INFORME TECNICO SOBRE NECESIDAD DE ADQUISICION CENTRO DE MONITOREO Y GESTION DE INCIDENTES DE CIBERSEGURIDAD CON TECNOLOGIA

GOBIERNO DE LA
REPÚBLICA DOMINICANA
EDUCACIÓN

DGTIC
DIRECCIÓN GENERAL DE TECNOLOGÍA
DE INFORMACIÓN Y COMUNICACIÓN

NOMBRE DEL DOCUMENTO		
Código del Documento:	**DGTIC-OP-INF-DOTIC-002**	GOBIERNO DE LA REPÚBLICA DOMINICANA EDUCACIÓN
Versión del Documento:	**000**	
Fecha de Creación y/o Revisión:	**21 de febrero 2022**	
Nivel de Confidencialidad:	**INTERNO**	

Se emite el presente documento **NECESIDAD DE ADQUISICION CENTRO DE MONITOREO Y GESTION DE INCIDENTES DE CIBERSEGURIDAD CON TECNOLOGIA FORTINET**, suministrado por la Dirección de Seguridad y Monitoreo de Información, con la finalidad de informar respecto a las necesidades actuales de adquisición.

VALIDACIÓN Y AUTORIZACIÓN DE ESTE DOCUMENTO

Preparado Por:		*Fecha:*	21/02/2022
Nombre:	Christopher Bonora / Anyelo García		
Firma:			
Cargo:	Director y Encargado		
Dependencia:	Dirección de Seguridad y Monitoreo de Información		

Colaboración:		*Fecha:*	
Nombre:			
Firma:			
Cargo:			
Dependencia:			

Aprobación:		*Fecha:*	14/02/2022
Nombre:	Dr. Jimmy Rosario Bernard		
Firma:			
Cargo:	Director General		
Dependencia:	Dirección General de Tecnología de la Información y la Comunicación		

HISTÓRICO DE REVISIONES

REVISIONES DEL DOCUMENTO			
Versiones del Documento	***Descripción***	***Fecha***	***Originador***
V1.0	Creación del documento	21/02/2022	Dirección de Seguridad y Monitoreo de Información

NOMBRE DEL DOCUMENTO		
Código del Documento:	**DGTIC-OP-INF-DOTIC-002**	GOBIERNO DE LA REPÚBLICA DOMINICANA EDUCACIÓN
Versión del Documento:	**000**	
Fecha de Creación y/o Revisión:	**21 de febrero 2022**	
Nivel de Confidencialidad:	**INTERNO**	

REVISIONES DEL DOCUMENTO			
Versiones del Documento	***Descripción***	***Fecha***	***Originador***

Sello y firma del área responsable de tramitar este documento:

_____

Firma

☐ ***Copia Controlada. No. Copia:*** _____

☐ ***Copia No Controlada***

TABLA DE CONTENIDO

1. ANTECEDENTES

La dirección general de tecnología de la información y comunicaciones es la entidad responsable de la implementación y gestión de la infraestructura tecnológica y las plataformas de servicios del Ministerio de Educación. Su alcance corresponde todo el territorio nacional considerando todas las instancias administrativas: Sede Minerd (1), Anexos 0 dependencias directamente conectadas (7), Regionales (18), Distritos (123) y otras dependencias descentralizadas a las cuales se les brinda soporte.

La plataforma tecnológica del Minerd se consolida en un centro de datos ubicado en la sede de la institución desde el cual se publican los servicios hacia internet además de los usuarios internos y a través de conectividad VPN con equipos hacia las oficinas remotas. Este tipo de conectividad y tecnología fue implementada en el periodo 2015-2016 con equipos específicamente FORTINET modelos 1500D, 60CX-ADSL entre otros brindando un nivel considerable de seguridad para ese momento.

Durante el periodo 2017-2018 se creó la dirección de seguridad y monitoreo de información desde su creación ha venido implementando más soluciones de seguridad para proteger la información que se genera y procesa a través de computadoras, servidores, redes y sistemas electrónicos contra ataques cibernéticos.

