00	0,00	0,0(

Tabla 1 - Corto Plazo

Prioridad Alta			
Controles	Procesos	Humanos	Tecnologicos
C1		50,00	50,00
C2			
C3	50,00	41,67	45,83
C4	53,57		
C5			
C6	50,00		
C7		56,25	56,25
C8			
C9			
C10			
C11			
C12			
C13	N/A	N/A	N/A
C14	50,00	50,00	50,00
C15			
C16	N/A	N/A	N/A
C17			
C18	N/A	N/A	N/A

Tabla 1 - Corto Plazo

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Glosario

Este informe sigue el estándar de nomenclatura Internacional:

Amenaza: causa potencial de un incidente, que podría resultar en daño.
Activo: cualquier bien que tenga valor para la organización.
Confidencialidad: Que no está disponible ni se revela a personas no autorizadas.
Disponibilidad: Que es accesible y utilizable por una entidad autorizada.
Impacto: daños y/o perjuicios resultantes de la explotación de una vulnerabilidad.
Integridad: salvaguardar la precisión y la integridad de los activos.
Probabilidad – Factor matemático que sugiere la posibilidad de un hecho.
Riesgo – Combinación de la probabilidad de un evento y sus impactos.
Vulnerabilidad: Fragilidad que puede ser explotada por una amenaza.
SI – Seguridad de la Información.
PSI - Política de Seguridad de la Información.
IP – Privacidad de la Información.
TI – Tecnologías de la Información.
PD - Datos Personales
SGSI – Sistema de Gestión de Seguridad de la Información.
BCM – Gestión de la Continuidad del Negocio.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Actividades

Entre el 19/01/2023 y el 03/03/2023, se llevó a cabo el proyecto Gap Análisis CIS a través de entrevistas con los directores, jefes y responsables de TIC del Ministerio de Educación (MEC), mediante análisis de procedimientos operativos y validación tecnológica, con el fin de comprender las actividades rutinarias en la materia.

A continuación, se detallan las actividades realizadas:

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

1.1. Inventario y control de activos corporativos

Detalles de las Medidas de Seguridad

En esta sección detallaremos el estado de las medidas de seguridad del Control de Inventarios y Control de Activos Corporativos a través de la siguiente tabla. Si desea comprobar las respuestas dadas, consulte el Apéndice B.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un inventario detallado de activos	Buenas Practicas	Buenas Practicas	-
[redacted]	Dispositivos No autorizados	-	-	-
[redacted]	Utilice una herramienta de descubrimiento de Activos	-	-	-
[redacted]	Utilice el registro del protocolo de configuración dinámica de host (DHCP) para actualizar el inventario de activos empresariales	-	-	-
[redacted]	Utilice una herramienta de descubrimiento pasivo	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión de activos de TI, el documento debe de establecer y mantener un inventario preciso, detallado y actualizado de todos los activos de la empresa con el potencial de almacenar o procesar datos, incluidos: dispositivos de usuario final (incluidos dispositivos portátiles y móviles), dispositivos de red, dispositivos IoT, servidores y todo el hardware , estén o no conectados a la red de la organización.

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

2.1. Inventario y control de activos de software

Detalles de las Medidas de Seguridad

En esta sección, detallaremos el estado de las medidas de seguridad de Control de Inventario y Control de Activos de Software a través de la siguiente tabla. Si desea comprobar las respuestas dadas, consulte el Apéndice B.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un inventario detallado de software	-	-	-
[redacted]	Asegurarse de que el software actual esté en soporte	-	-	-
[redacted]	Identificar el Software no autorizado	-	-	-
[redacted]	Utilice Herramientas de Automatización de Inventario	-	-	-
[redacted]	Lista Blanca de Software	-	-	-
[redacted]	Lista Blanca de Librerías	-	-	-
[redacted]	Lista Blanca para Script Autorizados	-	-	-

Recomendaciones

Implemente un proceso automatizado o manual para identificar activos de hardware no autorizados.

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

3.1 Protección de Datos

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad del control de Protección de Datos. Si desea comprobar las respuestas, consulte el Apéndice B.

ID	Detalles	Procesos	Humanos	Tecnológico
	Establecer y mantener un proceso de gestión de Datos	Buenas Practicas	Parte del Proceso	Parte del Proceso
	Establecer y mantener un inventario de Datos	-	-	-
	Configurar listas de control de acceso a datos	Parcialmente Escrito	Parte del Proceso	Parte del Proceso
	Hacer cumplir la retención de datos	Buenas Practicas	Parte del Proceso	Parte del Proceso
	Eliminación segura de datos	-	.	.
	Cifre los datos en los dispositivos de los usuarios finales	-	-	-
	Establecer y mantener un esquema de clasificación de datos	-	.	.
	Flujos de datos de documentos	-	.	.
	Cifrar datos en medios extraíbles	-	-	-
	Cifrar datos confidenciales en tránsito	-	-	-
	Cifrar datos confidenciales en repositorios	-	-	-
	Procesamiento y almacenamiento de datos de segmentos en función de la sensibilidad	.	.	.
	Integrar una Solución de DLP	-	.	.
	Registro de acceso a datos confidenciales	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión de Protección de Datos, que incluya:

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

- Proceso de Gestión de Datos
- Inventario de información confidencial
- Protección de la información a través de listas de control de acceso
- Eliminación de datos confidenciales o sistemas a los que no se accede
- Cifrado de datos en dispositivos de usuario
- Política de clasificación de datos
- Proceso de flujo de datos
- Cifrado de datos en dispositivos de almacenamiento USB (si aplica)
- Cifrado de datos confidenciales en tránsito
- Cifrado de datos confidenciales en repositorios
- Segmentación de red basada en la sensibilidad de la aplicación
- Habilitación de registros detallados para el acceso o cambios a datos confidenciales.

4.1 Configuración segura de activos y software corporativos

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad de la Configuración Segura de los Activos y el control del Software a través de la siguiente tabla. Si desea comprobar las respuestas dadas, consulte el Apéndice B.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un proceso de configuración seguro	-	-	-
[redacted]	Establecer y mantener un proceso de configuración seguro para la infraestructura de red	-	-	-
[redacted]	Configurar el bloqueo de sesión automático en activos empresariales	-	-	-
[redacted]	Implementar y Administrar un Firewall en Servidores	-	-	-
[redacted]	Implementar y administrar un firewall en dispositivos de usuario final	-	-	-
[redacted]	Gestione de forma segura los activos y el software de la empresa	-	-	-
[redacted]	Administrar cuentas predeterminadas	-	-	-

GEORGE TEMPERLET

GRUPO HORUS

GRUPO HORUS S.A.

	en activos y software empresariales			
	Desinstale o deshabilite los servicios innecesarios en los activos y el software de la empresa	-	-	-
	Configurar servidores DNS de confianza en activos empresariales	-	-	-
	Hacer cumplir el bloqueo automático de dispositivos en dispositivos portátiles de usuario final	-	-	-
	Hacer cumplir la capacidad de borrado remoto en dispositivos portátiles de usuario final	-	-	-
	Espacios de trabajo empresariales independientes en dispositivos móviles de usuario final	-	-	-

Recomendaciones

Preparar un documento que describa los procesos para gestionar la Configuración Segura de los activos y software corporativos, que incluya:

- Línea de base de entornos seguros;
- Línea de base de la configuración de seguridad predeterminada para dispositivos de red;
- Uso de cortafuegos basados en host o filtrado de puertos;
- Uso de cortafuegos basados en dispositivos de usuario final;
- Cambio de contraseñas predeterminadas;
- Línea de base para garantizar que solo se estén ejecutando los puertos, protocolos y servicios aprobados;
- Configuración de DNS de confianza;
- Bloqueo automático de intentos fallidos de inicio de sesión;
- Gestión remota de dispositivos portátiles;

5.1 Gestión de cuentas

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad de la Gestión de Cuentas corporativas.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un inventario de cuentas	-	-	-
[redacted]	Utilice contraseñas únicas	-	-	-
[redacted]	Deshabilitar cuentas inactivas	-	-	-
[redacted]	Restringir privilegios de administrador a cuentas de administrador dedicadas	-	-	-
[redacted]	Establecer y mantener un inventario de cuentas de servicio	-	-	-
[redacted]	Gestión de cuentas centralizada	-	-	-

Recomendaciones

Preparar un documento que describa los procesos de gestión de cuentas, que incluya:
Inventario de cuenta actualizado;

- Uso de contraseñas únicas;
- Desactivación de cuentas inactivas;
- Uso de cuentas administrativas dedicadas;
- Inventario de cuentas de servicio;
- Configuración del punto de autenticación centralizada

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

6.1 Gestión de Control de Acceso

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad de la Gestión de Acceso.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer un proceso de concesión de acceso	-	-	-
[redacted]	Establecer un proceso de revocación de acceso	-	-	-
[redacted]	Requerir MFA para aplicaciones expuestas externamente	-	-	-
[redacted]	Requerir MFA para el acceso remoto a la red	-	-	-
[redacted]	Requerir MFA para acceso administrativo	-	-	-
[redacted]	Establecer y mantener un inventario de sistemas de autenticación y autorización	-	-	-
[redacted]	Control de acceso centralizado	-	-	-
[redacted]	Definir y mantener el control de acceso basado en roles	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de Gestión de Controles de Seguridad, que incluya:

- Uso de autenticación multifactor para aplicaciones expuestas externamente
- Uso de autenticación multifactor en todos los inicios de sesión remotos
- Uso de autenticación multifactor para todos los accesos administrativos

7.1 Gestión Continua de Vulnerabilidades

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad de la Gestión Continua de Vulnerabilidades.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un proceso de gestión de vulnerabilidades	-	-	-
[redacted]	Establecer y mantener un proceso de mitigación	-	-	-
[redacted]	Realice la gestión automatizada de parches del sistema operativo	-	-	-
[redacted]	Realice la gestión automatizada de parches de aplicaciones	-	-	-
[redacted]	Realice exploraciones automatizadas de vulnerabilidades de los activos internos de la empresa	-	-	-
[redacted]	Realice exploraciones automatizadas de vulnerabilidades de activos empresariales expuestos externamente	-	-	-
[redacted]	Mitigar vulnerabilidades detectadas	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión continua de vulnerabilidades, que incluya:

- Proceso de gestión de vulnerabilidades
- Clasificación del riesgo de vulnerabilidad y estrategia de mitigación
- Verificación periódica de vulnerabilidades en un ambiente interno
- Verificación periódica de las vulnerabilidades de los activos expuestos externamente
- Calificación del riesgo de vulnerabilidad y estrategia de mitigación.

8.1 Gestión de Registros de Auditoría

Detalles de las Medidas de Seguridad

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

En este apartado, detallaremos el estado de las medidas de seguridad de la Gestión de Registros de Auditoría.

ID	Detalles	Procesos	Humanos	Tecnológico
	Establecer y mantener un proceso de gestión de registros de auditoría	-	-	-
	Recopilar registros de auditoría	-	-	-
	Garantice un almacenamiento adecuado de registros de auditoría	-	-	-
	Estandarizar la sincronización de NTP	-	-	-
	Recopile registros de auditoría detallados	-	-	-
	Recopilar registros de auditoría de consultas de DNS	-	-	-
	Recopilar registros de auditoría de solicitudes de URL	-	-	-
	Recopilar registros de auditoría de línea de comandos	-	-	-
	Centralice los registros de auditoría	-	-	-
	Conservar registros de auditoría	-	-	-
	Realizar revisiones de registros de auditoría	-	-	-
	Recopilar registros del proveedor de servicios	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión de registros de auditoría, que incluya:

- Registro y recopilación de registros de auditoría;
- Habilitación del registro de consultas de DNS;
- Habilitación del registro de auditoría de la línea de comandos;
- Recopilación de registros del proveedor de servicios

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

9.1 Protecciones de Correo Electrónico y Navegador Web

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad de la protección de correo electrónico y navegador web.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Asegúrese de usar solo navegadores y clientes de correo electrónico totalmente compatibles	-	-	-
[redacted]	Utilice los servicios de filtrado de DNS	-	-	-
[redacted]	Mantener y hacer cumplir los filtros de URL basados en la red	-	-	-
[redacted]	Restrinja las extensiones innecesarias o no autorizadas del navegador y del cliente de correo electrónico	-	-	-
[redacted]	Implementar DMARC	-	-	-
[redacted]	Bloquear tipos de archivos innecesarios	-	-	-
[redacted]	Implementar y mantener servidores de correo electrónico Anti-Malware Protegidos	-	-	-

Recomendaciones

Preparar un documento que describa los procesos para administrar el correo electrónico y las protecciones del navegador web.

10.1 Defensas Contra Malware

Detalles de las Medidas de Seguridad

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

En este apartado, detallaremos el estado de las medidas de seguridad de la defensa contra malware.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Implementar y mantener software antimalware	-	-	-
[redacted]	Configurar actualizaciones automáticas de firmas antimalware	-	-	-
[redacted]	Deshabilite la ejecución automática y la reproducción automática para medios extraíbles	-	-	-
[redacted]	Configurar el análisis antimalware automático de medios extraíbles	-	-	-
[redacted]	Habilitar funciones contra la explotación	-	-	-
[redacted]	Administre de forma centralizada el software antimalware	-	-	-
[redacted]	Usar software antimalware basado en el comportamiento	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión contra malware, que incluya:

- Procedimientos de Mitigación
- Procedimiento de Recovery
- Procedimiento de notificación

11.1 Recuperación de Datos

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad para la recuperación de datos.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un proceso de	Buenas	Parte del	Parte del

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

	recuperación de datos	Practicas	Proceso	Proceso
	Realizar copias de seguridad automatizadas	Buenas Practicas	Parte del Proceso	Parte del Proceso
	Proteger Recovery Data	-	-	-
	Establecer y mantener una instancia aislada de datos de recuperación	-	-	-
	Test de Data Recovery	-	-	-

Recomendaciones Preparar un documento que describa los procesos de gestión de la Recuperación de Datos.

12.1 Gestión de Infraestructura de Red

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad para la gestión de infraestructura de red.

ID	Detalles	Procesos	Humanos	Tecnológico
	Asegúrese de que la infraestructura de red esté actualizada	-	-	-
	Establecer y mantener una arquitectura de red segura	-	-	-
	Gestione de forma segura la infraestructura de red	-	-	-
	Establecer y mantener diagramas de arquitectura	-	-	-
	Centralice la autenticación, autorización y auditoría de red (AAA)	-	-	-
	Uso de Protocolos de Comunicación y Gestión de Redes Seguras	-	-	-

GEORGE TEMPERLEY
GRUPO HORUS
Grupo Horus S.A.

	Asegúrese de que los dispositivos remotos utilice una VPN y se conecten a la infraestructura AAA de una empresa	-	-	-
	Establecer y mantener recursos informáticos dedicados para todo el trabajo administrativo	-	-	-

Recomendaciones

Preparar un documento que describa los procesos de gestión de la infraestructura de red, que incluya:

- Diseño topológico de la Red
- Uso de protocolos de autenticación segura.
- Protocolo de Almacenamiento de contraseña de red

13.1 Monitoreo y Defensa de la Red

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad para el monitoreo y defensa de la red.

ID	Detalles	Procesos	Humanos	Tecnológico
	Centralice las alertas de eventos de seguridad	-	-	-
	Implemente una solución de detección de intrusos basada en host	-	-	-
	Implemente una solución de detección de intrusos en la red	-	-	-
	Realizar filtrado de tráfico entre segmentos de red	-	-	-
	Administrar el control de acceso para activos remotos	-	-	-
	Recopilar registros de flujo de tráfico de red	-	-	-

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

	Implemente una solución de prevención de intrusiones basada en host	-	-	-
	Implemente una solución de prevención de intrusiones en la red	-	-	-
	Implementar control de acceso a nivel de puerto	-	-	-
	Realizar filtrado de capa de aplicación	-	-	-
	Ajuste los umbrales de alerta de eventos de seguridad	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión de monitoreo y defensa de la red, que incluya:

- SIEM o herramientas de análisis de registros;
- Despliegue de sensores IDS basados en host;
- Despliegue de sensores IDS basados en red;
- Filtrado de cortafuegos entre VLAN/segregación de red lógica;
- Gestión de todos los dispositivos que se autentican de forma remota en la red interna;
- Recopilación de flujo de datos;
- Implementación de IPS basada en host;
- Despliegue de IPS basados en red;
- Control de acceso a nivel de puerto y uso de certificados de cliente para autenticar activos de hardware;
- Implementación de firewalls de aplicaciones (WAF - Web Application Firewall);
- Ajuste regular SIEM.

GEORGE TEMPERLEY

GRUPO HORUS
GRUPO HORUS S.A.

