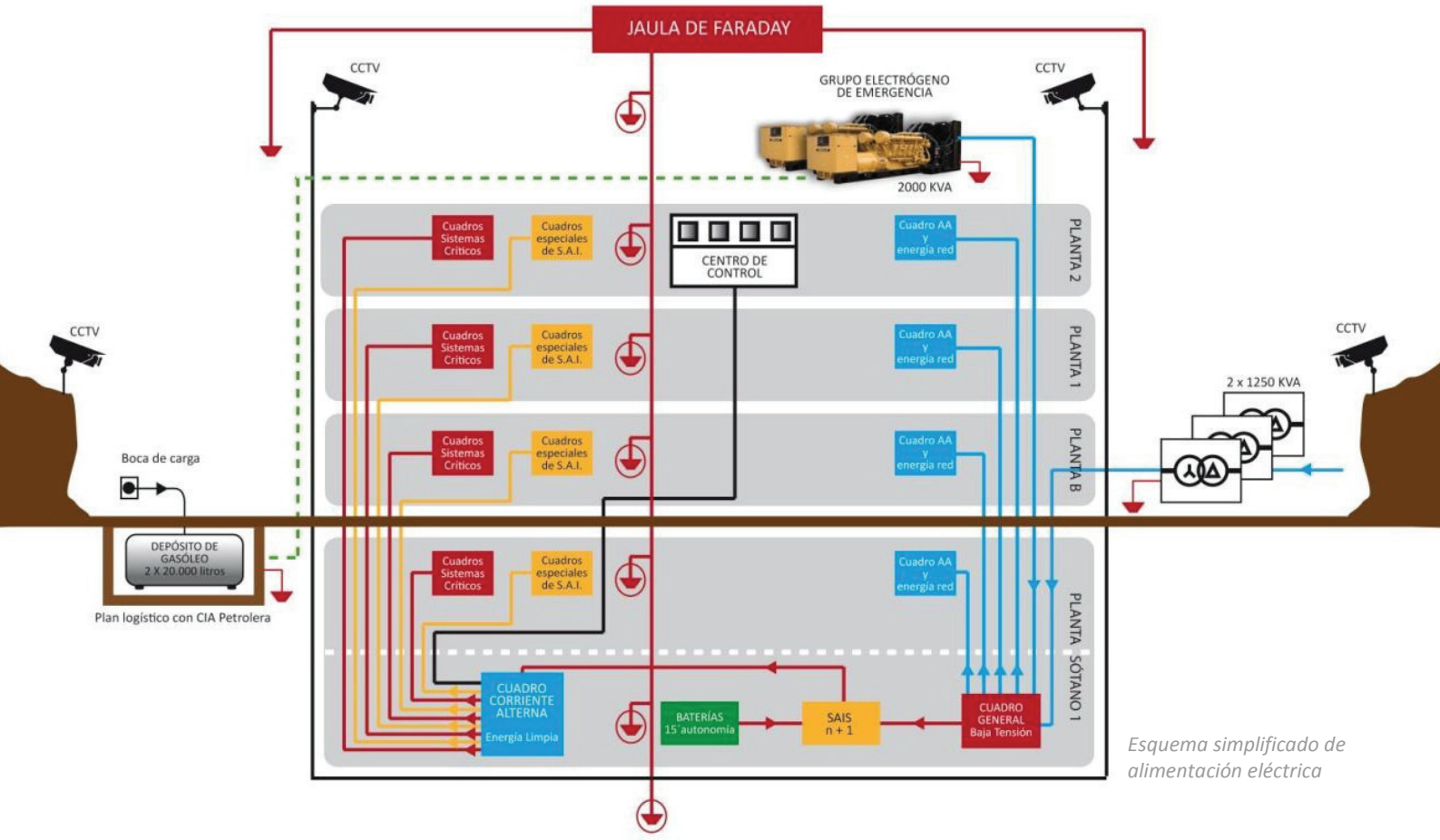
Alimentación eléctrica



Esquema simplificado de alimentación eléctrica

Transformación

Los centros de transformación se ubican en el jardín exterior del edificio. Transforman la alta tensión a 36 kV en trifásica a 400 V y está compuesto por los siguientes elementos:

