PLAN LISTA DE SEGURIDAD INFORMÁTICA SERVICIOS TIC

MINISTERIO DE EDUACIÓN NACIONAL

UNIÓN TEMPORAL GESTIÓN INTEGRAL MEN

Carvajal TECNOLOGÍA Y SERVICIOS

coinsa

Enero 2021

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.

TABLA DE CONTENIDO

INDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

1. INTRODUCCIÓN

El Ministerio de Educación Nacional, comprometido con el uso eficiente de las Tecnologías de Información y Comunicaciones (TIC), en su plan de gestión estratégico de TI, contempla lo referente a la gestión y administración de los componentes de seguridad informática. Este plan permite a la entidad contar con un registro detallado de intervalos de tiempo, actividades que se ejecutarán y los recursos que están involucrados en la ejecución del mismo.

Por medio del presente plan de trabajo, se busca validar deficiencias en la infraestructura y aplicaciones de la entidad con el fin de subsanarlas y de esta manera proteger al Ministerio de Educación Nacional de Colombia de cualquier ataque informático que pueda generarse debido a las vulnerabilidades existentes que se identifiquen durante el presente contrato.

2. OBJETIVO

2.1 OBJETIVO GENERAL

Definir el Plan de Seguridad Informática que se aplicará para el Contrato 1989604 celebrado entre el Ministerio de Educación Nacional y Unión Temporal Gestión Integral, con el fin de minimizar el impacto de eventos que puedan afectar la seguridad de la información de los sistemas y plataformas del Ministerio y de esta manera propender por la continuidad en la prestación del servicio, cumpliendo con los ANS definidos, identificando además oportunidades de mejora en la solución con la que cuenta la entidad.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar actividades de monitoreo, evaluación y contención de amenazas de seguridad que puedan afectar la confidencialidad integridad y disponibilidad de los servicios y plataformas tecnológicas del ministerio.

- Adoptar mejoras técnicas y de gestión para el mejoramiento del nivel de madurez en seguridad de la información mediante el uso de herramientas y técnicas, estándares y mejores prácticas.

- Identificar los procesos críticos del ministerio y las soluciones/servicios tecnológicos que los soportan para realizar el análisis y evaluación de riesgos para adoptar estrategias que maximicen su continuidad.

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

3. ALCANCE

Este plan de Seguridad Informática aplica para los servicios de Seguridad Administrada y Seguridad Informática del Contrato 1989604 celebrado entre el Ministerio de Educación Nacional y Unión Temporal Gestión Integral.

La mitigación de vulnerabilidades estará sujeta a la causa raíz de esta, ya que, el operador no tiene control sobre el código de los sistemas de información.

4. PLAN DE SEGURIDAD INFORMÁTICA

4.1 ENTREGABLES CONTRACTUALES

Durante la vigencia del contrato, se realizará la generación de los siguientes entregables documentales a nivel de seguridad:

- Informe mensual que deberá ser entregado en los primeros 5 días del mes.
- Informe trimestral de vulnerabilidades.
- Metodología - Análisis y Mitigación de Vulnerabilidades (una única vez).
- Informe con resultados de las pruebas de penetración que se realicen.
- Informe trimestral con la validación de bugs indicados por los fabricantes que puedan impactar el correcto funcionamiento de los dispositivos de seguridad perimetral y por ende el servicio TIC del Ministerio de Educación Nacional.
- Modelo de seguridad de la información, incluyendo Business Impact Analysis (BIA) y un Risk Assessment (RA).

