UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

SECURIZACIÓN DE UN CENTRO DE GESTIÓN DE TRANSPORTE PÚBLICO.

Ivan Ferrer Montilla

Tutor: Manuel Esteve Domingo

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2020-2021

Valencia, 9 de noviembre de 2020

Escuela Técnica Superior de Ingeniería de Telecomunicación
Universitat Politècnica de València
Edificio 4D. Camino de Vera, s/n, 46022 Valencia
Tel. +34 96 387 71 90, ext. 77190
www.etsit.upv.es

VLC/ CAMPUS VALENCIA, INTERNATIONAL CAMPUS OF EXCELLENCE

EMAS Gestión ambiental verificada REG.NO. ES-CV- 000030

Resumen

El proyecto trata el diseño de la seguridad de un centro de control de transporte público el cual monitoriza las diferentes alertas relativas al transporte público y contiene unos servidores en el que se ejecutaran las aplicaciones necesarias para el funcionamiento de dicho sistema.

Para saber a qué nos enfrentamos analizaremos el estado del ciberespacio para poder llevar a cabo correctamente la securización de la red de dicho centro de control, acto seguido veremos qué tipo de dispositivos existentes para la defensa de una red y analizaremos la red del centro de gestión, y adaptaremos la seguridad de cada sección de la red a sus necesidades.

Por otra parte, llevaremos a cabo el sistema de seguridad física del edificio, se tratarán tres aspectos de la seguridad, el control de acceso, la detección de intrusión y la videovigilancia, se llevará a cabo la explicación de la instalación de dichos dispositivos en las instalaciones del edificio.

Resum

El projecte tracta el disseny de la seguretat d'un centre de control de transport públic el que monitoritza les diferents alertes relatives al transport públic i conte els servidors en el que es trobaran les diferents aplicacions que son necessàries per al funcionament correcte del sistema.

Per a saber a que ens enfrontem primer analitzarem el estat del ciberespai per a poder portar a terme la correcta securització de la xarxa del centre de control, seguidament explicarem els analitzarem els diferents tipus de dispositius existents que es poden utilitzar per a la defensa d'una xarxa i analitzarem la xarxa del centre de gestió i adaptarem la seguretat de cada secció a les necessitats de la mateixa.

Per altra part, portarem a terme el sistema de seguretat física del edifici, es tractaran tres aspectes de dita seguretat, el control d'accés, la detecció d' intrusió y la videovigilància, es dura a terme la explicació del diferents dispositius en les instal·lacions del edifici.

Abstract

This project it's about the design of the security of a public transport control system, this system monitors any kind of alerts related to the public transport and contains the servers that grant the system the applications necessary to function correctly.

First we got to know what we are facing, for this we got to analyse the state of the cyberspace, then we will see the different kind of threats we are exposed to and then we will see what devices are best to fight said threats, then we will adequate the existent network of the centre to adapt to this security threats.

Secondly we will analyse the physical security of the building, we will cover three aspects of said security, access control, intrusion detection and video surveillance, and then we will analyse the differences on the building and adequate the devices to said differences.

Índice

Capítulo 1. Introducción.

1.1 Introducción a la normativa empleada para el proyecto.

1.1.1 ISO 27001

La norma ISO 27001 define uno de sus aspectos claves en la definición de un sistema de gestión de seguridad de la información (SGSI) el cual se encuentra en un ciclo continúo compuesto por cuatro fases que son Planificar-Hacer-Verificar-Actuar, la mayor parte del trabajo dentro de un diseño de una red de seguridad se encuentra dentro de la primera fase en la que se definirán los riesgos y se propondrán controles y autoridades dentro del sistema.