- Centro de datos conectado al anillo de la compañía eléctrica.
- 3 centros de transformación compuestos de 2 transformadores de 1.250 kVA cada uno (N+1)
- las cabinas de hormigón en donde se instalan los transformadores de acuerdo a la normativa actual, es del tipo prefabricado.
- todos los elementos de protección contraincendios adecuados.
- 2 SAI's para el sistema 1 de 600 kVA cada unidad (N+1)
- 2 SAI's de 300 kVA cada unidad para el sistema 2
- Dos generadores diesel con potencias de 2.000 y 2.250 kVA, con depósitos de gasoil de 1.000 litros.
- 2 depósitos nodriza de gasoil de 20.000 litros con dos bombas de trasiego automáticas.
- Posibilidad de acoplar grupos externos a la instalación.

Asimismo y para poder corregir el coseno de phi de la instalación, se incorpora una batería de condensadores de la potencia adecuada a tal fin.

SAI

El sistema de alimentación ininterrumpida (SAI) tiene como principales características las siguientes:

1. Se compone de unidades de 600 kVA en clúster y con grado de redundancia de n+1. El sistema incorpora por seguridad en su funcionamiento:
    - by-pass estático.
    - by-pass exterior.

Como elemento complementario de seguridad se ha incluido en cada planta un **módulo de transferencia automática de cargas** (STS), que permite, en todo momento, disponer de dos alimentaciones y una salida, siendo por consiguiente (y sin corte de tensión para la alimentación de los racks) un sistema de by-pass o emergencia total que permite mantener el servicio en situaciones extremas.

2. Las siguientes características describen la avanzada tecnología utilizada por los sistemas SAI que se instalan en el edificio:
    - rectificador de 12 pulsos (baja producción de armónicos = 3,5%).
    - inversor transistorizado (IGBT) regulado por modulación de ancho de impulso (PWM).
    - control por microprocesador.
    - sistema de comunicaciones.
    - fabricante: LIEBERT.

3. Las **baterías** que alimentan el sistema son del tipo Plomo Hermético sin mantenimiento y recombinación de gases (10/12 años de vida media). Estas baterías son capaces de dar una autonomía al 100% de carga del inversor durante un mínimo de 15 minutos.

Generación

Complementando los SAI, se instala el **grupo electrógeno** situado en la cubierta del edificio. La potencia individual del generador es de 2.000 kVA. La **autonomía mínima** es de **72 horas a plena carga** y el tiempo de entrada en servicio a régimen nominal inferior a 15 segundos.

El conjunto de la instalación se monta en una cabina metálica insonorizada y totalmente equipada para el uso a que se destina. En esta cabina se incluyen todos los elementos de control del sistema tales como cuadro eléctrico de control, elementos de ventilación de sala, escape de humos y, sobre todo, el sistema de gasóleo (depósito de 3.000 litros). En la zona anterior del edificio se ubica un depósito general subterráneo de 25.000 litros.

El sistema de regulación de la velocidad del motor es electrónico, con reparto de carga. El sistema de refrigeración es por radiador instalado en bancada. Los grupos incorporan la electrónica basada en microprocesadores del tipo NP2-2 a SEG. Asimismo, y para facilitar las labores de mantenimiento, la planta incluye un sistema de control formado por un PLC, integrado por los siguientes elementos:

- unidades centrales CPU con dos puertos de comunicaciones.
- procesadores con puerto adicional.
- adaptadores de comunicaciones.
- modulo de entradas digitales a 24 Vcc.
- módulo de salidas digitales a 24 Vcc.
- módulo de entrada y salidas analógicas, etc.