4.2 GESTIÓN OPERATIVA

A continuación, se relacionan actividades que se llevarán a cabo durante la vigencia del contrato entre el Ministerio de Educación Nacional y UT, las cuales serán bajo demanda de la operación:

Nombre de tarea	Comienzo previsto	Fin previsto	Nombres de los recursos
Escaneo y análisis bajo de demanda de Vulnerabilidades en la infraestructura tecnológica objeto de este contrato y a los desarrollos realizados por la fábrica de software o terceros contratados por la OTSI	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Identificar, diagnosticar y gestionar los problemas e incidentes de seguridad en	16/12/2020	31/07/2022	Especialistas Seguridad Informática

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

la infraestructura tecnológica objeto de este contrato			
Realizar recomendaciones con miras de optimizar y mejorar el rendimiento de los equipos de seguridad ubicados en el DC-Externo y DC-CAN	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Análisis de impacto en seguridad sobre los RFC propuestos	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Generación y actualización de Requerimientos de Cambios para activación o desactivación de firmas y/o políticas en los dispositivos de seguridad	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Actualización del inventario de activos gestionados, licenciamiento, soporte y diagramas de arquitectura	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Backup de la configuración de todos los dispositivos de seguridad administrados	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Atención de solicitudes a través de la plataforma definida para el contrato	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Realizar la Operación de toda la Infraestructura de seguridad del Ministerio, de los ambientes de prueba, desarrollo, certificación y producción.	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Presentar recomendaciones y planes de trabajo para optimizar el uso de los servicios y alertas tempranas sobre tendencias que justifican acciones por parte del Ministerio con respecto a los dispositivos de seguridad.	16/12/2020	31/07/2022	Especialistas Seguridad Informática
Realizar seguimiento a la custodia de cintas	16/12/2020	15/07/2022	Líder de gestión técnica y seguridad
Análisis de eventos de seguridad	16/12/2020	15/07/2022	SOC

Tabla 1. Actividades Operativas y recursos asignados

4.3 EJECUCIÓN DE PROTOCOLO DE ANÁLISIS DE VULNERABILIDADES

Con el objetivo de Identificar, diagnosticar y gestionar las vulnerabilidades presentes en la infraestructura tecnológica del Ministerio de Educación Nacional de Colombia, se define realizar la ejecución del protocolo de análisis de vulnerabilidades trimestralmente, teniendo en cuenta las siguientes actividades:

Nombre de tarea	Nombres de los recursos

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

Definición de objetivos por parte del Ministerio de Educación Nacional	MEN
Ejecución escaneo de vulnerabilidades de acuerdo con el ítem anterior	Especialista Seguridad
Organización y análisis de los resultados obtenidos del escaneo realizado	Especialista Seguridad
Generación del plan de mitigación de vulnerabilidades responsabilidad operador.	Especialistas APP, BD, Infraestructura y/o Seguridad
Generación de informe de resultados obtenidos	Especialista Seguridad
Seguimiento PDT de mitigación de vulnerabilidades	Especialista Seguridad

Tabla 2. Protocolo Análisis de Vulnerabilidades

El detalle de la metodología usada para el ejercicio de escaneo de vulnerabilidades, favor remitirse al documento ubicado en la ruta: https://mineducaciongovco.sharepoint.com/:b:/r/sites/Proyecto_UTGI_MEN/Documentos%20compartidos/PROYECTO_UTGI_MEN/2.%20Planes%20-%20Listas%20de%20Chequeo/2.1%20Planes/2.1.1%20Planes%20Unicos/7.%20Plan%20de%20Seguridad%20Inform%C3%A1tica/Metodolog%C3%ADa%20-%20An%C3%A1lisis%20y%20Mitigaci%C3%B3n%20de%20Vulnerabilidades%20(1).pdf?csf=1&web=1&e=SKtZub

Las fechas indicadas para los trimestres corresponden a las siguientes:

Plan de escaneo de vulnerabilidades	Duración	inicio	Fin
Ejecución del protocolo Análisis de Vulnerabilidades - Trimestre 1	107 días	jue 7/01/21	mar 15/06/21
Ejecución del protocolo Análisis de Vulnerabilidades - Trimestre 2	123 días	mar 16/03/21	mié 15/09/21
Ejecución del protocolo Análisis de Vulnerabilidades - Trimestre 3	124 días	mié 16/06/21	mié 15/12/21
Ejecución del protocolo Análisis de Vulnerabilidades - Trimestre 4	124 días	jue 16/09/21	mar 15/03/22
Ejecución del protocolo Análisis de Vulnerabilidades - Trimestre 5	124 días	jue 16/12/21	mar 14/06/22
Ejecución del protocolo Análisis de Vulnerabilidades - Trimestre 6	90 días	mié 16/03/22	Vie 29/07/2022

