PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DE UNA SOLUCIÓN PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE EVENTOS (SIEM) PARA LA ADMINISTRACIÓN DEL PRINCIPADO DE ASTURIAS

Expediente Nº 27/2017

Contenido

1. Introducción 3
2. Objeto de la Contratación 5
3. Descripción del suministro a realizar 5
3.1. Características técnicas 5
3.1.1. Recolección de información 6
3.1.2. Almacenamiento de la información 7
3.1.3. Procesamiento de la información. 8
3.1.4. Modularidad y escalabilidad 9
3.1.5. Consola de gestión. 10
3.1.6. Integraciones. 11
3.1.7. Notificación y gestión de incidentes 12
3.1.8. Informes y representaciones gráficas. 12
3.1.9. Manuales de la herramienta. 13
3.1.10. Hardware de la solución. 13
4. Servicios de instalación y soporte 13
5. Servicios de formación 14

1. Introducción

En los últimos años la Administración del Principado de Asturias ha hecho un importante esfuerzo en el ámbito de las tecnologías de la información, avanzando de forma importante en temas como la administración electrónica, los servicios electrónicos al ciudadano o la interconexión con otras administraciones y redes de terceros. En todo este proceso, la importancia y la criticidad del uso de la red Internet ha aumentado decisivamente, hasta convertirse en un servicio crítico para la Administración del Principado de Asturias y que por tanto debe ser objeto de especial salvaguarda. El permanente procesamiento de datos en numerosos sistemas informáticos, los crecientes servicios electrónicos, el uso de herramientas corporativas como el correo, las aplicaciones que facilitan el día a día del personal de las distintas Consejerías, todo ello conforma un vasto parque de datos, ficheros, identidades digitales, aplicaciones, servicios a la ciudadanía, que deben regularse en su uso atendiendo a criterios de disponibilidad, confiabilidad y máxima seguridad.

Es, vital que estos sistemas informáticos cumplan con su finalidad en las mejores condiciones técnicas y operativas, pero sin olvidar tampoco la atención prioritaria a la seguridad y a la protección de la información; la actual coyuntura de virulencia de los ataques informáticos obliga a rediseñar los mecanismos de seguridad y a disponer de dispositivos de última generación, con el objetivo de garantizar el mayor nivel posible de protección proactiva frente a cualquier ataque malicioso que se ejecute contra las infraestructuras y datos de la Organización.

Hoy en día los ataques a organizaciones son cada vez más sofisticados e inmunes a la detección por parte de dispositivos convencionales como IDS (Sistema de detección de intrusiones) o IPS (Sistema de prevención de intrusiones). Los indicios de posibles actividades maliciosas pueden ser difíciles de observar y pueden llegar a pasar desapercibidas. Se hace necesario por lo tanto, revisar y hacer continua correlación de indicios, de sucesos acaecidos sobre nuestros sistemas, de respuestas y tráficos entre activos, usuarios, redes y dispositivos, para así encadenar y entender lo que pueden parecer acciones inconexas o inocentes con el objetivo de finalmente detectar, lo más pronto posible, una intrusión en nuestros sistemas; se pretende, en definitiva, implementar un sistema que permitan analizar, comprender y reaccionar ante los eventos de seguridad que se produzcan en nuestra organización.

Sin embargo, llevar a cabo estas tareas de análisis es realmente complejo, ya que el número de fuentes que pueden generar eventos de seguridad es cada vez mayor; firewalls, IPS/IDS, VPN, Servidores Web, logs de aplicaciones, PC de usuarios, portátiles, dispositivos móviles, cámaras de video vigilancia, registros de entrada física a los edificios, etc.

Enfrentados a volúmenes ingentes de eventos que no pueden ser controlados de una forma manual, que carecen de sentido en cuanto que descontextualizados hemos de ser capaces de ensamblarlos con otros eventos provenientes de fuentes complementarias. Nuestro sistema de análisis ha de ser capaz de aplicar inteligencia en esa correlación de eventos. Además es imprescindible que realice su análisis en tiempo real, ya que en la mayoría de los casos la velocidad de detección será clave para que podamos reaccionar a tiempo ante una amenaza o incidente grave de seguridad.