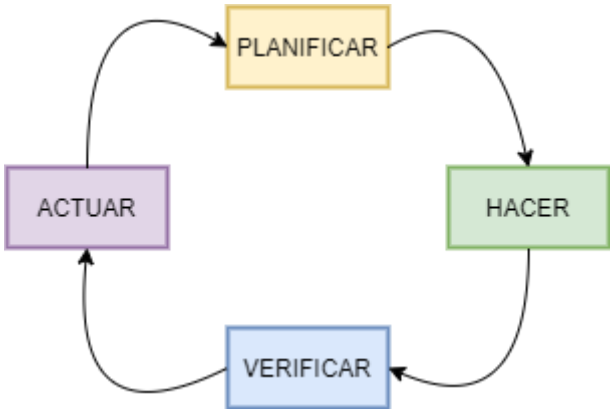

Figura 1. Ciclo PHVA ISO 27000

Las diferentes fases del ciclo se dividen a su vez en tareas más pequeñas las tareas de la primera fase serian:

- Analizar los activos disponibles de la organización y sus necesidades de seguridad.
- Analizar el impacto que tendría un ataque sobre estos activos.
- Evaluar las vulnerabilidades a la que se podrían enfrentar dichos activos, así como a las amenazas que se pueden encontrar.

La segunda tarea seria llevar a cabo las decisiones tomadas en la tarea de planificación. La tercera tarea sería una tarea de supervisión sobre el sistema implementado para tal y como indica su nombre verificar el correcto funcionamiento de esta misma y por último tendríamos la tarea que llevaría a actuar en posibles fallos que presente el sistema empezando así otra vez el ciclo.

1.1.2 Esquema nacional de seguridad

Este real decreto publicado 29 de enero de 2010 tiene por objeto fijar las medidas de seguridad que se deben aplicar a los dispositivos electrónicos utilizados en instalaciones públicas. Para ello en su artículo 4 define los diferentes principios que se deben tener en cuenta en este aspecto y establece unos requisitos mínimos que deberá cumplir una instalación dependiendo de su uso.

El ENS también determina los diferentes niveles de seguridad a los que tiene que adaptarse un sistema dependiendo de la importancia de este, identifica en total tres categorías, bajo, medio y alto, como en este caso la estructura del centro de control es crítica significa que debe de tener un nivel alto en la mayoría de los ámbitos.

El ENS se centra en tres sectores en concreto el marco operacional que trata de proteger la operación del sistema, el marco organizativo que trata las medidas relacionadas con la seguridad a nivel general y las medidas de protección que se encarga de tratar de proteger activos concretos según su naturaleza, en nuestro caso nos centraremos en los dos últimos sectores.

Los aspectos más importantes que trata ENS respecto al tema que nos atañe son los siguientes:

- Arquitectura de seguridad: Se plantearán ciertos aspectos de la seguridad como pueden ser los puntos de acceso, las áreas de tránsito para diferentes empleados o usuarios, las redes internas y su conexión con el exterior y las defensas de estas mismas. Cabe destacar el uso de diferentes tecnologías en las líneas de defensa para evitar las posibles vulnerabilidades que pueda presentar dicha tecnología y la redundancia de los sistemas para evitar fallos.
- Mecanismo de autenticación: Se definen diferentes niveles de seguridad dependiendo de que autenticadores se usen, por norma general lo menos seguro es una contraseña o código que se sepa, ya que estos pueden ser fácilmente conseguidos por terceros sin que el usuario se entere, por detrás de estos están las cosas que se tienen como pueden ser tarjetas u otro tipo de tokens estos pueden ser robados o copiados aunque es más fácil que el usuario sepa cuando se ha visto comprometido el dispositivo de autenticación y por ultimo tendríamos la biometría que estaríamos hablando que es casi imposible la suplantación sin el conocimiento del usuario.
- Medidas de protección de instalaciones e infraestructuras: Se definen los mecanismos que se tendrán que seguir para la protección de los activos, algunos ejemplos son la separación de áreas de equipamientos y el control de acceso a las mismas, a la vez que se identifica a las personas que usan el control de acceso.

1.1.3 UNE 50600-2-5

La UNE 50600-2-5 especifica la seguridad física que se tiene que aplicar a los centros de datos, más en concreto habla sobre la protección contra accesos no autorizados. Para hacer esto se definen 4 clases de acceso.