Tabla 3. Plan de ejecución escaneo de Vulnerabilidades

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

4.4 PRUEBAS DE PENETRACIÓN

Al momento de realizar este plan de seguridad informática, el Ministerio de Educación Nacional tiene en su repositorio el inventario de aplicaciones con versión número 75, en el cual relaciona un total de 148 sistemas, de los cuales, 67 están catalogados como misionales, esta información se encuentra en la siguiente ruta:

https://mineducaciongovco.sharepoint.com/:f:/r/sites/Proyecto_UTGI_MEN/Documentos%20compartidos/PROYECTO_UTGI_MEN/3.%20Operaci%C3%B3n%20Servicios%20TI/3.3%20Gesti%C3%B3n%20de%20Aplicaciones/3.3.1%20L%C3%ADnea%20Base%20de%20Aplicaciones?csf=1&web=1&e=2cnxB5

Para llevar a cabo las pruebas de penetración en el Ministerio de Educación Nacional, se debe acordar como primera medida los objetivos y dependiendo el sistema de información, la entidad deberá indicar si las pruebas son realizadas sobre el ambiente productivo (sujetas a aprobación del CAB con su respectiva orden de cambio y en horario no laboral) o si, por el contrario, es necesario clonar.

En caso de clonación, se podrán presentar atrasos en los ejercicios de penetración porque será necesario postular una orden de cambio para realizar dicha actividad, donde se incluyen ítems como: realizar cambio de direccionamiento IP, ajustes sobre la configuración y pruebas funcionales (tarea que no está a cargo de la UT) para garantizar que la clonación fue exitosa. Indicado lo anterior, las actividades que se desarrollarán son las siguientes:

Nombre de tarea	Nombres de los recursos
Definición de objetivos por parte del Ministerio de Educación Nacional	MEN
Dependiendo del objetivo del Ministerio se debe realizar un proceso de clonación	Especialista Infraestructura, Aplicaciones, BD y Seguridad
Ejecución pruebas de penetración entre las cuales se realiza los siguientes pasos: Fase de recolección de información Fase de Búsqueda de vulnerabilidades Fase de Explotación de vulnerabilidades Fase Post-explotación	Especialista Seguridad
Generación de informe de resultados obtenidos	Especialista Seguridad
Generación del plan de mitigación de vulnerabilidades	Especialista Infraestructura, Aplicaciones, BD y Seguridad
Seguimiento PDT de mitigación de vulnerabilidades	Especialista Seguridad

Tabla 4. Protocolo pruebas de penetración.

4.5 REVISIÓN TRIMESTRAL ACTUALIZACIÓN TECNOLÓGICA

Dentro de los objetivos del plan de seguridad, se realizará de manera trimestral un proceso de validación de actualización tecnológica de las diferentes plataformas de seguridad informática con las que cuente el

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

Ministerio de Educación Nacional, con el fin de determinar si es necesario realizar algún procedimiento para evitar falencias en los controles implementados para mantener la confidencialidad, disponibilidad e integridad de la información en los diferentes sistemas de información del Ministerio. Para poder llevar a cabo dicha tarea, se contemplan los siguientes pasos:

- Revisión de la documentación de los fabricantes en sus portales: Los fabricantes de tecnología acostumbran a publicar hallazgos sobre los productos que ofrecen y que pueden impactar la infraestructura de sus clientes. Por tal razón, la UT Gestión Integral MEN, revisará de manera trimestral los diferentes portales de las fábricas con las cuales el Ministerio tenga algún producto de seguridad para validar dichas publicaciones.
- Evaluación de la revisión realizada: Se determinará si los bug o fallas indicadas por las fábricas afectan o no la infraestructura del Ministerio, lo cual, se realizará validando el modelo, la versión y las funcionalidades activas del producto que se encuentra operando en la red de la entidad.
- Generar documento con las validaciones realizadas: Posterior a los pasos mencionados anteriormente, se desarrollará un documento que permita dar a conocer las publicaciones y/o recomendaciones de los fabricantes con respecto a los productos con los que cuenta la entidad y los pasos que se deben seguir para remediar cualquier inconveniente que pueda impactar la prestación de los servicios ofrecidos por el Ministerio.
- Generar RFC cuando aplique una actualización, parchado y/o modificación de la configuración: Del análisis realizado se podrán generar las correspondientes ordenes de cambio para llevar a cabo la mitigación de los riesgos identificados en el proceso de revisión tecnológica, que serán objeto de viabilidad y aprobación por parte de la entidad.

4.6 PRESTACIÓN DE UN SERVICIO DE SIEM

La Unión Temporal de Gestión Integral prestará el servicio de SIEM con un dispositivo FortiSIEM 3500F con el fin de:

- Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información y comunicaciones de la entidad.
- Analizar los ataques o posibles amenazas.
- Mejorar la capacidad de respuesta ante un eventual ataque.
- Retención de logs para revisión ante un eventual incidente de seguridad.

Para la implementación del servicio de SIEM, se debe definir la arquitectura que se usará y esto dependerá de la ubicación del dispositivo. La solución propuesta es la siguiente:

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

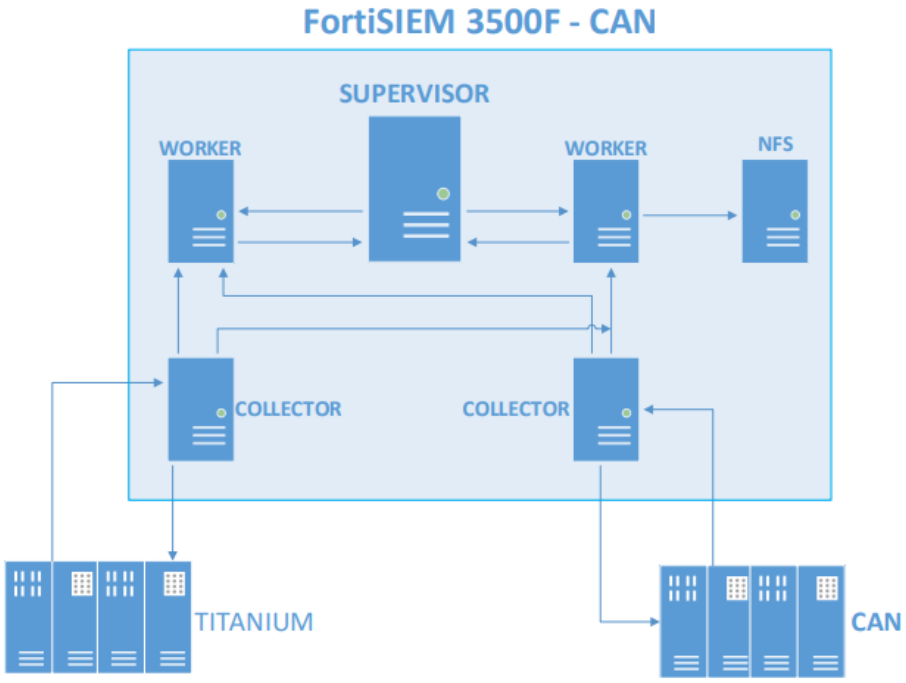

Ilustración 1. SIEM en la infraestructura del Ministerio de Educación Nacional.