Los diferentes parámetros de funcionamiento del PLC se visualizan y controlan a través de un terminal gráfico de operador con pantalla táctil.

Conmutación inteligente de carga

El edificio está dotado de un **sistema inteligente de transferencias de cargas** en función del funcionamiento con red o grupos, sin interrupción del suministro en ningún caso.

Suministro eléctrico en salas de equipos

El suministro eléctrico en las salas de equipos incluye los siguientes elementos avanzados:

- **cuadro eléctrico con protecciones selectivas** (incluyendo magnetotérmico y diferencial por circuito).
- circuitos de energía a racks con **sistemas redundantes** (doble alimentación).
- circuito de red comercial (energía sucia) en perímetro de sala para servicios auxiliares y pruebas.
- alimentación a racks de forma aérea para evitar interferencias con los cruces de voz y datos y permitir una máxima flexibilidad en la distribución de los servicios de voz, datos y electricidad.

Aire acondicionado

Se dispone de un sistema **de Unidades Autónomas de Precisión en cada planta** (para equipos electrónicos) y de confort para la zona de oficinas.

El grado de redundancia es de **n+1** por planta y zona y las tolerancias de temperatura y humedad son las siguientes:

- tolerancia de temperatura: **22º ± 2ºC** (ajustable).
- tolerancia de **humedad relativa 50 ± 5%** (ajustable).

Detección y extinción de incendios

La configuración básica del sistema de detección de incendios incluye:

- un sistema descentralizado por plantas.
- el control y gestión de alarmas centralizado en el Centro de Operaciones.

De este modo, en cada planta existen **detectores de humos** en ambiente y un sistema independiente de detección precoz por aspiración, todo ello complementado con indicadores acústicos y pulsadores de alarma.

Tan importante como la detección es la rápida **extinción** de un posible incendio. Para ello se dispone de **sistemas automáticos y manuales**:

- automático, mediante inundación por agente de baja toxicidad y nulo impacto ambiental (argón), así como extinción por agua en otras zonas.
- manual, mediante extintores portátiles (CO^2/polvo químico).

Suelo técnico

El suelo técnico elevado permite una altura libre sobre el suelo de **45 cm**. Soporta **hasta 1.500 kg/m² de carga** con las columnas de apoyo conectadas a tierra en toda su extensión y ofreciendo características **antiestáticas**.

Seguridad, control de acceso y vigilancia

Los sistemas de seguridad, control de acceso y vigilancia siguen los estándares más estrictos, incluyendo:

- control de accesos mediante sistema electrónico con tarjetas de proximidad y, adicionalmente, **sistemas biométricos** en las zonas de acceso a las áreas de co-location.
- control de presencia e intrusión.
- control de apertura de puertas.
- sistema de circuito cerrado de TV (color).
- sistema digital de videograbación (30 días).
- servicio de **vigilancia física** permanente y control de acceso (las **24 horas** del día).
- sistemas de intercomunicación distribuidos por el edificio, conectados con el puesto de seguridad y control.
- megafonía a todas las zonas del edificio.

Building management system

El **sistema de gestión del edificio (BMS)** centraliza todos los datos sobre la situación y el estado de la infraestructura del edifico y recibe y procesa posibles alarmas.

Los sistemas principales conectados y gestionados por el BMS son:

- centro de Seccionamiento.
- centro de Transformación.
- grupos electrógenos.
- sistemas de Alimentación Ininterrumpida.
- cuadros eléctricos principales de media y baja tensión.
- distribución eléctrica.
- sistemas de climatización.
- detección y extinción de incendios.
- detección de humedad.
- apertura de puertas.

La consola central del BMS será accesible tanto desde la central de seguridad como desde el centro de operaciones y será atendida 24 horas al día y 7 días a la semana.