	Clase 1	Clase 2	Clase 3	Clase 4
Protección contra accesos no autorizados	Área publica o semipública.	Área accesible a todo el personal autorizado (empleados y visitantes)	Área restringida a empleados específicos y visitantes.	Área restringida a empleados específicos que deben identificarse para poder acceder

Tabla 1.Clases de acceso UNE-50600-2-5

Que un empleado tenga acceso a una zona de clase 4 no significa que tenga acceso a otras zonas, aunque estas zonas sean de clase 2, 3 o a otras zonas de clase 4.

Para aumentar la seguridad del sistema estas zonas se deberán de delimitar la mejor posible dependiendo de las funciones que se lleven a cabo en cada zona, así como maximizar el control en el cambio entre zonas con dispositivos de control de acceso y con videovigilancia.

1.1.4 UptimeInstitute Tier Standard.

Este estándar establece cuatro Tiers para la infraestructura de centros de datos, esta clasificación se lleva teniendo en cuenta la continuidad de la operación de los centros de datos.

Estas Tiers van aumentando en severidad, por tanto, cada una incluye las especificaciones de las anteriores, un resumen sobre los requerimientos para cada Tier son los siguientes.

	Tier I	Tier II	Tier III	Tier IV
Componentes	N	N+1	N+1	N Después de cualquier fallo
Encaminamiento	1	1	1 activo + 1 alternativo	2 activos al mismo tiempo
Mantenimiento continuo	No	No	Si	Si
Tolerante a fallos	No	No	No	Si
Compartimentalización	No	No	No	Si
Enfriamiento continuo.	No	No	No	Si

Tabla 2. Resumen Tiers de seguridad.

1.2 Modelo Cyber Kill Chain

Para reaccionar apropiadamente a posibles ataques se debe comprender como estos se llevan a cabo y que fases tienen, un modelo existente es el llamado Cyber Kill Chain en el que cada fase del ataque es un eslabón de una cadena siendo los primeros eslabones acciones poco dañinas y resultando finalmente en el secuestro completo del sistema, el objetivo de los sistemas de seguridad es el de "romper" dicha cadena siendo preferible romperla lo más pronto posible.

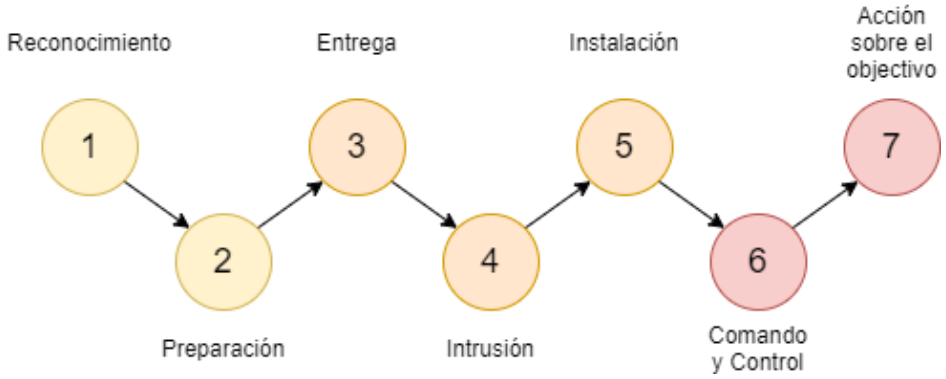

Figura 2. Modelo Cyber Kill Chain

Los diferentes "eslabones" que componen este modelo son los siguientes:

- Reconocimiento: El atacante busca, identifica y elige un objetivo, esto se puede hacer mediante información que el objetivo tenga en acceso abierto para el público o con por ejemplo un escaneo de puertos o con forzando mensajes de fallo para ver en que versión está corriendo el servidor.
- Preparación: El atacante prepara las diferentes herramientas que utilizara, como pueden ser archivos infectados u otro tipo de programa maligno.
- Entrega: El atacante introduce en la red objetivo las herramientas utilizadas, esto se puede hacer de muchas formas, aunque la forma más habitual es mediante el phishing o la llamada ingeniería social. Esta fase es la primera en la que las líneas de defensa instaladas pueden llevar a cabo la detección del ataque.
- Intrusión: La victima ejecuta el código dañino del atacante.
- Instalación: El código se instala en el sistema de la víctima abriendo una puerta trasera para el acceso del atacante al sistema.

- Comando y Control: El atacante toma el control del dispositivo infectado y a partir de este punto se empieza a propagar por la red.
- Acción sobre el objetivo: El ataque se completa llevando a cabo la acción por parte del atacante, esto puede variar desde el robo de información hasta la destrucción de esta o el secuestro de dicha información.

Por tanto, el ataque se suele dividir en diferentes fases:

- Fase de preparación que lo componen la fase de reconocimiento y preparación, fase en la que el sistema de defensa tradicional, por ejemplo, un firewall no suele actuar, pero que dispositivos más avanzados sí que pueden llevar a cabo el engaño del atacante respecto a las características del sistema.
- Fase del incidente que lo componen la fase de entrega, intrusión e instalación, siendo esta la fase más delicada en la que el sistema de seguridad debe detectar que se está llevando a cabo un ataque ya que una vez pasada esta fase el código dañino ya se encontraría dentro del sistema.
- Fase de intrusión activa que la componen la fase comando y control y la fase de acción sobre el objetivo, fase en la que el sistema ya se encuentra comprometido por lo que el código dañino ya podría estar expandiéndose por la red y es primordial pararlo lo antes posible.

Para frenar estos ataques existen diferentes acciones que pueden llevar a cabo el sistema de defensa estas acciones son:

- Detectar dicho ataque, esto es la primera línea de defensa a la hora de neutralizar un ataque por lo que se puede considerar la función más importante del sistema ya que es imposible neutralizar cualquier tipo de ataque si este no es detectado.
- Prevención del ataque esto consiste entre otras cosas en mantener el sistema actualizado para poder conocer que tipos de ataques se pueden llevar a cabo, así como llevar a cabo unas políticas de acceso bien implementadas.
- Disrupción consiste en dificultar la tarea al atacante mediante de esta forma el ataque puede ser menos efectivo o puede mejorar el tiempo de reacción del sistema, esto puede consistir en desplegar dispositivos trampa como son los honeypots o honeynets, o limitar el tiempo de las comunicaciones.
- Degradar consiste en debilitar la fuerza del ataque, esta acción se lleva a cabo una vez el ataque ya se ha efectuado, pero un sistema bien preparado se minimizan los daños que el ataque produce sobre el sistema.
- Engañar consiste en tal y como indica su nombre engañar al atacante sobre la estructura que tiene el sistema, de esta forma el ataque actuara sobre componentes no importantes del sistema.

1.3 SCADA.

Los SCADA (Supervisory Control and Data Acquisition) son sistemas de entorno industrial dedicados a la adquisición de datos provenientes de diferentes fuentes en tiempo real, el centro de control recibirá información de muchos sensores instalados a lo largo de la línea de transporte y llevar a cabo acciones respecto a los datos obtenidos de los sensores.

Este tipo de sistemas son muy vulnerables debido a su necesidad de conexión a sensores remotos, conexión para la cual se usan protocolos estándar que no aporta protección a los datos. Otro aspecto por el que son vulnerables es que al necesitar un funcionamiento continuo su actualización puede ser complicada.

Capítulo 2. Estado del arte

Mientras que la seguridad física no presenta las características de evolución continua, más allá del desarrollo de tecnologías para ayudar a la mejor detección que los dispositivos ya existentes.

El ciberespacio es un sistema en constante evolución, cada día aparecen nuevas vulnerabilidades y formas de combatir las mismas y con el continuo uso de tecnologías para ayudar al trabajo diario en tantos ámbitos hoy en día es imposible hablar de seguridad de una organización sin hablar antes de la ciberseguridad.

Para comprender la importancia de la ciberseguridad se debe antes conocer de qué ataques se puede ser víctima así de que daño producen estos mismos a la vez que conocer quienes producen dichos ataques para poder tener una mejor comprensión del ciberespacio así de a que nos enfrentamos.

2.1 Atacantes

Conocer la situación de los atacantes posibles a nuestro sistema es de vital importancia para poder saber que amenazas existen y que magnitud del ataque debemos esperar. A continuación, se puede ver un gráfico con el porcentaje de ataques que perpetua cada sector, se puede observar claramente que el cibercrimen perpetuo la mayor cantidad de los ataques.

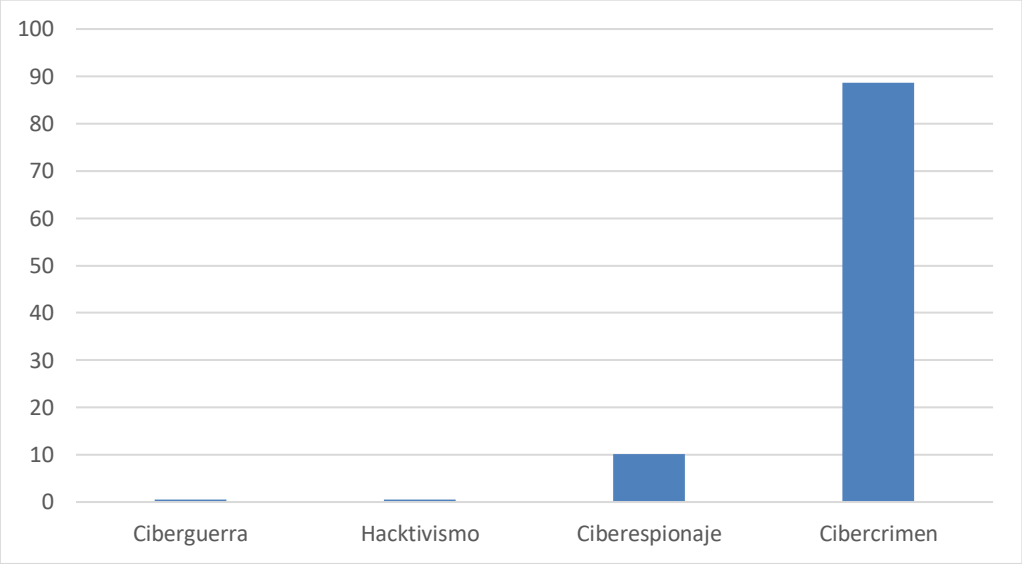

Figura 3. Perpetuadores de ataques cibernéticos.

2.1.1 Estados.

Con el avance de la tecnología los estados se han tenido que actualizar a nivel de espionaje, aunque no se conocen muchos casos de estos atacantes se han demostrado algunos casos en los que los objetivos eran estructuras SCADA para conseguir información de otros países, aunque los ataques llevados a cabo por estos atacantes no son muy habituales deben ser considerados muy peligrosos ya que los recursos que estos grupos tienen son muy superiores a los de los demás atacantes.

2.1.2 Terroristas.

Al tratarse de estructuras críticas que supervisa una infraestructura que afecta en el día a día de los habitantes de un país estas mismas pueden ser objetivo de organizaciones terroristas que intenten dañar dichas estructuras, aunque hoy en día no ha habido ningún ataque de gran magnitud

siempre se debe tener en cuenta estos atacantes ya que representan una gran amenaza en el futuro inmediato para las estructuras críticas.

2.1.3 Crimen organizado.

El secuestro de información a empresas u organizaciones ha demostrado ser muy lucrativo, ya que con la suficiente preparación y conocimientos una organización puede conseguir grandes cantidades de dinero o información de otra organización.

Existen empresas que se dedican a llevar a cabo ataques frente a ciertas estructuras con el fin de lucrarse mediante ataques como un Ransomware, pidiendo seguidamente el debido rescate por la recuperación de los datos encriptados, estos grupos pueden ser peligrosos ya que tienen los recursos y el conocimiento para llevar a cabo ataques avanzados y de gran magnitud y suelen llevar a cabo una gran preparación.

Algunas empresas se dedican a vender sus servicios a otros como por ejemplo los ataques DoS mediante el uso de botnets que tengan establecidas.

2.1.4 Empleados descontentos.

Cuando existen empleados descontentos son un gran peligro para la empresa ya que los empleados descontentos tienen acceso a la red interna por lo que pontean la protección de la red interna respecto a la red externa y estos pueden ser contactados por otros grupos de atacantes para llevar a cabo ataques, uno de los casos más simples en los que esto puede ser peligroso es que una organización interesada en atacar a otra, como pueden ser los ejemplos comentados anteriormente, contactará con un empleado descontento proporcionándole instrucciones como por ejemplo introducir una memoria USB en un dispositivo dentro de la red interna.

Este tipo de agentes son muy peligrosos ya que, aunque ellos no tengan los conocimientos necesarios para llevar a cabo grandes ataques en la red pueden ser utilizados por otros agentes para facilitar el llevar a cabo dichos ataques.

2.1.5 Hackers

Estos atacantes suelen ser gente con interés en el mundo de la seguridad que buscan la emoción de llevar a cabo ataques algunas veces por el reconocimiento de otros, estos atacantes no suelen actuar en grupos y los recursos que tienen son muy limitados por lo que, aunque sí que pueden llegar a ser una amenaza para los sistemas no pueden compararse a los otros atacantes que hemos mencionado anteriormente.

	Recursos.	Peligrosidad.
Estados	Muy altos.	Muy alta.
Terroristas	Medios.	Alta.
Crimen organizado	Altos.	Alta.
Empleados descontentos	Bajos.	Alta.
Hackers	Bajos.	Baja.

Tabla 3. Comparación diferentes atacantes

2.1.6 Botnets.

Las botnets son una herramienta que usan los atacantes para llevar a cabo ataques de mayor magnitud, estas redes consisten en grandes cantidades de equipos infectados, normalmente sin el conocimiento de los propios usuarios, una vez infectados los equipos son utilizados por un

atacante para por ejemplo enviar masivamente mensajes a una dirección concreta para colapsar el ancho de banda y denegar el uso a usuarios normales.

2.2 Ataques

Conocer los diferentes tipos de ataques es de vital importancia ya que para poder identificar cuando se está sufriendo un ataque se debe conocer como son estos ataques y como estos se llevan a cabo.

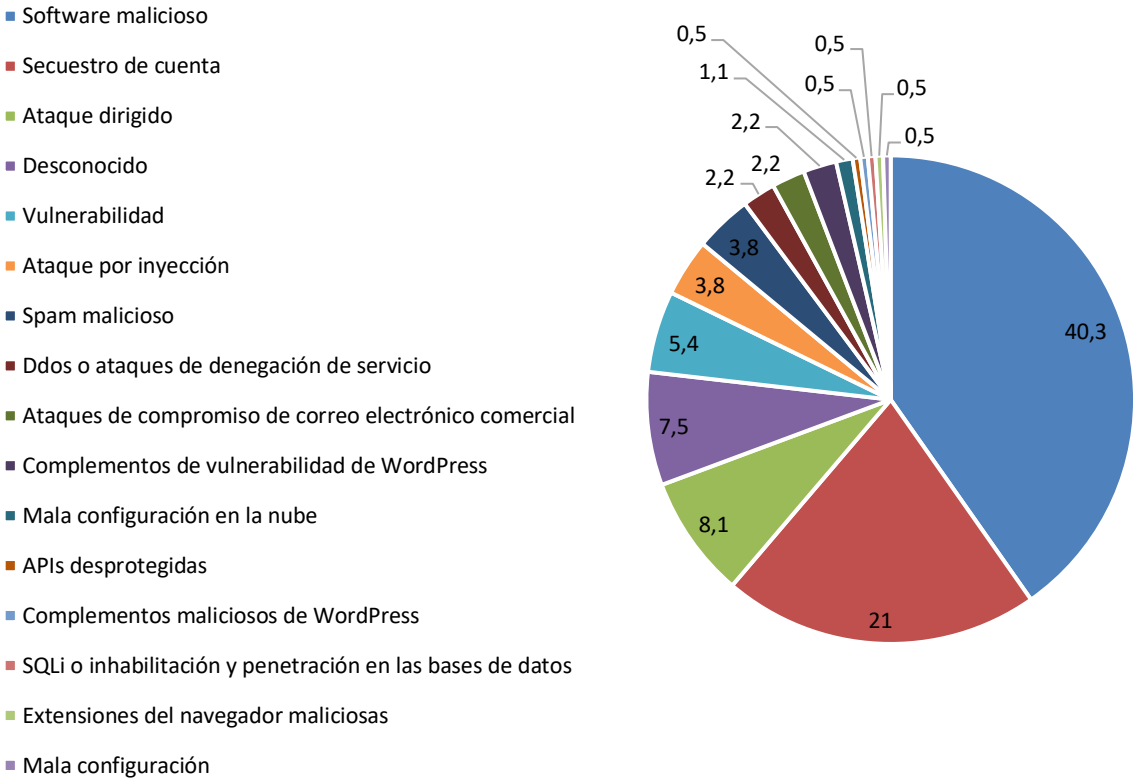

Figura 4. Técnicas ataque más usadas febrero 2020[28]

2.2.1 Phishing.

Los ataques de phishing son de lo que se llama ingeniería social, estos se hacen normalmente a través de correos y tiene como objetivo robar información del receptor o bien llevar a cabo una instalación de un programa maligno para llevar a cabo otros ataques como el Ransomware que se comenta más adelante, la forma de evitar estos ataques es mediante el uso de listas negras de correos, aunque la más efectiva es educar a los trabajadores para identificar este tipo de ataques.

2.2.2 Ransomware

Los ataques de Ransomware se basan en la encriptación de archivos, es decir una especie de secuestro de los archivos y sistemas para posteriormente pedir un pago en modo de rescate, estos ataques son muy dañinos ya que hacen imposible la recuperación de la información o los servicios a menos que se pague dicho rescate.