14.1 Concientización sobre Seguridad y Capacitación en Habilidades

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad en concienciación y capacitación en seguridad.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un programa de concientización sobre seguridad	-	-	-
[redacted]	Capacite a los miembros de la fuerza laboral para que reconozcan los ataques de ingeniería social	-	-	-
[redacted]	Capacite a los miembros de la fuerza laboral sobre las mejores prácticas de autenticación	-	-	-
[redacted]	Capacitar a la fuerza laboral en las mejores prácticas de manejo de datos	-	-	-
[redacted]	Capacitar a los miembros de la fuerza laboral sobre las causas de la exposición de datos no intencional	-	-	-
[redacted]	Capacitar a los miembros de la fuerza laboral sobre el reconocimiento y la notificación de incidentes de seguridad	-	-	-
[redacted]	Capacitar a la fuerza laboral sobre cómo identificar e informar si a sus activos empresariales les faltan actualizaciones de seguridad	-	-	-
[redacted]	Capacitar a la fuerza laboral sobre los peligros de conectarse y transmitir datos empresariales a través de redes inseguras	-	-	-
[redacted]	Llevar a cabo capacitación en habilidades y concientización sobre seguridad para roles específicos	-	-	-

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Recomendaciones

Elaborar un documento que describa los procesos de capacitación, que incluya:

- Capacitación de la fuerza laboral sobre las causas de la exposición no intencional de datos;
- Capacitación de los miembros de la fuerza laboral en la identificación y notificación de incidentes;
- Capacitación de los miembros de la fuerza laboral en la identificación de software obsoleto;
- Capacitación para mejorar las habilidades en seguridad de la información.

15.1 Gestión de Proveedores de Servicios

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad en la gestión de proveedores de servicios.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un inventario de proveedores de servicios	-	-	-
[redacted]	Establecer y mantener una política de gestión de proveedores de servicios	-	-	-
[redacted]	Clasificar proveedores de servicios	-	-	-
[redacted]	Asegúrese de que los contratos de los proveedores de servicios incluyan requisitos de seguridad	-	-	-
[redacted]	Evaluar proveedores de servicios	-	-	-
[redacted]	Supervisión de proveedores de servicios	-	-	-
[redacted]	Proveedores de servicios de desmantelamiento seguro	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión con los proveedores, que

GEORGE TEMPERLEY
GRUPO HORUS

incluya:

- Recomendar la evaluación y el mantenimiento de proveedores en seguridad, el objetivo es que los proveedores en este punto no cambien constantemente ya que manejan información sensible.

16.1 Seguridad de la Aplicación

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad a nivel de aplicaciones.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un proceso seguro de desarrollo de aplicaciones	-	-	-
[redacted]	Establezca y mantenga un proceso para aceptar y abordar las vulnerabilidades del software	-	-	-
[redacted]	Realice un análisis de causa raíz de las vulnerabilidades de seguridad	-	-	-
[redacted]	Establezca y administre un inventario de componentes de software de terceros	-	-	-
[redacted]	Use componentes de software de terceros confiables y actualizados	-	-	-
[redacted]	Establecer y mantener un sistema y proceso de clasificación de la gravedad para las vulnerabilidades de las aplicaciones	-	-	-
[redacted]	Usar plantillas de configuración de protección estándar para la infraestructura de aplicaciones	-	-	-
[redacted]	Sistemas separados de producción y no producción	Buenas Practicas	La Mayoría de los Sistemas	La Mayoría de los Sistemas
[redacted]	Capacite a los desarrolladores en	-	-	-

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A

	conceptos de seguridad de aplicaciones y codificación segura			
	Aplicar principios de diseño seguro en arquitecturas de aplicaciones	-	-	-
	Aproveche los módulos o servicios examinados para los componentes de seguridad de aplicaciones	-	-	-
	Implementar comprobaciones de seguridad a nivel de código	-	-	-
	Realizar pruebas de penetración de aplicaciones	-	-	-
	Realizar modelado de amenazas	-	-	-

Recomendaciones

Evaluar la aprobación de las recomendaciones del CERT sobre "Criterios mínimos de seguridad para el desarrollo y adquisición de software"

17.1 Gestión de Respuesta a Incidentes

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad a nivel de la gestión de respuesta a incidentes.

ID	Detalles	Procesos	Humanos	Tecnológico
	Designar personal para gestionar el manejo de incidentes	-	-	-
	Establecer y mantener información de contacto para informar incidentes de seguridad	-	-	-
	Establezca y mantenga un proceso empresarial para informar incidentes	-	-	-

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

[redacted]	Establecer y mantener un proceso de respuesta a incidentes	-	-	-
[redacted]	Asignar funciones y responsabilidades clave	-	-	-
[redacted]	Definir mecanismos para comunicarse durante la respuesta a incidentes	-	-	-
[redacted]	Realizar ejercicios de respuesta a incidentes de rutina	-	-	-
[redacted]	Realizar revisiones posteriores al incidente	-	-	-
[redacted]	Establecer y mantener umbrales de incidentes de seguridad	-	-	-

Recomendaciones

Desarrollar un documento que describa los procesos de gestión de respuesta a incidentes, que incluya:

- Equipo para gestionar el manejo de incidentes;
- Información de contacto para reportar incidentes de seguridad;
- Proceso comercial para reportar incidentes;
- proceso de respuesta a incidentes;
- Asignación de roles y responsabilidades esenciales;
- Definición de mecanismos de comunicación durante la respuesta a incidentes;
- Realización de ejercicios de respuesta a incidentes de rutina;
- Realización de análisis posteriores al incidente;
- Establecimiento de umbrales de incidentes de seguridad.

18.1 Pruebas de Penetración

Detalles de las Medidas de Seguridad

En este apartado, detallaremos el estado de las medidas de seguridad a nivel del test de penetración.

ID	Detalles	Procesos	Humanos	Tecnológico
[redacted]	Establecer y mantener un programa de pruebas de penetración	-	-	-

GEORGE TEMPERLEY

GRUPO HORUS

GRUPO HORUS S.A.