Se han desarrollado muchas herramientas para ayudar a las organizaciones en este ámbito de análisis de seguridad, agrupándose comúnmente bajo la denominación genérica de SIEM. Un SIEM (Security Information and Event Management) es una definición utilizada para aplicaciones que involucran a SEM (Security Event Management) o gestión de eventos de seguridad y SIM (Security Information Management) o gestión de información de seguridad, que correlaciona, normaliza e informa sobre los datos de eventos de seguridad recogidos, esencialmente es una capa de gestión por encima de los sistemas existentes y los controles de seguridad que conecta y unifica la información contenida en los sistemas existentes permitiendo que sean analizados y referenciados de manera cruzada desde una única interfaz. A día de hoy se considera que la presencia de un SIEM es imprescindible para reducir los graves riesgos que se ciernen sobre los sistemas de organizaciones como la nuestra.

Se hace necesario disponer de un sistema SIEM (Security Information and Event Management, gestión de la seguridad de la información y gestión de eventos), para detectar y seguir la pista de posibles ataques para no perdernos entre los innumerables ficheros de logs (ficheros de registros de actividad de un sistema informático) y para gestionar proactivamente, y con eficacia, las alertas, o evidencias de posibles alertas, de nuestros heterogéneos sistemas de información.

La Administración del Principado de Asturias, debido a su grado de implantación TIC para el desempeño de sus tareas, dispone de innumerables ficheros de logs que deben ser centralizados y analizados minuciosamente en una infraestructura centralizada, intentando asegurar niveles aceptables de confidencialidad, integridad y disponibilidad en la información.

En definitiva, una herramienta o solución SIEM nos ayudará a identificar y responder a ataques que podrían pasar desapercibidos por nuestros sistemas de defensa convencionales. Además, nos ayudarán a administrar y archivar nuestros logs más fácilmente y a generar valiosos informes técnicos y ejecutivos, así como disponer de un método efectivo para una "defensa en profundidad".

Nuestra protección contra ataques debe basarse en una pronta capacidad de detección y de respuesta, en una actitud no reactiva sino de defensa continua y de vigilancia permanente; la clave de esa respuesta eficaz está en su potencial para planificar y para detectar, en su capacidad para recoger datos de lo que pasa en tiempo real y en tiempo forense, en la inteligencia para agrupar y procesar de forma centralizada datos e indicios y generar incidentes de seguridad que se traten correctamente en tiempo y forma.

Es por ello que la Administración del Principado de Asturias busca dotar a su infraestructura de seguridad de una solución específica SIEM, en la línea de lo previamente expuesto en esta introducción, para la mejor protección de sus activos y para el mayor control de cualquier incidente que se produzca.

2. Objeto de la Contratación

El objeto de esta contratación es el suministro de una solución integral para la gestión, análisis, retención y correlación de logs (registros de actividad) de la infraestructura IT de la Administración del Principado de Asturias (en adelante APA), producto denominado SIEM (Security Information and Event Management, gestión de la seguridad de la información y gestión de eventos), con el fin de disponer de una inteligencia de seguridad en tiempo real aumentando con ello la visibilidad y mejorando la protección de los activos de información.

El suministro incluye la instalación, configuración, optimización y puesta en marcha de la solución de acuerdo con lo descrito en este pliego.

3. Descripción del suministro a realizar

3.1. Características técnicas

La herramienta objeto del contrato es una solución para la recolección, análisis y correlación de eventos e información de seguridad que facilitará el almacenamiento y la gestión combinada de información y eventos de seguridad, generando alertas en tiempo real y permitiendo configuraciones específicas de la herramienta en base a las necesidades de la APA.

La solución ofertada debe constar de los siguientes componentes:

- Hardware y software necesario para la recolección de todos los eventos y almacenaje de los mismos, integrándose con los sistemas actuales y complementando su potencial.
- Software necesario para el análisis y filtrado de todos los eventos almacenados, así como para la interrelación de eventos en tiempo real.
- Software de integración de todas las herramientas utilizadas en una única consola.
- Licencias.

Las características técnicas solicitadas en este pliego se dividen en diez grupos (**recolección de información, almacenamiento de la información, procesamiento de la información, modularidad y escalabilidad, consola de gestión, integraciones, notificación y gestión de incidentes, generación de informes, manuales de la herramienta y hardware de la solución**), las cuales están referidas a la solución de seguridad del suministro.