Mantenimiento edificio

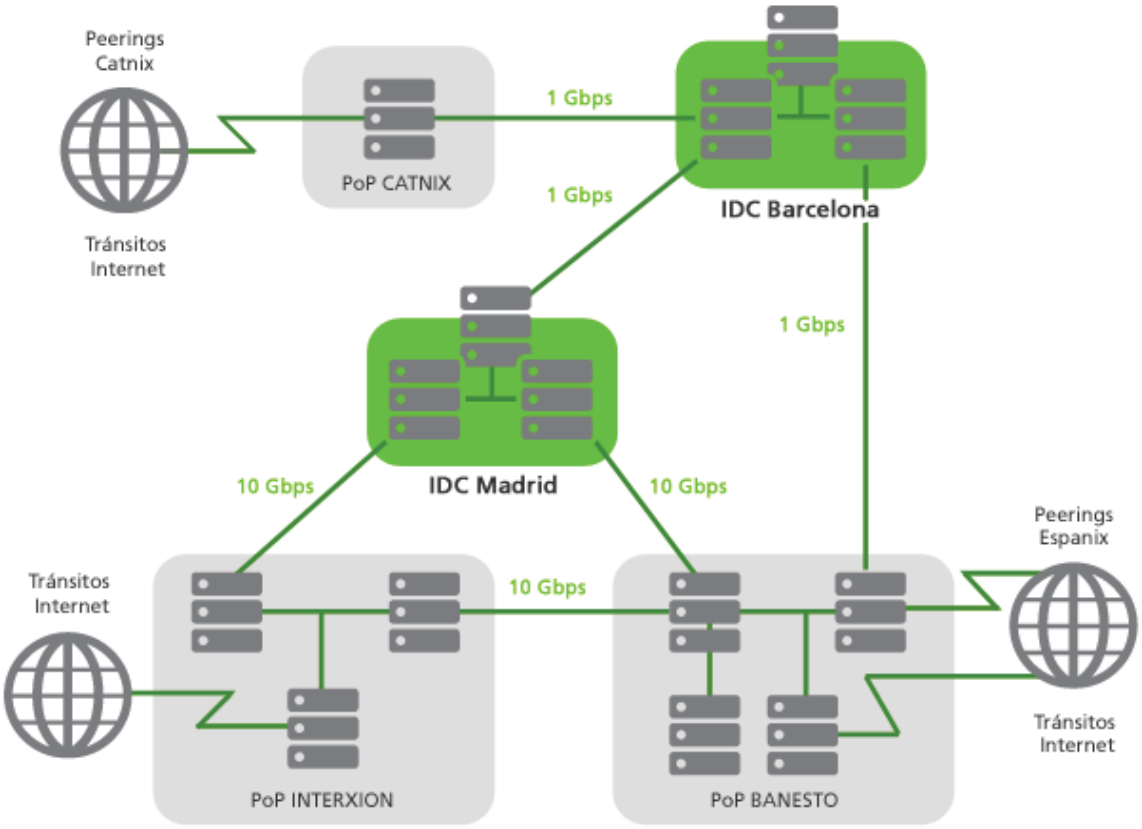
Todos los sistemas críticos de la infraestructura técnica del edificio disponen de un plan de mantenimiento preventivo y reactivo. Se realizan tareas preventivas para evitar, en lo posible, situaciones de deterioro de componentes. Para ello se dispone de un stock de repuestos clave y fungibles on-site en los almacenes del edificio.

Para casos de incidencias existe un plan de mantenimiento 24x7 para todos los componentes críticos de la infraestructura del edificio. Este plan será atendido tanto por personal propio, presente en las instalaciones del edificio, como mediante contratos de mantenimiento correspondientes a los fabricantes y suministradores de los diferentes sistemas.

Infraestructura de red

La red troncal de Aryan es una red multiservicio, basada en las más novedosas tecnologías, que incorpora los protocolos IP Multicast, BGP4 y MPLS. La operación y gestión de la red es realizada por Aryan extremo a extremo, ofreciendo al cliente las máximas garantías de nivel de servicio acorde a sus necesidades.

