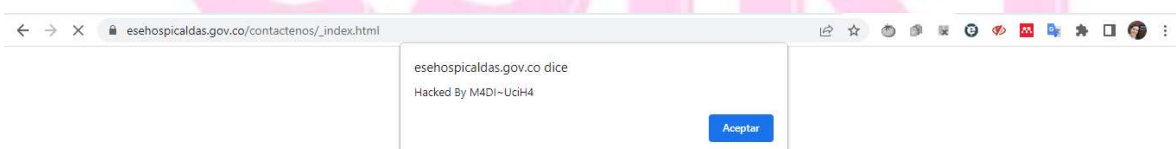


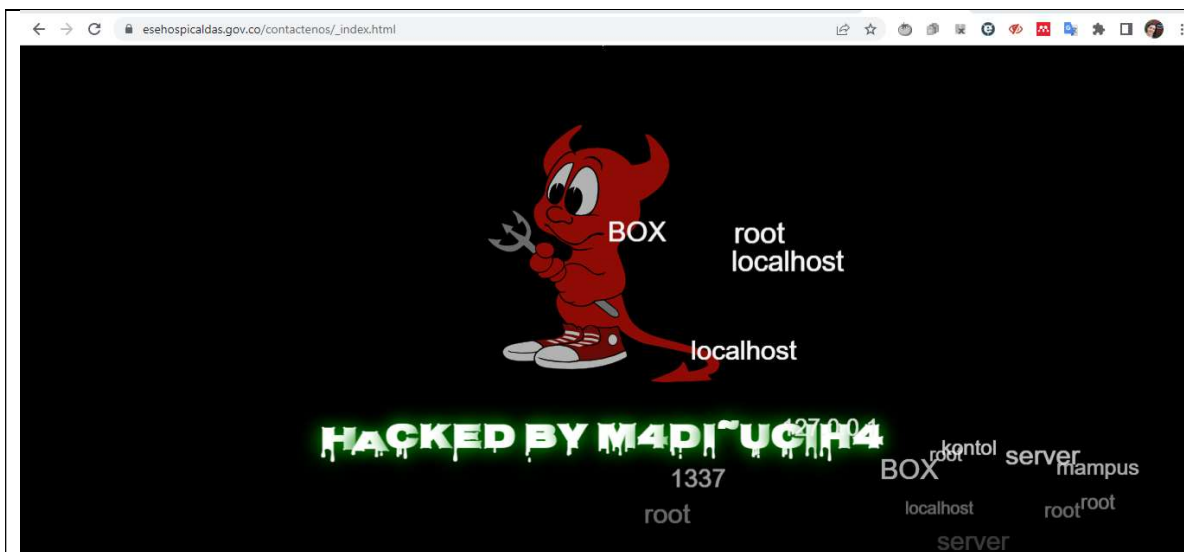


Reporte de Incidentes

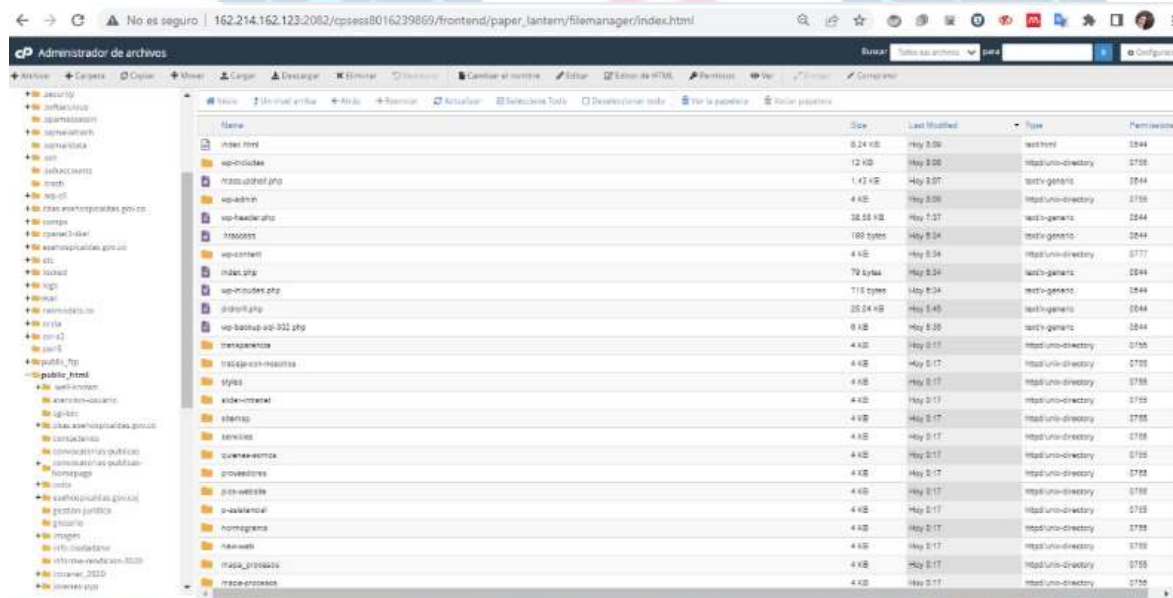
Fecha del Reporte: 29/07/2022 3:50 a. m.