3.1.1. Recolección de información

En el proceso de recolección de información se pueden utilizar **conectores**, entendiéndose como tales, los módulos software que recogen, pre-procesan y normalizan la información de un tipo concreto de fuente de eventos.

Por otro lado, en el presente pliego se denomina **sonda** al dispositivo o elemento, que mediante un conector o a través de un protocolo seguro de envío de logs, proporciona información para su posterior procesamiento en el motor de correlación o almacenamiento de forma centralizada, es decir, un conector se utiliza en la conexión de varias sondas de la misma tipología.

A continuación se indican las características mínimas de la herramienta SIEM que se solicitan relativas a la recolección de la información:

1. Recolección de información
1.1 Compatibilidad
La herramienta SIEM es compatible con todos los fabricantes fuentes de eventos que se utilizan en la Administración del Principado de Asturias.
1.2 Conectores Predeterminados
Dispone de un conjunto de conectores predeterminados (por defecto) que permiten la agregación de datos de distintas fuentes con distintos formatos (por ejemplo, conectores predeterminados para IDS, IPS o firewalls).
1.3 Creación de nuevos conectores
La solución de seguridad SIEM se proporciona con un manual de creación de nuevos conectores para llevar a cabo la conexión necesaria para que la información recogida de

distintas fuentes de datos (logs, bases de datos, xml) sea enviada e interpretada correctamente por la herramienta SIEM para su procesamiento.
1.4 Recopilación de logs de eventos en Windows y Linux
Recopila los eventos generados por las máquinas Windows y Linux.
1.5 Normalización
Permite una normalización de la información heterogénea recolectada en un modelo de amenazas común a todas las sondas, permitiendo la personalización de los campos.
1.6 Recolección segura y fiable de eventos
Realiza una recolección de forma segura y fiable de todos los eventos.
1.7 Firmado de logs
Realiza firmado de los logs recogidos y realiza sincronización en tiempo NTP (Network Time Protocol) con el fin de garantizar la integridad de los datos.
1.8 Rendimiento de recolección
Soporta 7.000 EPS (Eventos por segundo) en momentos normales y 12.500 EPS (Eventos Por Segundo) en momentos pico.

3.1.2. Almacenamiento de la información

A continuación se indican las características mínimas de la herramienta SIEM que se solicitan relativas al almacenamiento de la información:

2. Almacenamiento de la información
2.1 Seguridad de la solución
Toda la información y eventos de seguridad recogidos se mantienen en el sistema atendiendo a los requisitos de confidencialidad, integridad y disponibilidad.
2.2 Grandes Volúmenes de información
Dispone de almacenamiento, búsqueda y procesamiento eficiente de grandes volúmenes de información (Big Data), haciendo uso para ello de técnicas de indexación que permitan realizar investigaciones, análisis forenses y estudios en profundidad sobre los datos almacenados.
Dispone de capacidad de almacenamiento para la información tanto correlacionada como sin correlacionar. Ambos tipos de información estarán fuertemente indexadas y mantendrán la eficiencia y rendimiento en las búsquedas.
2.3 Tratamiento de logs a altas velocidades
Debe recopilar, analizar, normalizar, indexar y almacenar logs de seguridad a altas velocidades (más allá de 10k eventos por segundo y por nodo).
2.4 Configuración del tiempo de retención de los datos almacenados
Dispone de la posibilidad de configurar el tiempo de almacenamiento de la información en base a las necesidades que puedan surgir. El tiempo el almacenamiento online debe ser al **menos de 6 meses**.
2.5 Redimensionado del almacenamiento
Dispone de capacidad de redimensionamiento del almacenamiento, proporcionando mayor

escalabilidad en capacidad de retención y mejoras en el rendimiento de búsquedas, sin realizar cambios significativos en la configuración del sistema.

3.1.3. Procesamiento de la información.

A continuación se indican las características mínimas de la herramienta SIEM que se solicitan para el procesamiento de la información o la correlación de eventos de seguridad:

3. Procesamiento de la información
3.1 Inteligencia "out-of-the-box" (fuera de la caja)
Dispone de inteligencia "out-of-the-box", de forma que una vez instalada la herramienta, simplemente recibiendo logs, las reglas definidas por defecto proporcionen inteligencia sobre la actividad detectada.
3.2 Inclusión de reglas de correlación, alertas y políticas de forma sencilla
Dispone de la creación de reglas de correlación, alertas y políticas por parte del usuario de manera sencilla, además de la posibilidad de modificación de las ya existentes en función de las necesidades de la Administración del Principado de Asturias.
3.3 Alertas en tiempo real
El análisis automatizado de la información capturada deberá generar alertas en tiempo real (alerta temprana) configurables por el usuario de la herramienta SIEM.
3.4 Generación de conjuntos dinámicos de datos
Dispone de generación de conjuntos dinámicos de datos a partir de información procesada y reutilizable en reglas de correlación u otras acciones.
3.5 Clasificación de ataques y amenazas
Dispone de identificación y clasificación de los ataques y amenazas en tiempo real en función de su criticidad y/o prioridad y la posibilidad de modificación por parte del usuario de la solución, usando simultáneamente la lógica basada en reglas y en el riesgo.
3.6 Análisis y ejecución en memoria
El análisis de eventos de seguridad y ejecución de reglas en tiempo real, se realizan directamente en memoria, sin acceso a disco.
3.7 Reducción de la tasa de falsos positivos
Dispone de algoritmos optimizados para la reducción de la tasa de falsos positivos durante el procesamiento de la información.
3.8 Priorización de procesamiento
Dispone de la posibilidad de que durante el procesamiento de los datos (correlación) se permita la priorización en el procesamiento de los mismos en función de la criticidad de la fuente.
3.9 Rendimiento de correlación
El rendimiento de la solución en cuanto al volumen de eventos que se pueden procesar en el motor de correlación deberá ser de, al menos 7.000 EPS (Eventos Por Segundo) en momentos normales, y 12.500 EPS (Eventos Por Segundo) en momentos pico.
3.10 Detección de anomalías basado en los flujos de red
Dispone de capacidad para la detección de anomalías basado en los flujos de red.
3.11 Correlación histórica

Dispone de un modelo de correlación histórica, para la detección/evaluación recursiva de amenazas e imprescindible para investigación forense.
3.12 Modelo estadístico
Dispone de un modelo estadístico para la generación de alertas.

3.1.4. Modularidad y escalabilidad

A continuación se indican las características mínimas que se solicitan para la modularidad y escalabilidad de la solución de seguridad SIEM:

4. Modularidad y escalabilidad
4.1 Arquitectura modular y escalable
La solución de seguridad SIEM dispone de una arquitectura modular en su conjunto y es fácilmente escalable atendiendo a las necesidades de procesamiento de información que surjan, para proporcionar una detección en tiempo real o bien manejar el crecimiento continuo de manera fluida sin perder calidad en la solución ofrecida.
4.2 Arquitectura de balanceo
La solución de seguridad SIEM dispone de una arquitectura de balanceo integrada para recoger eventos desde sitios remotos.
4.3 Arquitectura con distintos formatos de appliances
La solución se seguridad SIEM dispone de appliances en formato físico y virtual que permiten ajustarse a las necesidades de recolección y procesamiento de los eventos y flujos de la organización. La arquitectura permite utilizar en un mismo despliegue los diferentes formatos de appliances, ofreciendo una arquitectura flexible y fácilmente adaptable a las necesidades del entorno.

3.1.5. Consola de gestión.

A continuación se indican las características mínimas de la interfaz o consola de gestión de la solución de seguridad SIEM que se solicitan:

5. Consola de gestión
5.1 Consola de gestión única
La solución de seguridad SIEM dispone de una consola de gestión única que facilitará la gestión de los eventos, alertas e informes. Se tendrá acceso a la información de seguridad según pertenencia de cada perfil.
La consola de gestión será basada en web.
5.2 Control de acceso basado en roles
Dispone de un control de acceso basado en roles para restringir el acceso a la consola y a los datos.
5.3 Interfaz intuitiva
Dispone de una interfaz de administración intuitiva desde la que configurar todas las opciones disponibles en la herramienta SIEM
5.4 Visualización del estado global
Dispone de visualización en la misma consola del estado del parque tecnológico y los eventos de seguridad.
5.5 Información intuitiva y personalizable
La información se presenta de forma homogénea e intuitiva al usuario, de modo que la comprenda fácilmente sin necesidad de estar familiarizado con la sintaxis concreta de la fuente de la que proceden los datos. Dispone además de opción de personalizar las vistas mostrando u ocultando distintos campos de datos o agrupando la información en función de distintos factores, como por ejemplo: tipo de sonda, de ataque, IP y criticidad.
5.6 Consultas y trazabilidad de los ataques detectados
Se permite acceder a toda la información necesaria para determinar la naturaleza del ataque (contexto, sensor, logs, vinculación con otros elementos dentro del sistema), sin necesidad de acceder a las máquinas receptoras de dicho ataque para obtener información detallada del mismo; además se usarán gráficas para facilitar la identificación y relación entre todos los elementos implicados.
5.7 Segregación de funciones
Dispone de separación de funciones, dentro del flujo de trabajo, dependiendo del rol de acceso del usuario que utilice la herramienta SIEM.
5.8 Gráficos interactivos
Se dispone de gráficos interactivos que muestran la topología de la infraestructura física y la conectividad entre dispositivos de red y la vía de acceso de red que utilizan para comunicarse, junto con los puertos, protocolos y reglas.
5.9 Exportación de datos
Desde la consola se permite la exportación de los datos consultados o resultados de búsquedas específicas en diversos formatos.
5.10 Sistema de ayuda
Dispone de un sistema de ayuda correcto y completo.

3.1.6. Integraciones.

A continuación se indican las características mínimas de integraciones de la solución de seguridad SIEM que se solicitan:

6. Integraciones
6.1 Sistema corporativo de gestión de incidencias
Integración con el sistema corporativo de gestión y seguimiento de incidencias de la organización.
6.2 Fuentes de inteligencia de ciberincidentes
Permite la integración con fuentes de inteligencia de ciberincidentes, CTI (Cyber Threat Intelligence). Las fuentes de inteligencia de ciberincidentes ofrecen información valiosa relativa a ataques actuales y potenciales.
6.3 Análisis de vulnerabilidades
Permite la integración con escáneres de vulnerabilidades.
6.4 Sistema de autenticación corporativo
Permite usar un sistema de autenticación centralizado, en concreto, permite usar el directorio corporativo de usuarios de la Administración del Principado de Asturias, para la autenticación de los usuarios administradores de la consola de gestión única.
6.5 Integración con herramientas para analizar comportamiento de usuarios
Permite la integración con herramientas específicas para realizar análisis del comportamiento de usuarios. Este análisis es empleado para disponer de visibilidad sobre las amenazas internas, y esto se consigue analizando los patrones de uso de los usuarios internos para determinar si sus credenciales y sistemas se han visto comprometidos por ciberdelincuentes.
6.6 Integración con herramientas de análisis forense
Permite la integración con herramientas de análisis forense para poder seguir la traza de las acciones realizadas por un atacante, también proporciona las funcionalidades para poder realizar de forma rápida y simple, investigaciones sobre incidentes de seguridad producidos en las redes, sospechosas de contener algún tipo de malware.
6.7 Integración con terceros fabricantes
Dispone de integración con terceros fabricantes, permitiendo aumentar la funcionalidad de la solución de seguridad SIEM, pudiendo disponer de una API para facilitar una integración más personalizada.

3.1.7. Notificación y gestión de incidentes

A continuación se indican las características mínimas de notificación y gestión de incidentes de la solución de seguridad SIEM que se solicitan:

7. Notificación y gestión de incidentes
7.1 Notificación de incidentes
Dispone de un framework de notificación de incidentes basado en políticas.
7.2 Secuencia de comandos de corrección
Dispone de la posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico, es decir, en caso de detectar un incidente de seguridad, además de generar una alerta, abrir un ticket o enviar un email, la solución de seguridad SIEM es capaz de ejecutar scripts que realicen una tarea definida en el mismo.
7.3 Sistema de ticketing
Dispone de un sistema de ticketing (sistema de gestión de incidentes) incorporado.

3.1.8. Informes y representaciones gráficas.

A continuación se indican las características mínimas de la solución de seguridad SIEM que se solicitan para la generación de informes y representaciones gráficas:

8. Informes y representaciones gráficas
8.1 Generación de informes según perfil
Dispone de generación de distintos tipos de informes según el perfil al que vayan destinados. Las plantillas de los informes están enfocadas a distintos perfiles dentro de la organización (auditor, técnico de seguridad, responsables de proyecto, director), pudiendo modificar dichas plantillas por el usuario atendiendo a sus necesidades.
8.2 Generación de informes desde cero
Dispone de generación de informes desde cero.
8.3 Explotación estadística
Dispone de un módulo de explotación estadística (dashboard) de la información recabada, personalizable por el usuario. La información estadística a obtener se puede configurar por el usuario y se apoyará en gráficas y tablas que facilitan su interpretación.
8.4 Personalización del formato de los informes
Dispone o permite la inclusión de logos corporativos, selección del formato de texto, de los colores, del formato para la generación de informes (XML, PDF, DOC), así como la inclusión de nuevos campos definidos por la Administración del Principado de Asturias.

3.1.9. Manuales de la herramienta.

La herramienta SIEM deberá venir provista con los siguientes manuales en el idioma castellano:

- Manual de instalación.
- Manual de configuración.
- Manual de uso.

Todo ello se realizará atendiendo a los criterios necesarios que puedan ser explicados por el Jefe de Proyecto de la DGTIC y en general siguiendo las metodologías existentes en la Administración del Principado de Asturias.

3.1.10. Hardware de la solución.

El hardware proporcionado con la solución debe tener las siguientes características mínimas:

- El hardware aportado para la solución de seguridad SIEM debe basarse en appliance/s dedicados.
- Cada equipo debe disponer de fuentes de alimentación redundante cambiables en caliente sin interrupción del servicio.
- Cada equipo debe disponer de soporte para IPv6 con tecnología de doble pila.
- Cada equipo de la solución debe contar con certificaciones de bajo consumo, protecciones de seguridad para su manipulación y compatibilidad electrónica.

4. Servicios de instalación y soporte

El contratista deberá prestar los servicios de instalación y soporte necesarios para la puesta operativa de la solución de seguridad SIEM, teniendo especial relevancia las siguientes tareas:

- Suministro de los componentes, servidores y licencias.
- Despliegue on-site de la solución SIEM. Toda la solución de seguridad SIEM debe ser desplegada y estar operativa en el Centro de Proceso de Datos (CPD) de la Administración del Principado de Asturias.
- Instalación y configuración de todos los componentes de la solución de seguridad SIEM.

- Estudio del tráfico y comportamiento de la red, así como de las posibles vulnerabilidades existentes, eventos generados y criticidad de los activos, para realizar un adecuado ajuste inicial personalizado de la solución ofertada y todos sus componentes. De esta forma se realizaría una correlación de los eventos y una configuración personalizada inicial para la eliminación de falsos positivos o configuración de alarmas que pudiesen ser importantes para la organización.

- Integración y recolección de eventos de los sistemas actuales de la Administración del Principado de Asturias.

5. Servicios de formación

El adjudicatario deberá prestar los servicios de formación o transferencia del conocimiento durante al menos cuatro sesiones (20 horas) sobre la operación y mantenimiento del sistema implantado. El contenido mínimo a impartir será el siguiente:

1. Principios básicos de la gestión de logs.
2. Arquitectura del sistema (Hardware, bases de datos que utiliza, comunicaciones con las fuentes, etc.).
3. Instalación del sistema (Hardware, base de datos que utiliza, integración y comunicación con otros elementos de la red, con Internet, etc.).
4. Instalación de los componentes de la solución de seguridad SIEM.
5. Arranque y parada del servicio.
6. Actualizaciones del sistema.
7. Tratamiento y explotación de los datos recopilados por la herramienta.
8. Creación de casos de uso, reglas de correlación.
9. Monitorización de la red y de actividades de log (filtrado de falsos positivos, búsquedas, agrupaciones y ordenaciones, almacenamiento de búsquedas, visualización de logs de auditorías, etc.).
10. Optimización, análisis y resolución de problemas en el sistema.
11. Configuración de fuentes específicas: parsing.
12. Configuración del cuadro de mando, generación y programación de informes.
13. Funcionalidad de informes, tratamiento de datos e información para la
14. Integración con otros sistemas.

La formación se realizará en las instalaciones de la Administración del Principado de Asturias.

Oviedo, a 25 de mayo de 2017

EL RESPONSABLE DE PROYECTOS DE SEGURIDAD

Fdo.: Luis Alberto Fernández Ardura