Cabe destacar la responsabilidad de la plataforma tecnológica del Minerd en brindar servicios de comunicación, de seguridad e infraestructura además de aplicaciones dirigidas a usuarios internos de la institución, así como a la comunidad educativa y la ciudadanía en general.

2. SITUACION ACTUAL

Hoy día el escenario de la tecnología es muy sofisticado, pues un ecosistema tecnológico típico podría implicar una diversidad de fabricantes y suplidores, así como múltiples arquitecturas de TI, lo cual complica poder lograr una visión íntegra de posibles errores de arquitectura, servicios, continuidad de negocios y problemas de ciber-ataques en todos los niveles.

El 85% de la tecnología de seguridad y comunicación del Minerd está sustentada en soluciones del Fabricante FORTINET en modelos antes mencionados y entre otros. Aunque los mismos están brindando un nivel de seguridad moderado aun así se necesita mejoras y principalmente un alto nivel de visibilidad centraliza y análisis del todo el tráfico de la información.

Las alertas generadas por estos sistemas pueden ser muy abrumadoras y que, además, en su mayoría, pueden resultar en falsas alarmas resultando que las labores concernientes al proceso de gestión de eventos e incidentes de seguridad informática, se ejecuta un proceso un poco desactualizado y carente de una mejor estructura que permita al ministerio definir de manera clara y precisa los procesos, roles y responsabilidades necesarios para una buena gestión de eventos/incidentes de seguridad.

Para un proceso eficiente se combinan herramientas y experiencia con un entendimiento del contexto que los rodea para determinar la exactitud y severidad de cada alerta. Esta complicada tarea requiere ser complementada rápida y efectiva. Desafortunadamente, a medida que las redes de Minerd crecen en tamaño y complejidad, se vuelve muy difícil para nuestros analistas mantener la delantera sobre los atacantes.

3. RECOMENDACION

La implementación de un Centro de Operaciones de Seguridad y SOC, por sus siglas en inglés con soluciones del fabricante FORTINET será una parte crítica de nuestra tecnología que tendrá el propósito de proveer servicios de detección y reacción a incidentes de seguridad **con mayor eficacia por el 99% de compactibilidad con sus mismos modelos de equipos que como antes mencionado un 85% de estos sustentan la seguridad del Minerd. Este SOC monitoreará y administrará todos los aspectos de seguridad de la información de Minerd en tiempo real,** desde una ubicación única y centralizada. Al mismo tiempo que el SOC tendrá estándares y mejores prácticas que podrán ayudar a Minerd a resolver las brechas entre enfoques teóricos, implementaciones y sistemas independientes con un conjunto de mejores prácticas a ser incluida en dicho esquema. También recomendamos que esta necesidad sea adquirida mediante un proceso de exclusividad dirigido a los proveedores que sean representantes o distribuidores autorizados oficialmente por el fabricante FORTINET.

Riesgos de no adquirir las soluciones:

- No se podría responder a los ataques detectados de forma eficiente a través del análisis de comportamiento de un sistema.
- Aunque en esta primera fase se necesitan de otras herramientas, si no se inicia con la misma no podríamos tener la capacidad de buscar, detectar y evitar ataques de forma proactiva, a partir de información otorgada por herramienta de inteligencia de amenazas y tendencias de explosión de vulnerabilidades.
- No se contaría con las herramientas necesarias, para incrementar la seguridad que ayuden al minerd de forma más eficiente a defenderse de ataques constantes que existen en las redes.
- Estar fuera de las mejores prácticas y tecnología de seguridad que en la actualidad se han desarrollado para mitigar las nuevas amenazas que cada día se mantienen en constante avance.

- No se podrá depurar y afinar reglas de correlación y alarmas efectivas de eventos log de seguridad, por la falta de una solución que recolecta de manera centralizada toda la información.