La información que se puede recolectar de los diferentes dispositivos que componen la infraestructura del ministerio depende de la naturaleza sobre la cual esté soportado el servicio. Por ejemplo, los parámetros que se pueden monitorear con el dispositivo FortiSIEM a nivel de servidores son los siguientes:

- **DISPOSITIVOS MICROSOFT WINDOWS SERVER**

Protocolo	Información	Métricas	Uso
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, **installed software**, running processes, open TCP/UDP ports)	Uptime, Overall CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, **Installed Software change**, Running process CPU/memory utilization, Running process start/stop, **TCP/UDP port up/down**,	Performance Monitoring
SNMP	Vendor specific server hardware (hardware model, hardware serial number, fans, power supply, disk, raid battery). Currently supported vendors include HP and Dell	Hardware module status - fan, power supply, thermal status, battery, disk, memory . Currently supported vendors include HP and Dell	
WMI	Win32_ComputerSystem: Host name, OS Win32_WindowsProductActivation: OS Serial Number Win32_OperatingSystem: Memory, Uptime Win32_BIOS: Bios Win32_Processor: CPU Win32_LogicalDisk: Disk info Win32_NetworkAdapterConfiguration: network interface Win32_Service: Services	Win32_OperatingSystem: Uptime Win32_PerfRawData_PerfOS_Processor: Detailed CPU utilization Win32_PerfRawData_PerfOS_Memory: Memory utilization, paging/swapping metrics Win32_LogicalDisk: Disk space utilization Win32_PerfRawData_PerfOS_PagingFile: Paging file utilization	Performance Monitoring

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

	Win32_Process: Running processes Win32_QuickFixEngineering: Installed Patches	Win32_PerfRawData_PerfDisk_LogicalDisk: Disk I/O metrics Win32_PerfRawData_Tcpip_NetworkInterface: Network Interface utilization Win32_Service: Running process uptime, start/stop status Win32_Process, Win32_PerfRawData_PerfProc_Process: Process CPU/memory/I/O utilization	
WMI		Security, Application and System Event Logs including logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
Snare agent		Security, Application and System Event Logs including logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
Correlog agent		Security, Application and System Event Logs ncluding logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
FortiSIEM Agent		Security, Application and System Event Logs, DNS, DHCP, IIS, DFS logs, Custom log files, File Integrity Monitoring, Registry Change Monitoring, Installed Software Change Monitoring, WMI and Powershell output monitoring	Security and Compliance

Tabla 5. Parámetros de lectura FortiSIEM sobre servidores Windows

- **DISPOSITIVOS LINUX**

Protocolo	Información	Metricas	Uso
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Swap space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	OS type, Hardware **(cpu details, memory**)	**Memory paging rate, Disk I/O utilization**	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance
Syslog (via FortiSIEM LinuxFileMon agent)		File or directory change: User, Type of change, directory or file name	Security Monitoring and Compliance

Tabla 6. Parámetros de lectura FortiSIEM sobre servidores Linux

Debido a que, el Ministerio de Educación en el anexo técnico “Anexo_Tecnico_OperacionGlobal_ServiciosTIC V2” menciona que la función de monitoreo de recursos se hará con la herramienta de CA, el objetivo del SIEM es centralizar logs para temas de seguridad. Para ello es necesario sobre los servidores Windows, instalar un agente FortiSIEM. Para el caso de los servidores Linux, se validará si es suficiente con el “protocolo” syslog. Esto

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

dependerá el tipo de aplicación que se encuentra corriendo sobre los sistemas. El plan de implementación se define de la siguiente manera:

- Implementación del equipo FortiSIEM de acuerdo con la arquitectura mencionada.
- Configuración de los dispositivos Fortinet para envió de logs al FortiSIEM
- Instalación de agente FortiSIEM sobre los servidores Windows correspondientes a los servicios prestados por el área de Gestión Técnica y seguridad del Ministerio, iniciando con el ambiente de certificación. Posterior a ello se realizará sobre el ambiente de producción. El inventario de los servidores se encuentra en la siguiente ruta: https://mineducaciongovco.sharepoint.com/:x:/r/sites/Proyecto_UTGI_MEN/Documentos%20compartidos/PROYECTO_UTGI_MEN/2.%20Planes%20-%20Listas%20de%20Chequeo/2.2%20Listas%20de%20Chequeo/2.2.1%20Gesti%C3%B3n%20T%C3%A9cnica/2.2.1.1.%20Inventario%20actualizado%20de%20activos%20a%20ser%20gestionados%20%E2%80%93%20CMDB/2.2.1.1.2%20Enero/servidores%20infraestructura%20y%20seguridad.xlsx?d=w7fd8bf5f83634615a8b30b384a3ad776&csf=1&web=1&e=GHTab4
- Configuración de servidores Linux por medio del protocolo syslog correspondientes a los servicios prestados por el área de Gestión Técnica y seguridad del Ministerio, iniciando con el ambiente de certificación posterior a ello sobre el ambiente de producción. El inventario de los servidores se encuentra en la siguiente ruta: https://mineducaciongovco.sharepoint.com/:x:/r/sites/Proyecto_UTGI_MEN/Documentos%20compartidos/PROYECTO_UTGI_MEN/2.%20Planes%20-%20Listas%20de%20Chequeo/2.2%20Listas%20de%20Chequeo/2.2.1%20Gesti%C3%B3n%20T%C3%A9cnica/2.2.1.1.%20Inventario%20actualizado%20de%20activos%20a%20ser%20gestionados%20%E2%80%93%20CMDB/2.2.1.1.2%20Enero/servidores%20infraestructura%20y%20seguridad.xlsx?d=w7fd8bf5f83634615a8b30b384a3ad776&csf=1&web=1&e=GHTab4
- Se realizará un reporte de los sistemas que están enviando logs para validar consumo de recursos y eventos por segundo.
- Instalación de agente FortiSIEM sobre los servidores Windows en ambiente de certificación para los sistemas de información indicados en la versión 75 del archivo de aplicaciones, el cual, se encuentra en la siguiente ruta: https://mineducaciongovco.sharepoint.com/:f:/r/sites/Proyecto_UTGI_MEN/Documentos%20compartidos/PROYECTO_UTGI_MEN/3.%20Operaci%C3%B3n%20Servicios%20TI/3.3%20Gesti%C3%B3n%20de%20Aplicaciones/3.3.1%20L%C3%ADnea%20Base%20de%20Aplicaciones?csf=1&web=1&e=2cnxB5
- Configuración sobre los servidores Linux en ambiente de certificación para los sistemas de información indicados en la versión 75 del archivo de aplicaciones, el cual, se encuentra en la siguiente ruta: https://mineducaciongovco.sharepoint.com/:f:/r/sites/Proyecto_UTGI_MEN/Documentos%20compartidos/PROYECTO_UTGI_MEN/3.%20Operaci%C3%B3n%20Servicios%20TI/3.3%20Gesti%C3%B3n%20de%20Aplicaciones/3.3.1%20L%C3%ADnea%20Base%20de%20Aplicaciones?csf=1&web=1&e=2cnxB5
- Se realizará un reporte de los sistemas que están enviando logs para validar consumo de recursos y eventos por segundo.
- Instalación de agente FortiSIEM sobre los servidores Windows en ambiente de producción para los sistemas de información indicados en la versión 75 del archivo de aplicaciones que se encuentra en la ruta indicada del punto anterior.

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

- Configuración sobre los servidores Linux en ambiente de producción para los sistemas de información indicados en la versión 75 del archivo de aplicaciones que se encuentra en la ruta indicada del punto anterior.

4.7 PRESTACIÓN DEL SERVICIO SOC

La Unión Temporal Gestión Integral ofrece el servicio de Security Operation Center - SOC con los objetivos de:

- Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de Información y comunicaciones de la entidad
- Analizar los ataques o posibles amenazas
- Responder de manera eficaz y oportuna ante cualquier ataque.