El acceso de la plataforma a Internet se realiza mediante múltiples conexiones con otras redes IP en puntos de intercambio y carriers de tránsito. Gracias al protocolo BGP4 se asegura un encaminamiento eficiente del tráfico IP y reacciones dinámicas a cualquier cambio que se produzca en la red Internet.



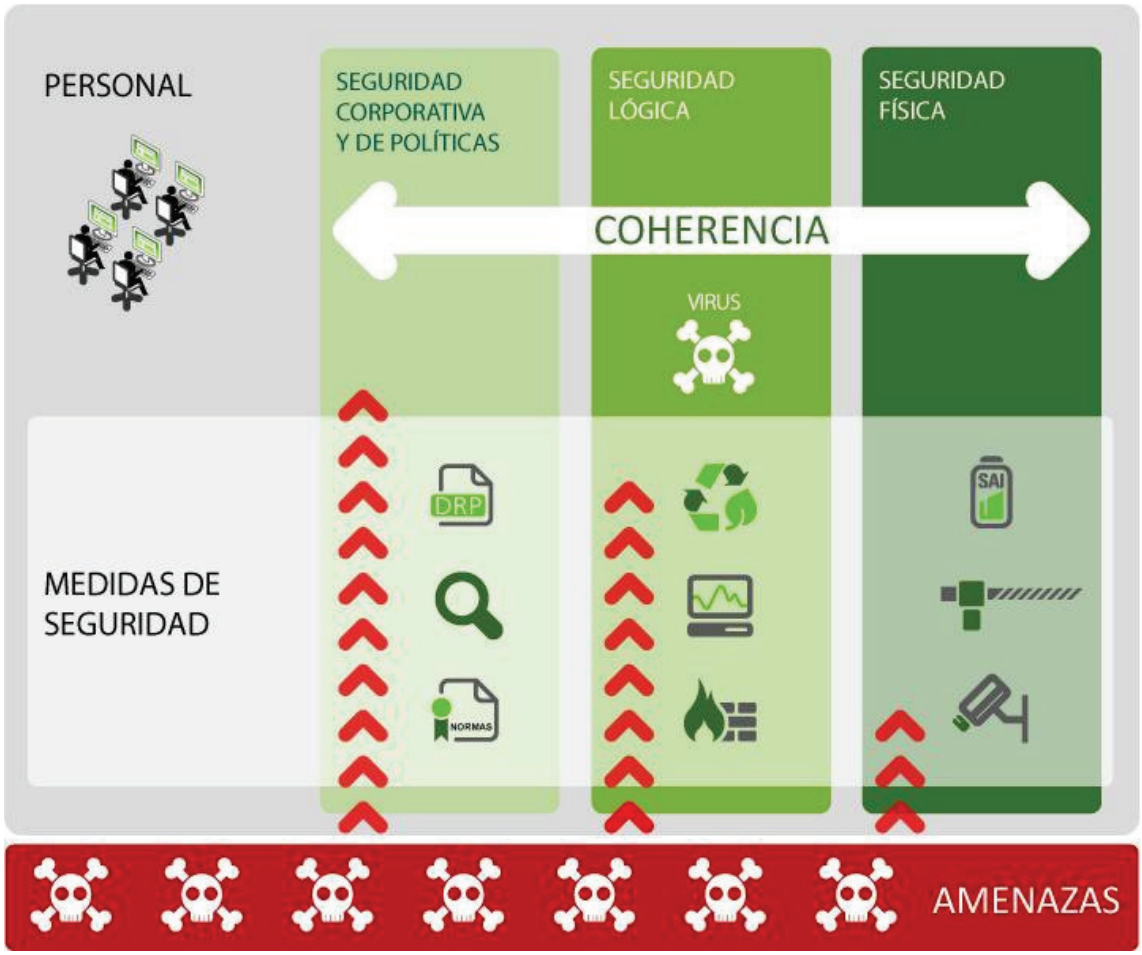
ARQUITECTURA SEGURIDAD

Introducción

En la arquitectura de seguridad existen tres áreas diferenciadas:

- **Seguridad física:** Comprendiendo la seguridad de los sistemas hardware, soportes, dependencias y demás entidades "tangibles" del entorno de prestación de servicios de Aryan.
- **Seguridad lógica:** Incluyendo los aspectos de protección aportados por aplicaciones, protocolos y procesos que intervienen en el sistema de Aryan.
- **Seguridad político-corporativa:** Formada por los aspectos de seguridad relativos a política general de la organización, normas, procedimientos y convenciones internas aplicables.

Dichas áreas están interrelacionadas, y la existencia coherente de medidas de seguridad en cada una ellas garantiza el nivel de protección óptimo frente a las posibles amenazas de seguridad.



Modelo de seguridad

Características de seguridad comunes

1. Seguridad física

El edificio en el que se alberga la infraestructura para prestar los servicios al cliente, se han implementado las siguientes medidas de seguridad física:

- Puesto de seguridad y control, con vigilantes en horario continuo 24x7.
- Autenticación y Control de Accesos:
  - Control de acceso al edificio mediante tarjeta de proximidad
  - Control de acceso a centros de proceso de datos basado en combinación de identificación biométrica por reconocimiento de geometría de mano y posesión de tarjeta de proximidad
  - Punto de control y gestión de alarmas
- Circuito cerrado de televisión con grabación digital permanente y detección de actividad en las cámaras distribuidas por todo el edificio y su perímetro.
- Alimentación redundante, dotando de dos líneas de alimentación eléctrica a los racks destinados a albergar los equipos.
- Sistemas de alimentación ininterrumpida.
- Grupo electrógeno para casos de corte eléctrico continuado con autonomía mínima de 3 días y contrato de suministro de gasoil en un plazo máximo de 24h
- Detección de incendios, basado en sistema combinado de detectores de humo y aspiración.
- Extinción de incendios, con sistemas automáticos mediante inundación por agente de baja toxicidad y nulo impacto ambiental y sistemas manuales con extintores portátiles.
- Sistemas de intercomunicación (interfonía) distribuidos por el edificio con comunicación con el

puesto de seguridad y control.
- Megafonía a todas las zonas del edificio.
- Climatización continua y adecuada de las zonas CPD con redundancia n+1 en cada zona.
- Aislamiento galvánico.
- Red equipotencial de tierra en todo el edificio y todas las instalaciones de los CPD
- Jaula de Faraday para el edificio de CPD
- Sala acorazada con armario ignífugo para almacenamiento de soportes magnéticos según norma S120DIS (Resistencia al fuego 2 horas).

2. Seguridad lógica

En lo referente a la seguridad de las comunicaciones y al software se emplean las siguientes medidas de protección:

Protección local

Los equipos instalados disponen de las versiones más estables de los sistemas operativos, con correcciones a múltiples bugs de seguridad. Aryan actualiza el software de forma periódica y aplica los parches correspondientes que solucionan los problemas de seguridad que surjan.

Protección perimetral

Todos los equipos cuentan con las siguientes medidas de protección comunes, mediante el filtrado y análisis de paquetes en los equipos de interconexión externos:

- Filtros para evitar ataques basados en spoofing
- Filtros para evitar ataques basados en smurfing

Detección y prevención de intrusos (IDS e IPS)

Aryan cuenta con equipos dedicados a la detección y prevención de intrusiones en red. Estos equipos envían sus alertas al sistema de gestión centralizada para su inspección y análisis por personal cualificado.

Estos dispositivos IDS/IPS poseen las siguientes características:

- **Detección de anomalías por análisis del protocolo:** alertando sobre los paquetes de red que violan el protocolo estándar de comunicaciones, posiblemente para provocar un mal funcionamiento en los equipos a los que se destinan.