Datos de Contacto de la Entidad		
Nombre de la Entidad: ESE HOSPITAL SAN VICENTE DE PAUL CALDAS ANTIOQUIA		
Dirección: Cra 48 #135sur - 41		Sede: Sede principal
Sector: Salud	Ciudad: Caldas	Departamento: Antioquia
Nombre de Quien Reporta: Diana Isabel Posada Villada		
Cargo: Directora Gobierno Digital, Tecnologías e información		Número Contacto: Fijo: Número Fijo. Ext Número de la extensión Celular: 3008947110
Correo Electrónico: lidersistemas@esehospicaldas.gov.co		Skype: Escriba su usuario de Skype

Incidente	
Fecha y Hora del descubrimiento: 29/07/2022 10:45 a. m.	Nombre de la Persona que Detectó el Incidente: Diana Isabel Posada Villada
Fecha y Hora de Detección: 29/07/2022 10:45 a. m.	Nombre del administrador del Activo Informático: Hostgator
Descripción Detallada: Quien: Diana Posada, realizo acceso a página web. Que: Se genera un mensaje emergente de Hackeo. Como: Ingresando al portal www.esehospicaldas.gov.co Cuando: el 29/07/2022 a las 10:45 am	
Método de Detección: Ingresando a la pagina web y generando mensaje emergente e imagen de pagina modificada:	
	



Se detecta archivos modificados desde el día 29/07/2022 a las 0:17 am. En toda la estructura



CSIRT

Acciones Realizadas:

Se ingresa al portal de cpanel e ingresa correctamente.

Se realiza cambio de contraseña de todos los usuarios.

Se visualiza todos los index.html modificados en todas las carpetas de la pagina web.

Se procede a modificar index de la página principal, inicialmente generando problemas de conexión y posteriormente con mensaje de pagina en mantenimiento.

Se genera reporte a hostgator, solicitando restablecimiento del sitio, con un respaldo que se encuentra en el cpanel del día 27/06/2022.

Acciones Pendientes:

En espera de respuesta por parte de hostgator y del restablecimiento del backup que se encontraba local. De lo contrario se cargaría uno que se tiene de forma local.

Clasificación del Incidente: Seleccione la clase y tipo de incidente.

Malware: RAT (Remote Acces Tools)

Disponibilidad: Sabotaje

Obtención de Información: Identificación de activos y vulnerabilidades (escaneo)

Intrusiones: Defacement (desfiguración)

Compromiso de Información: Modificación y borrado no autorizado de información

Fraude: Uso de recursos no autorizado

Contenido Abusivo: Elija un elemento.

Política de Seguridad: Acceso a servicios no autorizados

Otros:

Escriba la clasificación del incidente, si no se encuentra en las listas desplegadas

La respuesta al incidente fue efectiva:

SI NO

Duración del Incidente: **Días**

Horas

Minutos

Se Identifico el Responsable:

SI NO

Nombre: Escriba el nombre y apellidos de la persona responsable

Área: Escriba el nombre del área, al cual pertenece la persona responsable

Hardware y Software Afectado

Servicios Afectados: Misionales Estratégicos Financieros Tecnológico Soporte y Mejora

Servidor PC Portátil BD Portal WEB Aplicación Correo Equipo Activo Otros

TECNOLOGICO – PORTAL WEB

Descripción Detallada del Activo o Servicio Afectado:

Servidor web, alojado en hostgator.

Debido al Incidente:

Alguien no autorizado tuvo acceso a la información: SI NO

Se ha impedido a algún usuario el acceso a la información: SI NO

Se ha borrado, modificado y eliminado alguna información: <input checked="" type="radio"/> SI <input type="radio"/> NO	
Impacto del incidente: <input type="checkbox"/> Financiero <input type="checkbox"/> Reputacional <input type="checkbox"/> Operacional <input type="checkbox"/> Legal - OPERACIONAL	REPUTACIONAL
Causa Raíz: Escriba cual fue la causa raíz, por la cual se presentó el incidente.	
Realizo Plan de Mejoramiento: <input checked="" type="radio"/> SI <input type="radio"/> NO	
Acciones Planificadas para Solución Causa Raíz: Escriba las actividades de manera secuencial, que permitirán eliminar y/o controlar la causa raíz.	
Lecciones Aprendidas: Escriba las lecciones aprendidas generadas en las etapas antes, durante y después del incidente	
Después de realizar la contención y actividades de mitigación el incidente se encuentra: <input checked="" type="radio"/> Abierto <input type="radio"/> Cerrado	El incidente ya se había presentado: <input type="radio"/> SI <input checked="" type="radio"/> NO
Otros: Escriba cualquier otra información relacionada con el incidente, que no se encuentre contenida en este formato.	

Contáctanos

Si tienes alguna consulta técnica, comunicarse con CSIRT Gobierno a través de los siguientes canales:



Bogotá: 601 344 22 22

Línea Gratuita Nacional: 018000952525 Op. 2



csirtgob@mintic.gov.co