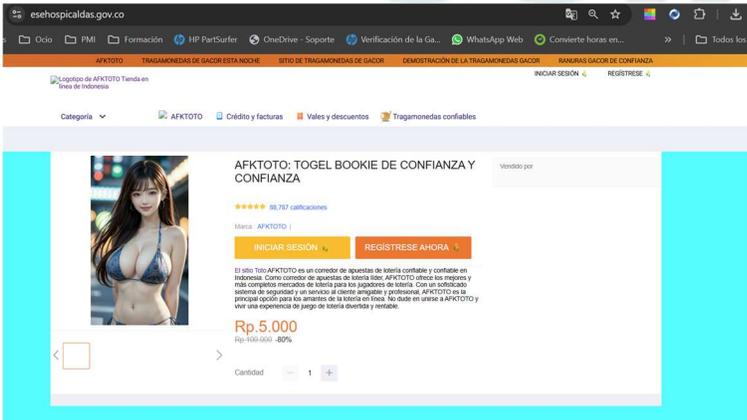


Reporte de Incidentes

Fecha del Reporte: 5/11/2024 9:30 a. m.

Datos de Contacto de la Entidad		
Nombre de la Entidad: E.S.E. Hospital San Vicente de Paul de Caldas		
Dirección: Cra 48 #135sur - 41		Sede: Sede Principal
Sector: Salud	Ciudad: Caldas	Departamento: Antioquia
Nombre de Quien Reporta: Ruth Nacarina Garzon Urrea		
Cargo: Directora de Gobierno Digital, Tecnología e Información		Número Contacto: Fijo: 6044448061 Ext 124 Celular: 3002224531
Correo Electrónico: leadersistemas@esehospicaldas.gov.co		Skype: Escriba su usuario de Skype

Incidente	
Fecha y Hora del descubrimiento: 5/11/2024 7:00 a. m.	Nombre de la Persona que Detectó el Incidente: Leonardo Tangarife
Fecha y Hora de Detección: 5/11/2024 7:05 a. m.	Nombre del administrador del Activo Informático: Ruth Nacarina Garzón Urrea
<p>Descripción Detallada: El día de hoy 05/11/2024 a las 7:00 a.m., el comunicador de la ESE se comunicó con el área de TIC para reportar que la Página Web no cargaba correctamente y se visualizaba información de una página de apuestas de Indonesia.</p>	

Método de Detección:
<p>Ingresando a la página web y generando mensaje emergente e imagen de página modificada:</p>  <p>The screenshot shows a browser window with the URL 'esehospicaldas.gov.co'. The page content includes a navigation menu, a category dropdown, and a product listing for 'AFKTOTO: TOGEL BOOKIE DE CONFIANZA Y CONFIANZA'. The product price is listed as 'Rp. 5.000' with a '-80%' discount. A pop-up message is visible over the product listing, and the page content appears to be a modified version of the original website.</p>

Acciones Realizadas:

Se ingresa al portal de cpanel e ingresa correctamente.
Se realiza cambio de contraseña de todos los usuarios.
Se genera reporte a hostgator, solicitando revisión de la falla en el sitio Web.



Tiene 1 ticket abierto. El plazo para la primera respuesta es de hasta 24 horas hábiles.
¡Esté siempre atento antes de que sea finalizado!

Sitio fuera de línea
esehospicaldas.gov.co

PENDIENTE

488380
Número del ticket

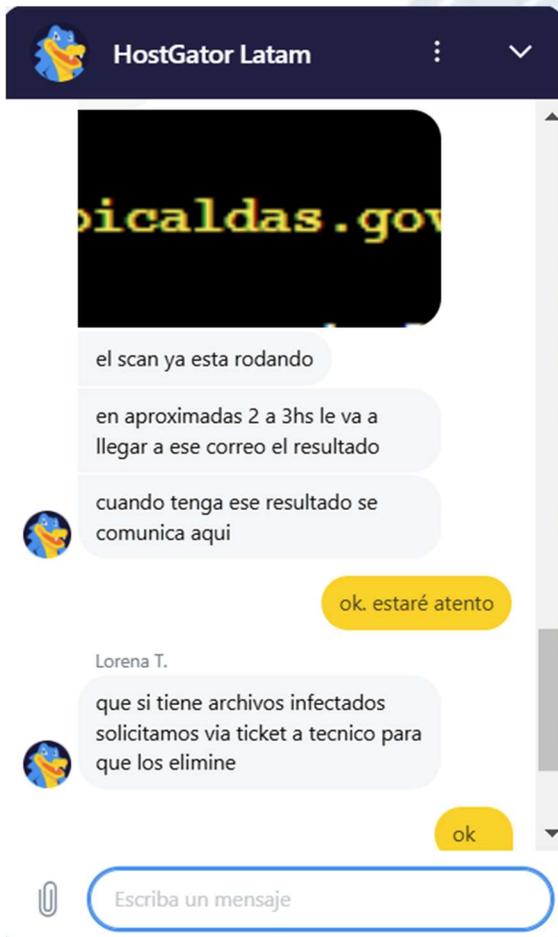
05/11/2024
Abierto

Nuevo ticket

Ver ticket

Acciones Pendientes:

Se debe modificar el index de la página principal.
Se debe restaurar la última copia de seguridad para activar de nuevo el sitio web.
En espera de respuesta por parte de hostgator del escaneo de los archivos de la página y del restablecimiento del backup



HostGator Latam

el scan ya esta rodando

en aproximadas 2 a 3hs le va a llegar a ese correo el resultado

cuando tenga ese resultado se comunica aqui

ok. estaré atento

Lorena T.

que si tiene archivos infectados solicitamos via ticket a tecnico para que los elimine

ok

Escriba un mensaje

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: Acceso no autorizado a 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: SI NO

Impacto del incidente: Financiero Reputacional Operacional Legal

REPUTACIONAL - OPERACIONAL

Causa Raíz:

Hasta el momento no se tiene claro cual fue la causa del incidente

Realizo Plan de Mejoramiento: SI 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:

Abierto Cerrado

El incidente ya se había presentado: SI NO SI, el 22/07/2022

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:



Csirtgob@mintic.gov.co



01 8000 910742 Opción 3.

CSIRT