[redacted]	Realice pruebas periódicas de penetración externa	-	-	-
	Mitigación los resultados de la prueba de penetración	-	-	-
	Validar Medidas de Seguridad	-	-	-
	Realice pruebas periódicas de penetración interna	-	-	-

Recomendaciones

Elaborar un documento que describa los procesos de gestión de respuesta a incidentes que incluya:

- Programa de Pruebas de Seguridad;
- Realización de pruebas periódicas de seguridad externa;
- Remediación de los hallazgos de la prueba del test de seguridad;
- Validación de medidas de seguridad;
- Realización de pruebas periódicas de test de seguridad interna.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Anexo A: Plan de Acción "Quick Wins"

CSC	Riesgos Asociados	Acción Organizativa	Acción Técnica
	No contar con una herramienta que analice los logs de las IP asignadas en la red puede comprometer la seguridad aplicada a la infraestructura y sistemas de red. Es importante identificar si el nombre de host asociado a la IP es parte de los activos de la organización. Un nuevo dispositivo se puede conectar a la red y puede infectar o usar herramientas de rastreo para recopilar datos confidenciales.	Elaborar una política de uso de activos, un procedimiento de configuración y administración de activos y actualizar la PSI.	Utilice una herramienta para actualizar el inventario en función de los registros del servidor DHCP, si no tiene otra solución de inventario automatizado.
	No tener una política o procedimiento definido puede comprometer a la empresa. El software descontinuado por el fabricante puede contener vulnerabilidades que no serán reparadas en tiempo y forma al no contar con el soporte necesario.	Actualice la PSI de Inventario de activos indicando el procedimiento para la garantía del software por parte del fabricante y el mínimo de años de vida útil solicitado. Ejemplo: Política de Uso de Activos, Gestión de Activos y Procedimiento de Configuración.	Instale Agentes en todos los dispositivos de servidor y estaciones de trabajo (Windows, Linux o MacOS)
	No tener una política o procedimiento definido puede comprometer ya que se podría perder el registro de los activos y esto lleve a tener activos desconocidos.	Actualizar la PSI en el inventario de activos de software Ejemplo: Política de Uso de Activos, Gestión de Activos y Procedimiento de Configuración.	Herramienta existente.
	No tener un control de las	Actualizar PSI en el uso	Configure el software

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

bibliotecas necesarias para el funcionamiento de las aplicaciones puede comprometer la seguridad aplicada en el entorno, permitiendo la carga de bibliotecas maliciosas al inicio del sistema.	de bibliotecas autorizadas incluidas en la lista blanca Ejemplo: Política de Uso de Activos, Gestión de Activos y Procedimiento de Configuración.	de la lista blanca de la organización para que solo las bibliotecas de software autorizadas (como *.dll, *.ocx, *.so, etc.) puedan cargarse durante el inicio del sistema.
No tener control sobre los scripts necesarios para el funcionamiento de las aplicaciones puede comprometer la seguridad aplicada en el entorno, posibilitando la carga de scripts maliciosos al inicio del sistema.	Actualizar PSI en el uso de bibliotecas autorizadas incluidas en la lista blanca Ejemplo: Política de Uso de Activos, Gestión de Activos y Procedimiento de Configuración.	Limite el uso de lenguajes de secuencias de comandos innecesarios en navegadores y clientes de correo electrónico. Incluyendo el uso de lenguajes como ActiveX y JavaScript en sistemas donde no es necesario soportar tales funciones. Mapee todos los usuarios que necesitan usar dichas herramientas, como administradores de red o desarrolladores de software;
No tener una política o procedimiento definido puede comprometer los datos, sensibles y confidenciales en los activos de la empresa, lo que puede ocasionar fugas (no intencionales) de datos de la organización. Cada violación de Datos Personales puede costar hasta el 2% de los ingresos anuales de la empresa o cincuenta millones de reales. Cabe mencionar que, si los datos filtrados pueden ser secretos	Actualizar PSI en el proceso de gestión de datos confidenciales Ejemplo: Política de Protección de Datos Personales, Procedimiento de Gestión de Privacidad	Instale una solución de gestión de datos que pueda clasificar la confidencialidad, la propiedad, el manejo, el tiempo de retención de datos y la eliminación segura de datos

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

industriales o comerciales, valen mucho más que eso, a pesar de no estar sujetos a la Ley General de Protección de Datos Personales		
Sin un mapeo de datos adecuado, la organización no tiene visibilidad de los sistemas que manejan datos personales, sensibles o confidenciales, lo que dificulta identificar la fuente de la fuga de datos. Con los datos inventariados es posible saber exactamente a qué se accedió, para poder calcular la extensión exacta del máximo daño posible a causar a la Organización, en base a lo que accedió el agente hostil.	Actualizar PSI en el proceso de gestión de datos confidenciales Ejemplo: Política de Protección de Datos Personales, Procedimiento de Gestión de Privacidad	Establezca y mantenga un proceso de gestión de datos que aborde lo siguiente: La sensibilidad de los datos; El propietario; El manejo; El tiempo de retención; Requisitos de eliminación, basados en la sensibilidad de la empresa y los estándares de retención. NOTA: Revise y actualice la documentación anualmente o cuando ocurran cambios significativos dentro de la empresa.
Los datos personales, sensibles o confidenciales deben conservarse durante el período máximo de actividad. Los datos que ya cumplieron su propósito no deben estar disponibles en el sistema, evitando así la fuga de información.	Actualizar PSI sobre el tiempo de retención requerido de datos sensibles y confidenciales según el proceso de gestión de datos Ejemplo: Política de Retención, Política de Protección de Datos Personales, Procedimiento de Gestión de Privacidad	Aplicar un procedimiento que conserve los datos de acuerdo con el proceso de gestión de datos de la empresa (mapeo de datos). La retención de datos debe incluir horarios mínimos y máximos.
La disposición indebida de datos personales, sensibles	Actualizar PSI en el proceso de gestión de	Asegúrese que los dispositivos