- **Detección y/o bloqueo de conexiones por firmas (signatures)**: alertando sobre paquetes de red que contienen ciertos patrones asociados a ataques conocidos contra sistemas y aplicaciones. Bloqueo automático de los ataques que claramente son identificados como tales.

- **Detección de aumento de paquetes de red de diferentes tipos basándose en umbrales o thresholds:** Alertando sobre aumentos significativos de los diferentes tipos de paquetes de red que superan cierto umbral definido.

- **Detección de desviación estadística de patrones de tráfico:** alertando de los aumentos significativos de tipos de paquetes TCP/IP en comparación con el patrón de tráfico habitual de la red.

La política configurada bloquea los paquetes de red que forman parte de ataques claros, y emite alertas ante actividades sospechosas o fuera de lo normal.

Las firmas y patrones de intrusiones se actualizan periódicamente para detectar y/o bloquear en el menor tiempo posible los nuevos tipos de ataques que pudieran aparecer.

- **Alta disponibilidad de líneas de salida**

  La comunicación exterior se compone de varias líneas de comunicación con diferentes proveedores, para garantizar la continuidad del servicio en caso de fallo de uno de ellos. Para ello, Aryan recibe y comunica la información de encaminamiento vía el protocolo BGP4.
  Se emplean routers físicamente distintos para garantizar la disponibilidad permanente de los enlaces con Internet y otros operadores.

Monitorización y control

Centro de operaciones (NOC) equipado con videowall (pantalla gigante) donde se recogen todas las alarmas de seguridad y mal funcionamiento.

Vigilancia de disponibilidad de servicios y comunicación en horario 7x24.

Seguridad político corporativa

En lo referente a gestión y aplicación de la política de seguridad, se garantiza su cumplimiento mediante el empleo de las siguientes técnicas:

- **Normas y procedimientos de administración**

  Los administradores / operadores cumplen una serie de normas y procedimientos elaborados para garantizar la correcta utilización de los sistemas informáticos y la información que estos albergan.

- **Formación y difusión del plan de seguridad**

  Los operadores son instruidos regularmente en materia de seguridad en aquellos aspectos que tienen que ver con sus labores diarias (operación, administración, etc.).

- **Seguros**

  Existen seguros que incluyen cobertura en caso de desastre y de daños ocasionados por actividades electrónicas.

- **Auditoría**

  Se efectúan auditorías periódicas realizadas por personal interno y por terceros independientes sobre la infraestructura tecnológica propia y el entorno de seguridad física, para garantizar que el nivel de robustez frente a ataques es el adecuado. Adicionalmente, se efectúan las revisiones pertinentes para comprobar el correcto cumplimiento de los procedimientos de seguridad por parte del personal.

DESCRIPCIÓN DE LA SOLUCIÓN TÉCNICA

Infraestructura

La plataforma de hardware y software se beneficia de los siguientes servicios:

Máximas medidas de seguridad: La seguridad del Data Center ha sido uno de los requisitos principales desde su diseño inicial. A los métodos convencionales de detectores de presencia, proximidad e incluso circuito cerrado de televisión, se han añadido sensores biométricos de acceso y control. Únicamente el personal autorizado dispone de acceso a los equipos.

En cuanto a los medios físicos de seguridad, los Data Centers disponen de los sistemas más modernos de protección contraincendios, extinción por agentes de nulo impacto ambiental y sistemas de detección de fugas de agua o combustible. Todo ello telegestionado por un sistema central de control y gestión del edificio.

Alimentación eléctrica redundante soportada con SAIs y grupos electrógenos: En el diseño de las instalaciones eléctricas se ha contemplado un grado de redundancia de equipos, añadiéndole una serie de elementos alternativos tales como sistemas de by- pass, transferencias de cargas criticas sin cortes de tensión, aislamiento galvánico, red equipotencial de tierra, etc., que permiten asegurar un nivel de disponibilidad eléctrica muy elevado para los equipos alojados.

