ACTUALIZACIÓN DE PROCEDIMIENTO DE INSTALACIÓN DE SECURIZACIÓN DE SERVIDORES Y EQUIPOS

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones informa de la **actualización** en el **procedimiento de instalación de securización de servidores y equipos** con fecha de 1 de febrero de 2022.

Debido a los ataques que diversas entidades del sector sanitario están recibiendo mediante código dañino, la Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones ruega encarecidamente **extremar la vigilancia y las precauciones** ante la posibilidad de ser abordados por *ransomware*. Llamamos vuestra atención sobre la necesidad de aplicar las siguientes instrucciones.

Instrucciones

A nivel técnico:

Paso 1. Mantener los dispositivos y aplicaciones actualizados: Contar con la última versión del navegador, sistema operativo, software o aplicación que utilicemos contribuirá a reforzar nuestra seguridad

---

Paso 2. Se debe **verificar** que el equipo está protegido con el **antivirus corporativo *Symantec Endpoint Protection***, dispone de las **últimas firmas publicadas y** tiene el **módulo IPS instalado y habilitado**.

Paso 3. Es **altamente recomendable verificar que está instalado** el **Agente EDR de Crowdstrike**. En caso contrario, puede ver **el procedimiento de instalación en la siguiente página: Instalación Agente EDR CrowdStrike**

Paso 4. Incluir IOCs (Indicadores de Compromiso) en proxies y firewalls provinciales

Actualmente desde la USTIC estamos trabajando en un sistema de implementación automática de IOC para el ámbito de la seguridad corporativa en distintas líneas de servicios de seguridad (proxies, firewalls, EDR...)

Los proxies **SQUID** son los primeros elementos de seguridad en los que se están pilotando esta solución, mediante una servicio de descarga diaria de los IOC del repositorio de Andalucia-CERT e integración en listas de denegación de Ip y dominios.

Este repositorio de Andalucia-CERT, a su vez, proviene de los análisis de la cibertinteligencia de la herramienta **REYES** (CC N-CERT).

Los **IOC que recomienda CCN-CERT**, que corresponden a indicadores de explotación de la vulnerabilidad, ya están incluidos en REYES, por lo que **se recomienda que se traten de manera automática** a través de la ejecución del script preparado para tal efecto.

El **script de configuración para la descarga e incorporación de los IOCs automática** es el siguiente: ScriptIOCautomatic .sh . En este script hay que sustituir <*password_ftp*> por la clave. Contactar con ustic.stic.sspa@juntadeandalucia.es para el envío de dichas credenciales.

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por su atención. Reciba un cordial saludo,

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud