CASO DE ÉXITO

Grupo Azkoyen S.A. es una multinacional con sede central en Navarra (España) especializada en el diseño, fabricación y comercialización de soluciones tecnológicas para medios de pago, máquinas expendedoras y sistemas de seguridad y control de accesos. Dispone de centros de fabricación en Peralta (Navarra), Schio (Italia), Bristol (Reino Unido) y Pereira (Colombia), así como sedes comerciales en Francia, Alemania, Italia y Portugal.

Desde el año 1945 las máquinas y productos del Grupo Azkoyen son símbolo de confianza e innovación tecnológica. Esto se debe al espíritu del Azkoyen de adelantarse a las necesidades y exigencias de sus clientes, facilitar sus operaciones cotidianas y ayudar a dar respuesta a cambios en el estilo de vida.

El afán de innovación y la firme apuesta por el I+D+i les distingue y caracteriza. Esto, unido al avance de las nuevas tecnologías y las vulnerabilidades de las mismas, planteó a Azkoyen la necesidad de contar con un *partner* en el que confiar a la hora de analizar y mejorar sus infraestructuras de ciberseguridad, el cumplimiento normativo relacionado con la información que maneja y sus procedimientos internos. De este modo, Azkoyen podría seguir caracterizándose por su sello innovador y competitivo, y continuar situada entre los líderes de los sectores donde opera.

En este proceso de contar con un servicio gestionado para la seguridad de la información, que abarque infraestructuras, cumplimiento normativo y procedimientos, Azkoyen ha confiado su seguridad a **Secure&IT**. Los principales valores diferenciadores que **Secure&IT** aporta son la especialización y la visión 360°, ya que la empresa cubre tanto infraestructuras de seguridad y seguridad gestionada, así como aspectos de cumplimiento y procesos de seguridad.

En este sentido, **Grupo Azkoyen ha apostado por el programa Gold Security.** Este programa de reconocimiento y certificación, acredita un estricto cumplimiento de los controles de seguridad seleccionados por la compañía en los estándares y normativas de gestión de la seguridad.

De esta manera, se puede hacer un seguimiento constante de la empresa; llevar a cabo auditorías en todas las materias; establecer un plan de actuación; asegurarnos de que la empresa cumple la normativa; implantar las medidas tecnológicas necesarias; establecer procesos corporativos de gestión de la seguridad; certificar a la organización conforme a la norma ISO 27001; integrar los sistemas de TI en un SOC y, además, impartir formación continuada. Incluye, por tanto:

- **Protección de datos y cumplimiento normativo**
- **Procesos corporativos de seguridad**
- **Seguridad informática**
- **Seguridad gestionada, a través del SOC-CERT de Secure&IT**

En primer lugar, y como punto de partida, se llevó a cabo una auditoría integral que incluía *hacking* ético, auditoría de procesos y auditoría sobre el mapa regulatorio aplicable a la seguridad de la información. El objetivo era conocer la situación de partida de Azkoyen, para poder emplear el resultado de la auditoría como entrada en el Plan de Seguridad posterior. Durante esta auditoría se realizaron:

- **Hacking ético.** Se llevó a cabo un análisis profundo de vulnerabilidades de seguridad lógica basado en Caja Negra, es decir, un examen realizado desde el exterior de Azkoyen.
- **Configuraciones de equipos de seguridad.** Tras la auditoría en caja negra se efectuó un análisis de las configuraciones de los elementos de seguridad existentes en la sede central de la empresa, desde donde se presta servicio a todos los usuarios y sedes del Grupo.
- **Análisis de procesos corporativos de seguridad.** Este tipo de auditoría establece la guía matriz para analizar los riesgos que asume Azkoyen en lo referente a la información que maneja. Se trata de una metodología propia de **Secure&IT**, basada en 44 controles, que nacen a partir de las normas internacionales ISO 27001 (Gestión de la Seguridad de la

Información), ISO 20000 (Gestión de los Servicios de TI) e ISO 22301 (Gestión de la Continuidad de Negocio).

- **Auditoría de cumplimiento de marco legal y regulatorio.** La auditoría sobre la normativa afectada por la seguridad de la información tuvo como punto de partida la realización de la entonces preceptiva auditoría en materia de protección de datos. Además, se realizó un análisis del mapa regulatorio que afecta a Azkoyen en materia de seguridad de la información: normas que van desde la Ley de Servicios de la Sociedad de la Información a la Ley de Propiedad Intelectual o Protección de Datos.

Los aspectos de mejora identificados durante el proceso de auditoría constituyeron, junto con las buenas prácticas de seguridad, en un Plan de Seguridad diseñado a tres años, que incluyó múltiples proyectos encaminados a mejorar la seguridad de Azkoyen. Dentro de este plan se han ejecutado múltiples proyectos:

- **Auditorías de seguridad de hacking ético**

Se realizan auditorias anuales en dos modalidades, caja negra (exterior) y caja gris (interior). Dentro de una correcta planificación de protección preventiva y correctiva, se debe considerar este tipo de auditorías como una actividad clave, que nos asegure que estamos al día ante las crecientes amenazas. Estas auditorías nos ayudan a conocer el nivel de protección de los servicios y a establecer un plan de acción que solvente los problemas encontrados.

- **Seguridad perimetral**

Azkoyen partía de una situación en la que su seguridad perimetral descansaba sobre dispositivos Stonesoft, Juniper, F5, Blue Coat y otros fabricantes. Esto provocaba dificultad en la gestión y la falta de una visión global de la seguridad. El proyecto, que era complejo debido a la cantidad de elementos a integrar, consistió –en un primer momento- en la implantación de una barrera de seguridad basada en la plataforma Fortinet en alta disponibilidad y, sobre ella, se crearon las políticas de seguridad y gestión de Red necesarias. Esta plataforma se integró con el SIEM BigSIEM desarrollado por **Secure&IT**, que detecta eventos y alertas de seguridad en tiempo real.

En la actualidad, la seguridad perimetral sigue descansando en el fabricante Fortinet. Pero, en los últimos tres años, se han actualizado los equipos para que respondieran a las necesidades del cliente y a los avances tecnológicos. Las plataformas de seguridad FortiGate constituyen una nueva generación de

equipos de seguridad de muy alto rendimiento que garantizan la protección completa de los sistemas de empresas, en tiempo real.

Azkoyen tiene desplegados *firewalls* en todas sus sedes remotas (Madrid, Pamplona, Italia, Reino Unido, Alemania y Colombia) y en su sede central. El licenciamiento de estos equipos es UTP e incluye: 24x7 FortiCare *plus application control*, IPS, AV, *web filtering* y *antispam* y FortiSandbox Cloud.

- **Seguridad de puesto de trabajo**

Para acompañar a esta seguridad perimetral, se llevó a cabo el despliegue de la seguridad de puesto, en este caso con el fabricante Bitdefender. Además de disponer de un motor avanzado de detección de amenazas (el más laureado por las comparativas independientes), permite la administración del *endpoint* en lo referente a gestión de dispositivos, aplicaciones y accesos web.

Recientemente, se ha realizado un *upgrade* de las licencias de los *endpoint* de Bitdefender a la versión ULTRA, que añade a las capacidades de Bitdefender GravityZone, la unificación de la prevención, detección, respuesta y análisis de riesgos en los *endpoints*.

Además, Azkoyen tiene desplegado, junto con los *endpoints*, el módulo de cifrado que permite mantener los datos empresariales a salvo y cumplir con las normativas, y la gestión de parches de los dispositivos, que permite gestionar el parcheo y actualización de todas las aplicaciones de sus equipos. Todo ello completamente integrado en el SIEM del Centro de Operaciones de Seguridad (SOC-CERT) de **Secure&IT**.

- **Seguridad de servicios WEB - WAF (*web application firewall*)**

Como valor añadido y medida de protección extra para la infraestructura de Azkoyen, se desplegó la solución Fortiweb de Fortinet, un elemento de protección de sus servidores, servicios y aplicaciones web. Fortiweb tiene la capacidad de realizar escaneos de vulnerabilidades y permite mitigar ataques y riesgos provenientes de *botnets*, *proxies* anónimos, *host* maliciosos, etc. Todo mediante análisis de reputación IP; *DDoS protection* a nivel de aplicación; validación de protocolo HTTP (RFC); prevención de ataques conocidos mediante firmas; integración con *firewalls* FortiGate y FortiSandbox para detección de APT; protección avanzada contra escaneos, y análisis en base a comportamiento para prevenir ataques no conocidos.

- **Wifi segura**

Adicionalmente, Azkoyen contaba en sus delegaciones con puntos de acceso Cisco, sin controlador, lo que hacía más complicadas las tareas de configuración y mantenimiento. Estos puntos fueron sustituidos por la solución de Fortinet, basada en Forti AP, que se controla de forma centralizada por el clúster de la sede de Peralta (Navarra). Aquí hay que tener en cuenta el valor añadido que supone contar con Fortinet como respaldo en materia de seguridad: autenticación segura y robusta, integración con Radius y AD WPA2 Entreprise, Autoprovisionamiento Guest, Captive Portal + SSL, Perfiles IDS y Rogue AP Detection, etc. Todo ello gestionado y controlado de forma centralizada desde los *firewalls* FortiGate e integrando con las soluciones de SIEM y FortiAnalyzer de **Secure&IT.**

- **Bastionado de electrónica de red**

Con objeto de garantizar la seguridad de todas las comunicaciones, así como la correcta segmentación y control de accesos en la electrónica de red de Azkoyen, aparte de la integración con el SIEM para la recopilación de todos los eventos, se ha llevado a cabo la correcta aplicación de segmentación de redes a nivel 2 (*port security*, *anti spoofing* y *flooding*) como medida de restricción e identificación de direcciones MAC en los puertos; protección mediante configuración segura de los accesos remotos; correcta definición de las comunidades SNMP para la monitorización; configuración adecuada de HSRP, VRRP y STP. El objetivo es garantizar una correcta continuidad de negocio y prevenir impactos graves en el servicio.

- **Bastionado de servidores (alojados tanto en los CPD como en *cloud*)**

Con objeto de dotar de una mayor seguridad a los diferentes servidores (tanto físicos como virtuales) que sustentan los servicios y procesos de negocio de Azkoyen, se llevó cabo el *hardening* o bastionado de sus servidores principales (es una tarea que se sigue llevando a cabo bajo demanda, según se van desplegando nuevos). Con esto se busca:

- ✓ Aplicar las configuraciones necesarias para protegerse de posibles ataques físicos o de *hardware* de la máquina (deshabilitando periféricos, dispositivos USB, restringiendo arranque en BIOS, protección con contraseña, etc.).
- ✓ Instalación segura del sistema operativo.
- ✓ Activación y/o configuración adecuada de servicios de actualizaciones automáticas.

- ✓ Instalación, configuración y mantenimiento de programas de seguridad y correcta aplicación de parches de seguridad.
- ✓ Configuración de la política local del sistema, política robusta de contraseñas, gestión de privilegios, restricciones de *software*, activación de auditoría de sistema, restricción y configuración adecuada de protocolos de red, configuración segura de los accesos remotos, cuentas de usuario, cifrado, etc.
- ✓ Etc.

Para ello, se han empleado las guías de los distintos fabricantes, y como patrón general las guías STIC publicadas por CCN-CERT para la protección de distintos entornos.

- **Seguridad en el correo electrónico**

Los dominios de Azkoyen se encuentran protegidos por el servicio de correo electrónico seguro de **Secure&IT**. Este servicio permite disponer de seguridad consolidada para el correo electrónico, protección contra los virus y *spam*. Pero, también identifica y neutraliza amenazas específicas, como los ataques avanzados de *phising*. Está dotado de una *sandbox*, de última generación, que analiza los ficheros antes de que lleguen a sus infraestructuras, permitiendo un elevado nivel de protección contra amenazas desconocidas y *zero-days*.

- **BigProbe® y monitorización de servidores**

Para completar la monitorización avanzada de amenazas de seguridad, Azkoyen tienen instalado en su centro de datos una sonda BigProbe®, desarrollada por **Secure&IT.** Está basada en código abierto y es capaz de detectar todo tipo de ataques, tanto verticales como horizontales. La sonda trabaja mediante la comparación del tráfico analizado con más de 150 fuentes de información (*feeds* de inteligencia) que **Secure&IT** gestiona y carga diariamente.

También se encuentran monitorizados los principales servidores de Azkoyen. Se recogen los diferentes eventos que generan y se focalizan las alertas en el entorno de la seguridad, como el control de acceso, el comportamiento del usuario o los administradores del sistema y la integridad de los ficheros.

- **Seguridad Cloud**

Se ha llevado a cabo la protección del entorno *cloud* Azure de Azkoyen, mediante la instalación de un *cluster* de *firewalls* que incluyen: 24x7 FortiCare plus Application Control, IPS, AV y FortiSandbox Cloud.

- **Seguridad IoT**

En la creación de nuevos productos es fundamental aplicar la seguridad desde el diseño. Es decir, incorporar la seguridad en las fases más tempranas del desarrollo. Con este objetivo, **Secure&IT** ofrece soporte al departamento de desarrollo de Azkoyen. De esta forma, sus productos nacen teniendo siempre presentes los pilares de la ciberseguridad (confidencialidad, integridad, disponibilidad y autenticación).

Además, se lleva a cabo una auditoría de los sistemas antes de sacarlos al mercado.

- **Seguridad gestionada desde el SOC-CERT de Secure&IT/SIEM**

La necesidad de gestionar, administrar y contar con alertas tempranas de eventos de seguridad, llevó a la integración de Azkoyen en el Centro de Operaciones de Seguridad **Secure&View®** de **Secure&IT.** Aquí se realizan las diferentes tareas propias de un SOC-CERT y equipo de respuesta rápida ante eventos de seguridad:

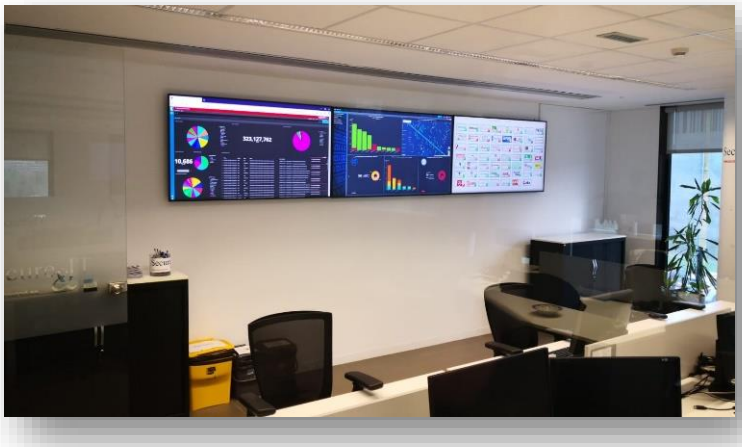
- ✓ Monitorización y supervisión de los sistemas en tiempo real, 24 horas al día, los 365 días del año.
- ✓ Soporte 24x7 los 365 días del año.
- ✓ Log Management.
- ✓ SIEM: recolección y correlación de todos los logs de la infraestructura de Azkoyen.
- ✓ Generación de alarmas ante eventos de seguridad 24x7.
- ✓ Supervisión reactiva y activa de los sistemas de Azkoyen para garantizar la seguridad de la información.

Como se expone, dentro del servicio se incluye: la monitorización de seguridad, la gestión de incidentes de seguridad, el análisis forense de seguridad y la gestión de vulnerabilidades y logs.

CASO DE ÉXITO

El núcleo del sistema de correlación de eventos de seguridad se lleva a cabo a través de una solución SIEM (*Security Information and Event Management*), que ha sido desarrollada y evolucionada a lo largo de los años, y de forma íntegra, por **Secure&IT**. BigSIEM®, combina las funciones de SIM (*Security Information Management)* y SEM (*Security Event Management*) en un único sistema de seguridad.

El servicio se presta 24x7x365 en nuestros centros de seguridad, ubicados en Madrid y Arrasate-Mondragon (Euskadi). Contamos con un equipo de varios tipos de analistas especializados (seguridad defensiva, seguridad ofensiva, analistas de seguridad y respuesta ante incidentes), que gestionan la seguridad de los sistemas y monitorizan de forma constante las alertas y las amenazas que se reciben desde los distintos elementos de seguridad.



- **Protección de datos y Derecho TIC**

En la actualidad, en el plano jurídico y de consultoría, se está llevando a cabo:

- Mantenimiento de las obligaciones que en materia de protección de datos tiene el Grupo Azkoyen, lo que incluye todas las empresas a nivel internacional y su correspondiente normativa (Italia, Portugal, etc.). Este servicio de mantenimiento implica:

    - ✓ la inscripción, modificación o, en su caso, supresión de los ficheros responsabilidad del Grupo.
    - ✓ la realización de las auditorías en materia de protección de datos.
    - ✓ la actualización de los Documentos de Seguridad y registros correspondientes.
    - ✓ la revisión continúa del cumplimiento de las medidas de seguridad reflejadas en los Documentos de Seguridad.
    - ✓ la redacción y revisión de clausulado o contratos en materia de protección de datos.
    - ✓ la actualización de los procedimientos del Grupo Azkoyen a la nueva normativa sobre protección de datos.
    - ✓ atención al ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando se producen.

- Mantenimiento en Derecho TIC, que consiste en un servicio libre y a demanda que comprende:

    - ✓ la revisión de contratos informáticos o redacción de contratos con sus principales proveedores de IT.
    - ✓ la redacción de condiciones de uso o contratos para sus clientes.
    - ✓ la revisión del clausulado preceptivo y políticas de privacidad correspondientes de todas las páginas web pertenecientes al Grupo Azkoyen.
    - ✓ informar sobre las novedades normativas que puedan afectar al Grupo en materia de seguridad de la información.

- Delegado de Protección de Datos

Dentro de los servicios que **Secure&IT** presta a Azkoyen, se encuentra el de la figura del Delegado de Protección de Datos, que da soporte a todas las sedes del grupo.

El Reglamento General de Protección de Datos (RGPD), que sustituye a la Directiva de 1995, incluyó la figura del Delegado de Protección de Datos (DPD o DPO por las siglas en inglés de *Data Protection Officer*). El DPD se hace cargo de:

- ✓ Informar y asesorar a los empleados de cuáles son las obligaciones que establece la normativa.
- ✓ Monitorizar los procedimientos establecidos en la organización, certificando que se adaptan a la normativa sobre protección de datos.
- ✓ Cooperar con las autoridades nacionales de protección de datos.

Es necesario apuntar que las actividades de esta figura, reguladas en el RGPD, se llevan a cabo por personal de **Secure&IT** diferente al que realiza el mantenimiento de Azkoyen y, a su vez, diferente al que lleva a cabo las auditorías.

- **Implantación y mantenimiento ISO 27001:2013**

Se han establecido procesos corporativos de gestión de la seguridad de la información, que permiten a Azkoyen trabajar bajo un marco de gobierno IT, basado principalmente en la reducción de riesgos y en la gestión de la seguridad de la información. En este sentido, se ha implantado y se mantiene el estándar ISO 27001:2013.

- **Concienciación en seguridad a todos los empleados de la empresa**

Las personas representan el eslabón más débil de la cadena de ciberseguridad. Por este motivo, semanalmente y con el objetivo de concienciar y formar a los usuarios de Azkoyen, se envían consejos de seguridad, que recogen alertas y aspectos técnicos y legales. Además, periódicamente, los trabajadores reciben un examen tipo test que trata de evaluar los conocimientos en seguridad de la información que han adquirido.

Adicionalmente, se han impartido cursos de ciberseguridad, Derecho TIC y procesos de seguridad.

Todo ello ha permitido a Azkoyen **obtener el sello "GOLD SECURITY"** de **Secure&IT**, esquema bajo el que, como hemos explicado al principio, se enmarca el servicio de **Secure&IT** de gestión integral de la seguridad.

A pesar de los proyectos realizados, aún queda mucho por hacer. En una empresa como Grupo Azkoyen los activos de información son muy importantes; le permiten ser líder del mercado, una posición que no puede ceder. Sus competidores nacionales e internacionales lo saben y muchos de ellos han tomado a Azkoyen como modelo a seguir y a imitar.

Esto supone una amenaza creciente, llevada a cabo por ciberdelincuentes que emplean técnicas imaginativas que incluyen aspectos tecnológicos, pero, también, de ingeniería social. Los cibercriminales aprovechan cada vez más las brechas en los procesos internos de la compañía, buscando el hueco por el que entrar.

Por este motivo, Azkoyen y **Secure&IT** seguirán trabajando en la identificación y mejora de los procesos de seguridad de la empresa, acompañando su cumplimiento con la tecnología más adaptada al entorno, con el objetivo de garantizar la continuidad de negocio y el liderazgo de Azkoyen en el mercado.