Climatización controlada: El sistema de climatización se ha conseguido mediante equipos autónomos que aseguran unos niveles de temperatura y humedad óptimos para el funcionamiento de los servidores.

Monitorización y vigilancia permanente 24x7x365: El sistema de gestión del edificio (BMS) centraliza todos los datos sobre la situación y el estado de la infraestructura del edifico y recibe y procesa posibles alarmas. Los sistemas principales conectados y gestionados por el BMS son: el Centro de Transformación, los grupos electrógenos, los sistemas de Alimentación Ininterrumpida, los cuadros eléctricos principales de media y baja tensión, la distribución eléctrica, los sistemas de climatización, la detección y extinción de incendios, la detección de humedad y la apertura de puertas.

Conectividad

La conectividad con el servicia está fijada en 100MB. La infraestructura quedará conectada de manera directa a Internet mediante circuitos de alta capacidad redundantes, asegurando así alta disponibilidad y calidad de acceso.

La red troncal es una red multiservicio, basada en las más novedosas tecnologías, que incorpora los protocolos IP Multicast, BGP4 y MPLS. La operación y gestión de la red es realizada por Aryan de extremo a extremo, ofreciendo al cliente las máximas garantías de nivel de servicio acorde a sus necesidades.

El acceso de la plataforma a Internet se realiza mediante múltiples conexiones con otras redes IP en puntos de intercambio y carriers de tránsito. Gracias al protocolo BGP4 se asegura un encaminamiento eficiente del tráfico IP y reacciones dinámicas a cualquier cambio que se produzca en la red Internet.

Seguridad Lógica

Para garantizar la protección lógica de la plataforma ofertada se incluye en la propuesta el servicio de firewall compartido básico. Este servicio, implantado sobre una plataforma redundante gestionada, permite la definición personalizada de 5 reglas de seguridad en sentido entrante y el uso de un Ancho de Banda de 1 Mbps en "percentil 95".

Para garantizar la protección lógica de la plataforma ofertada se incluye en la propuesta el servicio de firewall compartido avanzado. Este servicio, implantado sobre una plataforma redundante gestionada, permite la definición personalizada de 30 reglas de seguridad y el uso de un Ancho de Banda de 1 Mbps en "percentil 95".

La protección proporcionada también incluye la detección y el bloqueo de diversos tipos de ataques:

- Intentos de localización e inspección de servidores y servicios abiertos
    - Barridos de puertos TCP
    - Barridos mediante ICMP
- Ataques de denegación de servicio (Denial Of Service - DOS) por vulnerabilidades del S.O.:
    - SYN Flooding
    - ICMP Flooding
    - UDP Flooding
- Ataques

○ Ping de la muerte ○ Ataque Tear Drop ○ Ataque WinNuke ○ Ataque Land

- Envío de paquetes IP incorrectos o malformados:
    - Paquetes con opción Source Route
    - Spoofing de IP
    - Paquetes IP con opciones/flags incorrectas
    - Paquetes IP con opciones/flags inseguras

- Número de conexiones excesivas desde un origen
    - Límite de sesiones TCP, UDP e ICMP
- Ataque a vulnerabilidades de servicios:
    - URL's maliciosas
    - Ataques de "buffer-overflow"
    - Vulnerabilidades particulares de los diferentes servicios

Aryan cuenta también con equipos dedicados a la detección y prevención de intrusiones en red IDS/IPS en sus centros de alojamiento de servidores. Estos equipos envían sus alertas al sistema de gestión centralizada para su inspección y análisis por personal cualificado.

Servicios de monitorización

Los servidores dedicados disponen de una monitorización constante de los equipos y puertos que el cliente desee desde el Centro de Control. El C.O.R.S. (Centro de Operaciones, Redes y Sistemas) emplea dos herramientas para la gestión y supervisión de la plataforma.