Para ello, el SOC realizará un monitoreo continuo y proactivo de la seguridad, clasificando las alertas detectadas y ajustando las defensas correspondientes en base a dicha detección. Para cumplir con los objetivos del SOC se realizan además las siguientes tareas:

- Gestión de vulnerabilidades: El SOC apoyará el proceso de gestión de vulnerabilidades indicado en el numeral 4.3 de este documento, con el fin de llevar un proceso continuo de la detección y mitigación de vulnerabilidades.
- Pruebas de Hacking Ético: Con el fin de identificar deficiencias en configuraciones que representan vulnerabilidades y que pueden ser aprovechadas por un atacante, se realizaran pruebas de penetración no solo con el fin de realizar la explotación sino para generar las recomendaciones pertinentes con la finalidad de subsanar todos los errores o malas prácticas que puedan tener los sistemas de información o hardware del Ministerio, el desglose de estas actividades se menciona en el numeral 4.4 de este documento.
- Análisis de ataques: Apoyados en la implementación del FortiSIEM, se realizará análisis de los eventos de seguridad que se puedan presentar en la infraestructura del Ministerio, ya que, se llevará a cabo la correlación de alertas, proceso que se llevará a cabo diariamente después de implementado el dispositivo FortiSIEM en su primera fase (incluir todos los equipos Fortinet)y se convertirá en una tarea operativa (numeral 4.2 de este documento).

4.8 BUSINESS IMPACT ANALYSIS (BIA) Y RISK ASSESMENT (RA)

4.8.1 BUSINESS IMPACT ANALYSIS

Debido a que el desarrollo del análisis de impacto para el negocio y la evaluación de riesgos se realizará para el Ministerio de Educación Nacional, es necesario seguir las directrices indicadas por el Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC, por lo cual, para el desarrollo de este ejercicio se deben seguir los siguientes aspectos:

- **IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DE GESTIÓN DE SERVICIOS TIC**

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad. Este punto tiene como resultado generar un listado de roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del BIA.

- **EVALUACIÓN DE IMPACTOS OPERACIONALES**

Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad. El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles:

- Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
- Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.
- Nivel C: La operación no es una parte integral del negocio.

- **IDENTIFICACIÓN DE PROCESOS CRÍTICOS**

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones.

- **ESTABLECIMIENTO DE TIEMPOS DE RECUPERACIÓN**

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación de describen a continuación:

- **MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable:** Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse
- **RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo:** Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.
- **RPO (Recovery Point Objective) o Punto de Recuperación Objetivo:** Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.
- **WRT (Work Recovery Time):** Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

Una vez identificados los procesos críticos del negocio, función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio).

- **IDENTIFICACIÓN DE RECURSOS**

Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de las Entidades.

- **DISPOSICIÓN DE LOS RTO/RPO (RECOVERY TIME OBJECTIVE / RECOVERY POINT OBJECTIVE)**

Se debe tener en cuenta el Tiempo de Recuperación Objetivo (RTO), asociado con la restauración de los recursos que han sido alterados de las Tecnologías de la Información; comprende el tiempo disponible para recuperar recursos alterados. Igualmente, con el Punto de Recuperación Objetivo (RPO)se debe determinar por cada uno de los procesos críticos (servicios), el rango de tolerancia que una Entidad puede tener sobre la pérdida de información y el evento de desastre.

- **IDENTIFICACIÓN DE PROCESOS ALTERNOS**

La identificación de procesos alternos hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno que las Entidades tengan métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción; por lo tanto, para cada proceso crítico que se establezca (en los servicios), se debe poseer un procedimiento manual de continuidad del servicio.

- **GENERACIÓN DE INFORME DE IMPACTO DEL NEGOCIO**

Generar un informe de impacto de negocio que corresponde a la guía para el BIA con los siguientes puntos:

- Listado de procesos críticos
- Listado de prioridades de sistemas y aplicaciones
- Listado de tiempos MTD, RTO y RPO
- Listado de procedimientos alternos

4.8.2 RISK ASSESSMENT

Para la evaluación del riesgo se deben contemplar los siguientes aspectos:

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

- Identificación de activos
- Identificación de las amenazas.
- Identificación de controles existentes
- Identificación de vulnerabilidades
- Definición de métodos para la valoración de vulnerabilidades técnicas
- Identificación de las consecuencias

El producto final, será una matriz que relacione los diferentes apartes mencionados anteriormente.

