Expone:

El presente informe trata de aportar aclaraciones al informe provisional emitido por el Consejo de Cuentas en relación a la iniciativa fiscalizadora en del plan Anual de Fiscalizaciones para el ejercicio 2021 del consejo de cuentas en sobre el "Análisis de la seguridad informática del Ayuntamiento de Palencia". Dejando constancia que desde el comienzo de la auditoría realizada por el Consejo de Cuentas se han realizado numerosas avances y mejoras en la infraestructura tal como se comentó durante el proceso presencial de revisión, ya que actualmente estamos inmersos en procesos de evolución continua en desarrollo de medidas de ciberseguridad que aporten mejoras sustanciales en los sistemas del organismo. Estas mejoras son debidas:

- Al continuo avance de contramedidas de mitigación de riesgos.
- A la mejora continua motivada por ser un sistema cambiante.
- Al proceso final de cumplimiento de medidas y procedimientos para la certificación ENS.
- A la adecuación de los sistemas para la implantación de la futura línea de ciberseguridad subvencionada por los fondos Next Generation.

Por todo ello queremos destacar que actualmente el informe provisional de auditoria en determinados apartados corresponde a revisiones anteriores que actualmente están obsoletas, corregidas las deficiencias posibles encontradas o en proceso final de actualización de medidas y procedimientos.

También remarcar la necesidad de no informar sobre cualquier dato que pueda ser utilizado como informe de ciberinteligencia para ciberdelincuentes que aprovechan información pública como base de conocimiento y realizar ataques dirigidos sobre posibles vulnerabilidades aportadas como puede ser el caso del apartado V - Resultado de la fiscalización.

Por ultimo constatar la importancia de la auditoría realizada en este ámbito para la mejora continua de los sistemas de ciberseguridad y agradecer la labor, compresión e interés mostrada por todos los integrantes del consejo de cuentas.

Alegaciones

A continuación, aportaremos los razonamientos y justificaciones para demostrar o apoyar la versión del organismo sobre aspectos, datos o valoraciones que consideramos de interés y que pueden puntualizar aspectos tratados en la auditoria de los cuales destacamos los siguientes apartados del informe provisional:

Apartado 3 Inventario y control de software autorizado y no autorizado (CBCS 2)

Alegación 1: Apartado V3.1

En la revisión realizada se detectó un equipo sin soporte, pero dicho equipo ya había sido retirado del sistema de forma física y únicamente constaba a nivel de inventario, por lo que lo consideramos un falso positivo.

Alegación 2: Apartado V 3.2.1

Los servidores que están fuera de soporte técnico, son equipos que dan soporte a software imprescindible para el correcto funcionamiento del Ayuntamiento y es necesario mantener con requisitos que no son aplicables en máquinas más actuales y con soporte. Además, se aplica un proceso de aislamiento para minimizar el impacto.

Alegación 3: Apartado V3.4

Según el modelo de evaluación definido el resultado obtenido en el cuadro 10 resultado control CBCS 2. Mostramos disconformidad en la valoración de L1 ”En el nivel L1 de madurez, el proceso existe, pero no se gestiona. Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad.”

Opinamos que toda la información aportada coincide con una clasificación mínima de L2 “En el nivel L2 de madurez, la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y riesgo.”

Apartado 5 Uso controlado de privilegios administrativos (CBCS 4)

Alegación 4:

En el aparatado III.5 se hace referencia que se siguen manteniendo en parte de su equipamiento cuentas genéricas, mostrando la disconformidad en esta cuestión. Tal y como se comenta en el aparatado V 5.2 solo se mantiene una cuenta genérica (empleada exclusivamente para la función desempeñada), al ser un sistema aislado fuera del dominio.

Alegación 5: Apartado V 5.4

Observamos que aun siendo una valoración positiva "Las medidas anteriores aplicadas en su conjunto serian eficaces si estas continúan y se consolidan, aunque es necesario realizar esfuerzos más decididos en este sentido.". La valoración final obtenida CBCS 4.4 Control poco efectivo. Por lo que mostramos nuestro desacuerdo en esta valoración.

Apartado 6 Configuración segura del Software y Hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores (CBCS 5)

Alegación 6: Apartado V 6.1.1

Como ya se comentó, los resultados obtenidos mediante la herramienta de comprobación del estado de seguridad de los dispositivos no expresa la realidad exacta del sistema, provocando falsos positivos en sus resultados Pues la herramienta si se utiliza con privilegios de usuario (mínimos privilegios) provoca errores al no tener permisos de lectura en mucha de las comprobaciones, y si aplicamos los permisos de administrador para su ejecución los resultados se desvirtúan debido al incremento de permisos dados. Por ello insistimos que para contrastarlo es necesario en paralelo revisar las políticas empleadas en los aspectos en los cuales la evaluación es deficiente. Ejemplo de ello pueden ser los apartados:

- OP.EXP.8 - Registro de actividad de los usuarios (0%)
- OP.EXP.10 - Protección de los registros de actividad (0%)

Que aportan valoraciones de 0% cuando por GPO son valores que están configurados. (Ver Anexo 1)

También queremos constatar la disconformidad de los valores citados y dado la importancia de su valoración y resultados sería recomendable revisar los valores obtenidos ya que los valores del organismo superan el 60% en el bastionado de equipos de usuario.

Por todo esto la valoración obtenida en el apartado CBCS 5.1 Control poco efectivo expresamos nuestro desacuerdo y discordancia con el resultado expresado.

Apartado 8 Copias de seguridad de datos y sistemas (CBCS 7)

Alegación 7: En relación con este apartado creemos que puede existir un posible error al valorar de forma discordante el mismo apartado III.8 copias de seguridad de datos y sistemas sección nº43 y apartado III.9 cumplimiento normativo sección 47.

Valoración final

Una vez aportado los datos que consideramos de interés solo nos queda agradecer el esfuerzo, cooperación y compresión por parte de todas las partes integrantes en este proceso de auditoria en relación al análisis de la seguridad informática de nuestro ayuntamiento, expresando la importancia de estos estudios que permiten analizar y optimizar los recursos informáticos del organismo, reducen los riesgos al eliminar y comprobar posibles vulnerabilidades del sistema tomando acciones antes de que se generen deficiencias y nos sirven como punto de control sobre el estado de situación en relación a la ciberseguridad con el fin último de conseguir una mejora continua en los sistemas.

En Palencia, a fecha de la firma electrónica

Fdo. Mario Simón Martín
Alcalde/Presidente