IMPLANTACIÓN DE UNA SOLUCIÓN PARA LA VIGILANCIA, SUPERVISIÓN Y AUDITORÍA DE LOS ACCESOS A LA INFORMACIÓN DE LOS DATOS NO ESTRUCTURADOS

Pliego de Prescripciones técnicas particulares.

1.- Objeto del Contrato.

Es objeto del contrato la adquisición y mantenimiento de una solución para la vigilancia, supervisión y auditoría de los accesos a la información de los datos no estructurados.

2.- Situación Actual.

El Consorcio de Aguas dispone de una serie de servidores de ficheros Windows donde se guardan los datos no estructurados (documentos, imágenes…) que son accesibles por los usuarios en función de los permisos correspondientes. En concreto se dispone de 10 Servidores de Ficheros principales a lo que habría que añadir carpetas compartidas distribuidas por el resto de los servidores de la organización.

El numero de usuarios que acceden a los recursos se estima en torno a 500.

Así mismo los usuarios tienen acceso a la plataforma de Office 365 (Teams, SharePoint, OneDrive…) donde también se alberga información de la empresa en diversos repositorios..

Debido al volumen y variedad de documentación que se encuentra en dichos repositorios, se ha visto la necesidad de adquirir una solución que permita controlar el acceso y uso que se hace de esa información y así mismo, poder cumplir la normativa GDPR.

3.- Características técnicas de la solución:

Entre las características de la solución se debe incluir al menos las siguientes:

1. La solución deberá incorporar una consola de gestión desde la que se podrá controlar la administración, operación y mantenimiento del sistema, así como la consulta, seguimiento y análisis de las incidencias detectadas. Se podrá monitorizar el estado y rendimiento del propio sistema.
2. Deberá permitir la configuración de distintos roles de administración y gestión, así como la personalización para cada uno de estos grupos. El número de usuarios con permisos de administración no estará restringido. La autenticación y autorización de los usuarios deberá poder integrarse con el Directorio Activo de Microsoft y la autenticación integrada de Windows.
3. Tendrá que integrarse con los almacenes de datos no estructurados existentes actualmente en el Consorcio de Aguas de Bilbao Bizkaia, así como permitir gestionar otros almacenes de datos que se puedan incorporar en un futuro. Los tipos de entornos requeridos son:
    a. Almacenamiento Windows
    b. Plataforma de Office 365: Sharepoint Online, Onedrive
4. Dispondrá de derechos de acceso a la propia aplicación para definir los diferentes perfiles de los usuarios del software.
5. En caso de que los servidores auditados estén descentralizados con líneas de comunicaciones lentas o de alta latencia debe disponer de la capacidad de gestionar el flujo de comunicación entre la sede remota y la sede central permitiendo la gestión del tráfico de red y no impactar en las comunicaciones compartidas.

6. Propondrá un sistema de almacenamiento de los logs de la información auditada basado en una base de datos SQL Server. Dicha base de datos también albergará la configuración del sistema propuesto.
7. El sistema será compatible con las funcionalidades de alta disponibilidad de la arquitectura de SQL Server proporcionada por el cliente.
8. Deberá disponer de un cliente para instalar en los puestos de trabajo de los administradores, evitando la necesidad de acceso remoto al servidor.
9. Disponer de una conservación de los logs generados por los usuarios durante un periodo flexible y configurable por parte del Consorcio en una base de datos específica, así como un sistema de archivado y recuperación que permita gestionar de manera óptima el almacenamiento e histórico de la información recolectada cuando sea necesario.
10. Sistema de auto-vigilancia de la propia herramienta que detecte y notifique:
    - El fallo de la auditoría de los servidores monitorizados
    - Falta de espacio en la Base de datos de la aplicación
    - Fallo de alguno de los servicios dependientes tanto de la herramienta de supervisión como de los servidores monitorizados
11. Despliegue de la solución
    - El despliegue de la instalación debe poder ser realizado en dos semanas desde que se adjudique el proyecto y se cumplan los requisitos de instalación.
    - Debe disponer de un diseño de implementación en gran escala con posibilidad de implementar una arquitectura de alta disponibilidad y tolerante antes fallos para los diferentes roles de servidores.

4.- Auditoría de actividad de Acceso

La solución propuesta deberá tener el control de todos los accesos a los ficheros de todos los almacenes de información monitorizados. Podrá auditar y consultar todos los logs de acceso a los ficheros contenidos en carpetas compartidas. Para ello, se requiere que la solución cuente con las siguientes funcionalidades:

1. Dispondrá de auditoria exhaustiva de todos los eventos de acceso a la información contenida en carpetas compartidas: fichero abierto, modificado, borrado, movido, renombrado, o bien carpeta abierta, modificada, movida, o renombrada, así como los cambios de permisos realizados en las carpetas monitorizas.
2. Debe poder procesar todos los eventos generados por el sistema auditado.
3. Dicha auditoría debe estar disponible en formato listable y en formato gráfico con filtros preestablecidos como pueden ser:
    a. Usuarios con más o menos actividad
    b. Carpetas con más o menos actividad
    c. Directorios accedidos por un usuario concreto
    d. Usuarios que han accedido a un directorio concreto
    e. Ficheros compartidos con enlace público fuera de la organización
    f. Usuarios fuera de la organización con acceso a ficheros de la organización compartidos públicamente.
4. En dicha auditoría de actividad se deben identificar la siguiente información del evento:
    a. Dirección IP y nombre del equipo desde el que se realiza la operación
    b. En el caso de la plataforma Office 365 se debe poder identificar la IP pública del equipo del usuario que está generando la actividad en Office 365.
    c. Si el fichero accedido está identificado por alguna regla de clasificación de la información
5. Para la auditoría de los file Servers se deberá contar con un agente propietario y no depender de la auditoría nativa de Windows.

6. Si el sistema auditado requiere instalación de agente, éste deberá garantizar el impacto mínimo en el rendimiento de los sistemas monitorizados.
7. Deberá disponer de un sistema de búsqueda personalizable de logs desde el cual se podrá buscar de manera central los logs de carpetas compartidas. Además, la búsqueda deberá ser ágil, y la solución deberá proponer la posibilidad de filtrar los logs para buscar los logs generados por un usuario en concreto, sobre un recurso en concreto, durante un cierto periodo de tiempo, etc.
8. El análisis forense de actividad debe estar disponible tanto por cliente pesado como por cliente WEB permitiendo en ambos la exportación de los resultados generados a ficheros estructurados.
9. Tendrá la posibilidad de exportar los resultados de una búsqueda a una hoja Excel, un fichero PDF o un fichero csv de manera rápida y directa además de ofrecer un sistema de informes personalizable en las consultas de la información suministrada.
10. Deberá permitir generar búsquedas personalizadas, almacenarlas y reutilizarlas sin necesidad de configurarlas de nuevo, así como permitir la programación y envió periódico de la activad mediante informes en diversos formatos a través del correo electrónico.

5 . Gobierno de la Seguridad de los datos Auditados

La solución propuesta debe permitir realizar las labores de administración de permisos de los servidores monitorizados. Entre ellos:

1. Permitir la gestión unificada de todos los entornos auditados desde una única consola.
2. Permitir la auditoria de los permisos de acceso a las carpetas compartidas en la red. El sistema deberá ser capaz de diferenciar los permisos NTFS de los permisos compartidos en la red.
3. Permitir la gestión de los permisos de acceso de manera sencilla, e incluir una funcionalidad de simulación para poder hacer cambios sin afectar a los permisos definidos en producción.
4. Permitir la identificación gráfica y por informes de las carpetas afectadas por inconsistencias de permisos.
5. Alertar del fallo de aplicación de permisos en caso de detectar una inconsistencia en la ruta afectada por el cambio.
6. Permitir el análisis de las estadísticas de acceso de cada usuario sobre los diferentes recursos auditados.
7. La solución debe permitir búsquedas bidireccionales de accesos basadas en usuarios, datos o la combinación de estas.
8. La herramienta deberá ofrecer recomendaciones en los permisos y grupos en base a actividad y tipo de actividad, recomendado por ejemplo eliminación de usos inactivos o de permisos inactivos en los recursos de los servidores monitorizados. El rango de inactividad de los recursos inactivos debe ser personalizable en el tiempo.
9. La herramienta debe Incluir la capacidad de asignar sobre cada carpeta del sistema un potencial propietario de la información para permitir un seguimiento sencillo de la carpeta, así como la capacidad de configurar un informe automático de dicha actividad al propietario. La asignación de dicho propietario también se debe poder realizar de manera masiva mediante un fichero predefinido.
10. Toda la actividad realizada desde la consola en la gestión de permisos deberá ser registrada por la solución propuesta permitiendo las siguientes funcionalidades:
    a. Revisión de los cambios propuestos basados en roles de revisión y autorización
    b. Permitir el rollback de los procesos a la situación previa al cambio.
    c. Permitir la planificación de la realización de los cambios en fecha y hora concreta.
    d. Permitir la elaboración de informes periódicos y la notificación automática mediante correo electrónico.
    e. Permitir la búsqueda e informes de acciones realizadas por la consola del producto identificando al operador que las realizó y los objetos afectados por el cambio.
11. Todos los cambios realizados de permisos deben permitir comparativas de la nueva configuración con la

configuración previa al cambio.

6.- Clasificación de la información

La solución propuesta podrá localizar y señalar los datos de carácter personal de manera general, y sobre un usuario en concreto. Para ello, la solución:

1. Dispondrá de un sistema de clasificación de la información para detectar los PII (Personally Identifiable Information o información de carácter personal) sobre los ciudadanos de la Unión Europea, y los PCI (Payment Card Information o información de tarjetas de pago) así como los datos personales tratados por la normativa GDPR.
2. Dispondrá de un sistema de detección de contraseñas en ficheros sin protección.
3. Permitirá la clasificación de la información sobre ficheros Office, PDF, ficheros de texto plano, así como permitir la clasificación en función de extensiones de archivos, por ejemplo, archivos multimedia.
4. Podrá escanear los permisos sobre las carpetas que contienen información de carácter personal de cara a evaluar el riesgo asociado.
5. Permitirá la creación de patrones específicos para realizar la búsqueda de expresiones regulares. Esas expresiones podrán corresponder a los datos a carácter personal sobre un usuario en concreto, o bien podrá ser una palabra específica que podría corresponder a un proyecto sensible en Aguas de Bilbao. Dicha personalización también debe permitir la incorporación de diccionarios personalizables en temáticas generales o definidas por Aguas de Bilbao.
6. Permitirá listar por informes los ficheros que contienen algún tipo de calificación identificando Política de cumplimiento y tipo de dato y si el tipo de permiso de acceso a dicha información es de acceso global o nominativo.
7. Dispondrá de una clasificación que se reflejará sobre los datos como un metadato adicional tipo tag/flag, integrable con otras soluciones de seguridad vía API o algún conector.
8. La herramienta debe permitir la opción de poder importar información de clasificación de otros sistemas, p.e. DLP, de manera automática e incorporarlos a la gestión de la clasificación de la solución.

7.- Alertas

La solución propuesta detectará las amenazas potenciales y reales que puedan afectar a la información, las infracciones de seguridad y avisará sobre esos problemas en tiempo casi real. Por consiguiente, la solución:

1. Deberá disponer de la capacidad de detectar alertas comportamentales basadas en comportamientos en el exceso de eventos, cambio de actividad o accesos inusuales a carpetas sin actividad, así como borrados masivos de la información.
2. Además, estas alertas deberán tener en cuenta la clasificación de la información previamente detallada de cara a proveer alertas sobre las incidencias sobre la información de carácter personal. Finalmente, también hay que tener en cuenta la dirección IP y el nombre del equipo desde donde se generan los eventos para detectar acciones de intrusión.
3. Se valorará la disponibilidad de alertas predefinidas para la actuación a las amenazas más comunes de ciberataques, así como la posibilidad de actualización y ampliación de estas alertas en la evolución de la solución.
4. Se debe permitir la creación de alertas a medida basadas en cualquier propiedad identificada en la información de los eventos auditados por la solución
5. Se debe permitir la creación de alertas personalizadas en función del tipo de evento generado, del número de eventos generados durante un cierto periodo de tiempo, del usuario que ha generado el evento, de cuándo ha ocurrido el evento, qué objeto del sistema de ficheros ha sido afectado por el cambio (servidor, carpeta, ruta, tipo de ficheros, etc.) y en qué período horario.
6. Se debe poder convertir una alerta en un mensaje tipo “syslog” o en un mensaje SNMP. Se deberá integrar de manera sencilla con un sistema SIEM.

7. Enviará alertas e informes mediante correo electrónico.
8. Permitirá el almacenamiento de los registros generados durante un periodo de tiempo flexible y configurable en una base de datos específica.
9. Actuación sobre la detección de la alerta mediante powershell, batch, programas ejecutables o VBScript obteniendo de manera sencilla las variables del script de los eventos que han generado la alerta. P.E: Deshabilitará automáticamente un usuario en caso de que genere una actividad sospechosa detectada por el sistema de alerta.
10. El sistema tendrá que disponer de un análisis del comportamiento de los usuarios para detectar las desviaciones: la herramienta tendrá que incluir modelos de amenazas predefinidos para detectar y parar ciertas acciones. Por ejemplo: detectar tentativas de conexión anormal, tentativas de acceso a carpetas que contienen ficheros con información de carácter personal, tentativa de robo o de fuga de información, comportamiento inhabitual por parte de administradores, ataques mediante ransomware, copia masiva sobre ficheros con información de carácter personal, etc.
11. Para evitar en lo posible falsos positivos, se debe permitir la identificación manual y automática de cuentas administrativas o de servicio con patrones diferentes que adapten la alerta al comportamiento típico de su comportamiento.
12. Permitirá la definición de perfiles de usuarios para que las alertas respondan de manera diferente en función de dichos perfiles: Los perfiles deben permitir identificar: cuentas administrativas, cuentas de servicio y cuentas que manejen información crítica.
13. Soporte del fabricante ante alertas y comportamientos no soportados para el posterior desarrollo e implementación en las siguientes actualizaciones del producto, así como la disponibilidad para ayudar en el análisis de las alertas detectadas.

8.- Formación y documentación

Una vez implantada la solución, se realizará una formación, de mínimo una jornada, al personal del Consorcio que vaya a gestionar la herramienta de cara a que puedan ser capaces de administrar autónomamente la solución, y así mismo, se elaborará y entregará la documentación necesaria sobre la arquitectura implantada de la solución y los procedimientos de uso habituales para gestionarla.

9.- Soporte

Se ofertará una bolsa de horas de 100 horas a consumir durante la duración del contrato de cara a cubrir necesidades de soporte, incidencias, realización de tareas sobre la solución, actualizaciones del producto, formación…

10.- Infraestructura tecnológica

De cara a implementar los servidores y sistemas que soporten la solución, el Consorcio de Aguas dispone de la siguiente infraestructura tecnológica:

- Sistema de virtualización para servidores: Se dispone de 4 nodos VMware ESX 6.7 para la virtualización de servidores.
- Sistema de bases de datos: SQL Server 2017
- Se dispone de Directorio Activo de Microsoft, en equipos Windows 2012 R2.

Bilbao Bizkaia Ur Partzuergoa
Consorcio de Aguas Bilbao Bizkaia
Informatika Zuzendariordetza
Subdirección de Informática

Bilbao, a 4 de junio de 2020

El Gestor del Contrato
David Alonso Villafáfila

Subdirector de Informática
Jose Luis Unzueta