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

y confidenciales puede comprometer el negocio, a través de la fuga de información importante descartada, eliminada de forma insegura, sin seguir los procedimientos definidos por la organización.	datos confidenciales	defectuosos que contienen almacenamiento de datos, como HDD, SSD, Pen Drive, etc. se destruyen de tal manera que los datos no se puedan recuperar. Evaluar las cláusulas de confidencialidad para las empresas que realizan el mantenimiento de los dispositivos, asegurando que la información recuperada de los dispositivos no pueda ser divulgada.
Asegúrese de que todos los datos personales, sensibles o confidenciales estén clasificados y etiquetados. Esta información de clasificación debe incluirse en el PSI.	Establecer y mantener un proceso de clasificación de datos para la empresa. Las empresas pueden usar etiquetas como "Sensible", "Confidencial" y "Público" y clasificar sus datos de acuerdo con estas etiquetas.	Finalice la asignación de datos que está en curso y luego ordene los datos.
No contar con un flujo de datos mapeado y actualizado dificulta la comprensión de la regla de negocio de la empresa e imposibilita la identificación de fallas en el proceso. Es importante mantener un flujo de datos bien documentado para ayudar a identificar las mejoras del proceso y las fallas potenciales.	Establezca y mantenga un proceso de flujo de datos documentado, incluido el proveedor de servicios, que debe basarse en el proceso de gestión de datos de la empresa.	Finalice el mapeo de datos que está en progreso y luego cree el flujo de datos, identificando el ciclo de vida de la información.
No aplicar el cifrado en los medios extraíbles puede comprometer la	Crear y actualizar PSI con Política de Protección de	Asegurar que en los casos excepcionales de uso de medios

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

confidencialidad y la integridad de los datos almacenados; personal no autorizado puede acceder a los medios extraíbles que contienen datos personales, sensibles o confidenciales, lo que puede provocar una fuga de datos de la empresa.	Información Personal, Procedimiento de Gestión de Privacidad, Política de Control de Acceso.	removibles, el pendrive esté encriptado permitiendo la confidencialidad e integridad de la información. Si no tiene una solución de cifrado, asegúrese de que al menos todos los datos estén comprimidos con una contraseña simétrica.
No tener una política o procedimiento definido puede comprometer a la fuerza laboral en fallas en el manejo y tratamiento de datos personales, sensibles y confidenciales en los activos de la empresa, lo que puede ocasionar fugas (no intencionales) de datos de la organización. Asegúrese de que toda la comunicación se realice a través de protocolos seguros.	Crear y actualizar PSI con Política de Protección de Información Personal, Procedimiento de Gestión de Privacidad, Política de Control de Acceso.	Utilice HTTPS para el acceso a la intranet, evitando el tráfico de información en texto sin formato, incluidas las credenciales de los usuarios.
Los datos personales, sensibles o confidenciales en repositorios/almacenados, cuando no están encriptados, pueden ser leídos o manipulados por personas no autorizadas.	Crear y actualizar PSI con Política de Protección de Información Personal, Procedimiento de Gestión de Privacidad, Política de Control de Acceso.	Asegúrese de que toda la información confidencial almacenada en los sistemas esté encriptada y requiera un mecanismo de autenticación secundario, no integrado en el sistema operativo, para acceder a ella.
El no tener implementada una solución de prevención de pérdida de datos permite el acceso a datos confidenciales sin ningún tipo de alerta o monitoreo,	Crear Política de Protección de Datos Personales, Procedimiento para la Gestión de la Privacidad y actualización sobre	Identifique toda la información confidencial almacenada, procesada o transmitida por los

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

	imposibilitando identificar quién está accediendo, copiando, transfiriendo o compartiendo la información.	PSI.	sistemas tecnológicos de la organización, incluida la que se encuentra localmente o en un proveedor de servicios remoto, y actualice el inventario de información confidencial de la organización".
	No tener implementada una herramienta de monitoreo de integridad de archivos (FIM) o administración y correlación de eventos de seguridad (SIEM) hace que sea imposible realizar un registro de auditoría o crear una alerta que sea capaz de identificar quién está accediendo, copiando, transfiriendo o compartiendo la información.	Crear Política de Protección de Datos Personales, Procedimiento para la Gestión de la Privacidad y Actualización sobre PSI.	Habilite el registro de auditoría detallado para acceder a información confidencial, registro de acceso, modificación y eliminación a través de la herramienta de monitoreo de integridad de archivos (FIM) o administración y correlación de eventos de seguridad (SIEM).
	Todos los puntos finales deben protegerse y considerarse como vectores potenciales de acceso a personas no autorizadas.	Crear una Política o Procedimiento de configuración de puntos finales.	Escribir sobre las configuraciones mínimas de seguridad.
	No tener una política o proceso de acceso administrativo definido puede comprometer a la organización en fallas en la configuración de los activos de la organización, dejando el ambiente vulnerable a amenazas conocidas.	Crear procedimiento y actualizar PSI sobre gestión de activos de forma segura. Ejemplo: Procedimiento de Gestión de Activos y Configuración, Procedimiento de Administración de Red	Escribir sobre las configuraciones mínimas de seguridad.
	No tener una política o proceso de configuración seguro definido puede comprometer a la organización al configurar incorrectamente los activos	Crear un procedimiento de gestión de configuración y activos, un procedimiento de administración de red y actualizar PSI	Describir la configuración segura del DNS

GEORG LEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A

de la organización, dejando el entorno vulnerable a amenazas conocidas.		
Los dispositivos móviles o portátiles de los usuarios finales pueden contener datos confidenciales de la empresa; si el dispositivo se pierde o es robado, existe el riesgo de que se acceda a esta información, lo que permite la fuga de información confidencial.	Crear un procedimiento de gestión de configuración y activos, una política de uso de activos, una política de trabajo remoto y actualice el PSI	Implementar una solución MDM - Administración de dispositivos móviles para teléfonos celulares y tabletas corporativas.
Los dispositivos móviles o portátiles de los usuarios finales pueden contener datos confidenciales de la empresa; si el dispositivo se pierde o es robado, existe el riesgo de que se acceda a esta información, lo que permite la fuga de información confidencial.	Crear un procedimiento de gestión de configuración y activos, una política de uso de activos, una política de trabajo remoto y actualice el PSI	Implementar una solución MDM - Administración de dispositivos móviles para teléfonos celulares y tabletas corporativas.
No tener una política o proceso definido para el uso de Multi-Factor Authentication (MFA) para sistemas expuestos a internet puede comprometer a la organización en fallas en la configuración de los activos de la organización, dejando el ambiente vulnerable a amenazas conocidas.	Actualizar PSI en el proceso de gestión de acceso mediante MFA Ejemplo: Política de control de acceso, Procedimiento de gestión de acceso	Utilizar MFA para todas las aplicaciones corporativas o de terceros expuestas externamente.
No tener una política o proceso definido para el uso de Multi-Factor Authentication (MFA) para sistemas expuestos a internet puede comprometer a la organización en fallas en la configuración de los activos de la organización, dejando el ambiente vulnerable a amenazas	Actualizar PSI en el proceso de gestión de acceso mediante MFA Ejemplo: Política de control de acceso, Procedimiento de gestión de acceso	Habilitar el uso de MFA para el acceso remoto a la red, pudiendo hacer una combinación de certificado + usuario y contraseña, o token cuando esté disponible.