4.9 ARQUITECTURA DE SEGURIDAD Y EL MODELO DE SEGURIDAD DE LA INFORMACIÓN

Para definir el modelo de seguridad de la información, se pretende preservar los siguientes componentes:

- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].
- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].

Se deben llevar a cabo unas etapas previas, y entendiendo que este modelo será implementado en una entidad del gobierno, se toma como base, los lineamientos del modelo de privacidad y seguridad de la información – MPSI, indicados por MINTIC en su página WEB. Dentro de los pasos a seguir se tiene:

- Validar el estado actual del modelo de seguridad del Ministerio de Educación Nacional
- Identificar el nivel de Madurez

Después de realizadas las actividades anteriores se puede proseguir con las etapas de implementación de un modelo de seguridad de la información, es importante contar con el apoyo y compromiso de la dirección para poder continuar con las siguientes actividades:

PLANIFICACIÓN

En la planificación se definen todos los componentes necesarios para la implementación del modelo de seguridad de la información:

- Entender el contexto del Ministerio de Educación Nacional, las necesidades que tiene para cumplir la visión y misión; de esta manera poder definir los objetivos y el alcance que tendrá el modelo de seguridad de la información.
- Es importante que, dentro del modelo, quede explicito el compromiso por parte de los directivos.

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

- Las políticas mínimas para implementar deben ser: Gestión de activos, control de acceso, no repudio, privacidad de la información, integridad, disponibilidad del servicio e información, registro y auditoría.
- Procesos y procedimientos, debidamente definidos.
- Asignación del recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información
- Integración del modelo de seguridad de la información con los demás sistemas de gestión.
- Descripción de los flujos de los activos de tipo información que contengan datos personales.
- Acciones para tratar riesgos y oportunidades de seguridad de la información.
- Identificación y valoración de riesgos de (Metodología, Reportes).
- Tratamiento de riesgos.
- Definir un plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional,

Basándonos en el modelo de seguridad de la información propuesto por MINTIC, se continuará con la documentación de la definición de la arquitectura de seguridad informática y demás componentes que puedan dar cumplimiento a lo establecido en el anexo técnico "Anexo_Tecnico_Operacionglobal_ServiciosTIC V2", y como resultado se tendrán los siguientes entregables:

- Definición de la guía de arquitectura de seguridad
- Plan de recuperación tecnológica (DRT)
- Definición de la infraestructura de seguridad
- Plan de recuperación de desastres (DRP)
- Guía de capacidades tecnológicas aseguradas
- Guía de tratamiento de la información, los datos, los sistemas de información, la infraestructura tecnológica y física de la organización.
- Guía para el aseguramiento de la confidencialidad, integridad, disponibilidad, autenticación, autorización, no repudio, auditoría y privacidad.

5. REFERENCIAS

- http://icutuder.com/wp-content/uploads/2018/01/Modelo-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n.pdf
- https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA

CONTROL DE VERSIONES DEL DOCUMENTO				
Versión	**Fecha**	**Descripción del Cambio**	**Elaborado por**	**Aprobado por**
1.0	28-12-2020	Primera versión del documento	Líder de Gestión Técnica y Seguridad	Gerencia de Proyectos
2.0	25-01-2020	Atención al comunicado INT-MEN-COM-0121-070 - Fe de erratas / Acción correctiva	Líder de Gestión Técnica y Seguridad	Gerencia de Proyectos
3.0	04-02--2020	Atención al comunicado INT-UT-COM-0221-088 - Devolución Plan de seguridad	Líder de Gestión Técnica y Seguridad	Gerencia de Proyectos

La propiedad intelectual de este documento es de Carvajal Tecnología y Servicios
Se prohíbe su reproducción total o parcial sin autorización.
COPIA NO CONTROLADA