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A

conocidas.		
No tener una política o proceso definido para el uso de Multi-Factor Authentication (MFA) para sistemas expuestos a internet puede comprometer a la organización en fallas en la configuración de los activos de la organización, dejando el ambiente vulnerable a amenazas conocidas.	Actualizar PSI en el proceso de gestión de acceso mediante MFA Ejemplo: Política de control de acceso, Procedimiento de gestión de acceso	Validar que todos los accesos administrativos (de gestión) admitan el uso de MFA. De lo contrario, asegúrese de que los accesos se realicen solo con protocolos seguros.
Sin un proceso de gestión de vulnerabilidades definido, la organización no puede identificar y abordar las fallas encontradas en el entorno o las aplicaciones, por lo que el atacante puede aprovechar las vulnerabilidades conocidas para obtener acceso a información confidencial o incluso detener los sistema de la empresa.	Crear una Política o Procedimiento para la Gestión de Vulnerabilidades Técnicas Definir el proceso de gestión de vulnerabilidades.	Implementar herramientas para gestión de Incidentes Ejemplo RTIR.
La ausencia de una política o un proceso definido para mitigar las vulnerabilidades puede comprometer a la organización al no escanear los activos de la organización, dejando el entorno vulnerable a las amenazas conocidas.	Crear una Política o Procedimiento para la Gestión de Vulnerabilidades Técnicas	Clasificar las vulnerabilidades encontradas; Garantizar que se prioricen las vulnerabilidades de mayor riesgo; Establezca los plazos esperados para las instalaciones de parches en función de la clasificación de riesgo.
La ausencia de una política o proceso definido para realizar escaneos de vulnerabilidades externas puede comprometer a la organización en fallas en la configuración de los activos	Crear y actualizar el PSI con Política o procedimiento para la Gestión de Vulnerabilidades Técnicas	Documentar y establecer el proceso de gestión de vulnerabilidades para escanear automáticamente todos los sistemas de

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

de la organización, dejando el ambiente vulnerable a amenazas conocidas.		la red, al menos mensualmente, para identificar todas las vulnerabilidades con potencial de ser explotadas en los activos corporativos expuestos externamente.
No documentar los tipos de logs a recopilar puede llevar a la organización a almacenar información que no sirve para procesos de auditoría.	Crear o actualizar la PSI donde clasifique el tipo de logs a ser recopilados.	Garantizar los registros de auditorías de los sistemas críticos.
No recopilar registros de la aplicación le impide realizar las investigaciones de auditoría para identificar el acceso no autorizado a los datos o la información.	Crear o actualizar la PSI que incluya la recopilación de los logs.	Implementar soluciones integradas a soluciones de monitoreo.
No contar con logs de sistema podría llevar a la organización a no detectar fallos de seguridad.	Crear o Actualizar la PSI	Garantizar que todos los activos críticos generen y alojen los logs.
No contar con una correcta sincronización unificada de hora podría llevar a no poder realizar auditorías válidas.	Actualizar la PSI indicando los datos NTP unificados.	Establecer un servidor NTP unificado.
Los registros sin información detallada dificultan el registro de auditoría y evitan que se recopile información importante como la IP de origen, la fecha, la hora, el host, etc.	Crear o Actualiza la PSI	Definir la información necesaria que debe contener la bitácora para cada sistema o dispositivo de red de la organización, en particular y en detalle los activos que manejan datos confidenciales;
No contar con un registro de las líneas de comando ejecutadas en los equipos críticos. Un agente atacante	Crear o Actualizar la PSI	Recopilar los registros de auditoría de línea de comandos. Se debe recopilar

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

puede ejecutar scripts maliciosos a través de las líneas de comando.		registros de auditoría de PowerShell®, BASH™ y terminales administrativas remotas.
Al no contar con un repositorio de log se pueden perder registros necesarios para identificar eventos de seguridad.	Crear o actualice la PSI indicando la utilización de un centralizador de logs	Configurar una syslog centralizado.
Realizar controles periódicos sobre los logs	Crear o Actualizar la PSI	Revisar y clasifique la información obtenida
La ausencia de una política o proceso definido para recopilar registros de los proveedores de servicios puede comprometer la organización en fallas en la configuración de los activos de la organización, lo que puede dejar el entorno vulnerable a amenazas conocidas.	Crear o Actualizar la PSI	Recopilar registros, siempre que sea posible, de las operaciones realizadas a través de los proveedores de servicios. Algunos ejemplos de estas operaciones incluyen: • Recopilación de eventos de autenticación y autorización; • Eventos de Gestión de Usuarios.
No tener habilitado el filtro de consultas DNS se podría abrir brechas de seguridad en el entorno	Crear o actualizar las PSI	El firewall debe realizar un filtrado DNS para identificar solicitudes maliciosas. Y para las estaciones de trabajo que se encuentran en una oficina remota, las consultas DNS también deben de poder filtrarse.
DMARC es un protocolo que utiliza el marco de políticas del remitente, (SPF) y el correo identificado DomainKeys (DKIM) para determinar la autenticidad de un mensaje de correo	Crear o actualizar la PSI que contemple la utilización del protocolo	Implementar el DMARC

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

electrónico.		
Revise las versiones de software mensualmente, o con mayor frecuencia, para verificar si se dispone de actualizaciones de seguridad..	Establecer revisiones de los sistemas dentro de la PSI	Consultar la disponibilidad de actualización o correcciones de seguridad.
Establecer un modelo de seguridad de la infraestructura garantiza poder llevar a cabo controles estándares.	Establecer revisiones de los sistemas dentro de la PSI	Realizar revisiones de compliance.
La transmisión de información por canales no seguros podría ser fácilmente interceptada.	Crear o actualizar las PSI	Forzar el uso de conexión seguras: https, ssh y conexiones VPNs.
Establecer un recurso dedicado para los controles, recurso operativo que pueda realizar un control independiente a los controles técnicos.	Crear o actualizar las PSI	Definir un recurso administrativo para realizar los checklist de los controles y subcontroles.
Los registros descentralizados dificultan el seguimiento de auditoría, lo que permite que los registros importantes no se controlen.	Crear o actualizar las PSI	Utilizar herramientas SIEM e integrar todos los registros de activos, como: AD, Firewall, Antivirus, etc.
La ausencia de alertas de seguridad o la clasificación de gravedad de las alertas dificulta la identificación de un incidente de seguridad. Las alertas creadas indebidamente pueden comprometer el entorno en cuanto al tipo de severidad, aumentando el tiempo de análisis de la anomalía identificada.	Crear la política de seguridad de la red, el procedimiento de administración de la red, la política de gestión de eventos y actualizar la PSI.	Ajustar la herramienta SIEM para alertar sobre eventos de seguridad para clasificar la gravedad de los eventos como crítica, alta, media y baja.
Los empleados sin capacitación específica en el área pueden hacer un mal uso de los activos y	Establecer capacitaciones	Capacitar

GEORGE EMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

	exponer datos confidenciales o debilitar las configuraciones de seguridad aplicadas en el entorno.		
16	N/A	N/A	N/A
	La ausencia de un programa de pruebas de seguridad puede comprometer toda la seguridad aplicada en el entorno al no tener una forma de identificar las fallas que pueden ser explotadas por los agentes de amenazas.	Crear un procedimiento documentado y pautas sobre el programa de pruebas de seguridad y la frecuencia y el alcance de las pruebas	Validar las pruebas realizadas
	Los entornos y las aplicaciones expuestos a Internet pueden contener vulnerabilidades explotadas por atacantes y no ser identificados por el personal. La ausencia de pruebas de seguridad externas periódicas puede comprometer toda la seguridad aplicada a las aplicaciones publicadas para Internet, ya que no hay forma de identificar las fallas que pueden ser aprovechadas por los agentes de amenazas.	Crear un procedimiento documentado y pautas sobre el programa de pruebas de seguridad y la frecuencia y el alcance de las pruebas	Realizar pruebas de seguridad externas periódicas para identificar vulnerabilidades y posibles vectores de ataque que se pueden utilizar para explotar con éxito los sistemas de la empresa
	La ausencia de un procedimiento de mitigación para las vulnerabilidades detectadas deja el entorno o la aplicación vulnerable a los ataques. Se debe aplicar un proceso de mitigación cada vez que se detecta una vulnerabilidad".	Crear un procedimiento documentado y pautas sobre el programa de pruebas de seguridad y la frecuencia y el alcance de las pruebas	Realizar las correcciones necesarias para mitigar las vulnerabilidad detectadas.

GEORGE TEMPERLET
GRUPO HORUS
GRUPO HORUS S.R.

Respuestas de la Organización

Las respuestas a estas subsecciones CIS Controle 1,2 y 3 fueron respondidas por los siguientes responsables de TI:		
MEC	•	Adriana Canclini
MEC	•	Arnaldo Ruiz
MEC	•	Marcos Rotela
Las respuestas a estas subsecciones CIS Controle 4,5,6,7,8,9 y 10 fueron respondidas por los siguientes responsables de TI:		
MEC	•	Adriana Canclini
MEC	•	Arnaldo Ruiz
MEC	•	Gustavo Toledo
MEC	•	Juan Barrios
Las respuestas a estas subsecciones CIS Controle 11,12,13,14,15,16,17 y 18 fueron respondidas por los siguientes responsables de TI:		
MEC	•	Arnaldo Ruiz
MEC	•	Juan Barrios

GEORGE TEMPERLEY
GRUPO HORUS
GRUPO HORUS S.A.

Conclusión

- Análisis de Seguridad y Capacidad de Infraestructura Física de TIC: En función del aumento de uso de la infraestructura TIC del MEC en el predio de la sede, se sugiere un análisis de una solución híbrida (nube) de la infraestructura TIC.
- Preparación y ejecución de campañas internas de concientización de ciberseguridad y buenas prácticas.
- **Actualización Constante:** Asegurarse de contar con la última versión de los aplicativos utilizados en los servidores o que las versiones si bien no sean las últimas, estas no tengan problemas de seguridad conocidos.
- **Capacitación en manejo de Seguridad de la Información**: Se requiere de suficiente personal capacitado y exclusivo para la correcta realización de las tareas, así como el acompañamiento local posterior a dicha formación.
- **Realización de un Gap Análisis** de forma periódica para contar con un diagnóstico más preciso de la realidad de la institución y tener un marco base sobre el cual emitir recomendaciones de mejora.
- **Mínimo Punto de Exposición (MPE).** Minimizar la superficie de ataque exponiendo solo los puertos que sean necesarios.
- **Actualizar la documentación** existente o elaborarla en caso de no existir, para que todos los procesos y procedimientos estén debidamente soportados y se cumplan tales disposiciones.

GEORGE TEMPERLEY

GRUPO HORUS
GRUPO HORUS S.A.