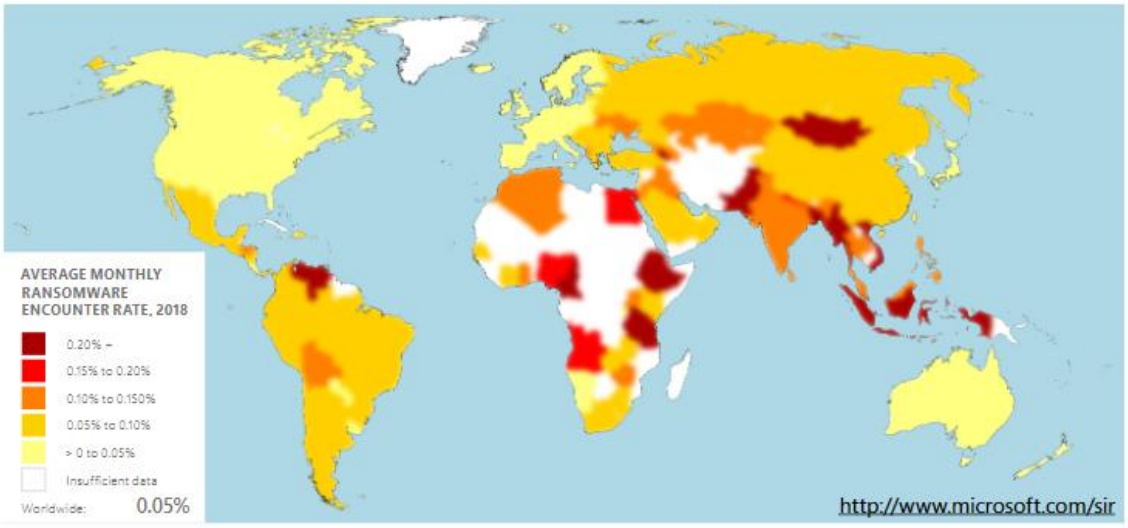

Figura 5. Mapa estadística ataques Ransomware en el mundo

Los ataques de Ransomware suelen tener la siguiente estructura:

1. Normalmente el archivo llega mediante un correo y un usuario de la red es engañado para introducirlo en la red.
2. El código infecta el dispositivo del usuario forzando al sistema operativo a hacer correr el código.
3. El código se extiende por la red utilizando fallos que pueda tener el sistema operativo para duplicarse a el mismo en diferentes dispositivos y así conseguir acceso a archivos más importantes.
4. Por último, el atacante ya tiene secuestrado el sistema y pide el rescate por recuperar el mismo, normalmente estos pagos se piden usando criptomonedas para evitar el rastreo del pago.

Para evitar estos ataques se debe llevar a cabo guardados de seguridad regulares para reducir el daño producido y educar a los trabajadores en las técnicas que de phishing para evitar la infección en primer lugar.

2.2.3 Denegación de servicios (DoS)

Los ataques de denegación de servicios son ataques que tienen la finalidad de interrumpir el correcto funcionamiento de dispositivos en concreto, esto lo hacen mediante el envío masivo de peticiones para agotar los recursos del dispositivo. Estos ataques pueden provenir de un equipo o de varios equipos, en estos casos se llama a estos ataques DDoS (Denegación de servicio distribuidos). Estos ataques suelen usar botnets para el envío masivo y se han visto potenciados por el aumento de dispositivos IoT ya que estos pueden ser infectados y usados por las botnets.

Estos ataques aparte de ser dañinos en si pueden ser utilizados para desviar la atención de otros posibles ataques, ya que los ataques Dos y DDos requieren de gran cantidad de recursos para ser combatidos.

Este tipo de ataques se pueden prevenir con la temprana detección y con el consiguiente redireccionamiento de tráfico, esto normalmente se consigue con firewalls, aunque algunos tipos de ataque DoS requieren de otros dispositivos para su prevención.

2.2.4 SQLi

Los ataques de inyección SQL se basan en la introducción de código dentro de las sentencias que se utilizaran para la obtención de datos de la base de datos, con este tipo de ataques los atacantes podrían acceder a datos privados o que no deberían de ser obtenidos por el público general.

Estos ataques se dan en los entornos que trabajan con SCADA ya que la mayoría de los servidores utilizan este tipo de lenguaje y debido a la facilidad de este ataque es por lo que cabe destacarlo.

2.2.5 APT.

APT de sus siglas en ingles Advanced Persistent Threats son un tipo de ataques los cuales tal y como indica su nombre suelen ser ataques más avanzados respecto a los ataques típicos, avanzados en varios aspectos, llevan más preparación por parte del atacante por lo cual los objetivos son más claros, suelen utilizar herramientas más potentes que los ataques habituales y por tanto estos suelen ser más difíciles de detectar y por norma general son mucho más dañinos que los ataques habituales.

Capítulo 3. Ciberseguridad

3.1 Arquitecturas de seguridad de redes.

La seguridad de una red se basa en esencia en la arquitectura que esta presenta, existen diferentes enfoques en este documento se van a detallar los dos más utilizados, la seguridad perimetral y la seguridad de confianza cero (Zero Trust).

3.1.1 Arquitectura de seguridad perimetral.

Este tipo de arquitectura ha sido el estándar durante mucho tiempo, se basa en la protección de los puntos de conexión que unen la red privada con la red pública dejando sin protección a la red internamente tal y como se puede ver en la siguiente imagen.

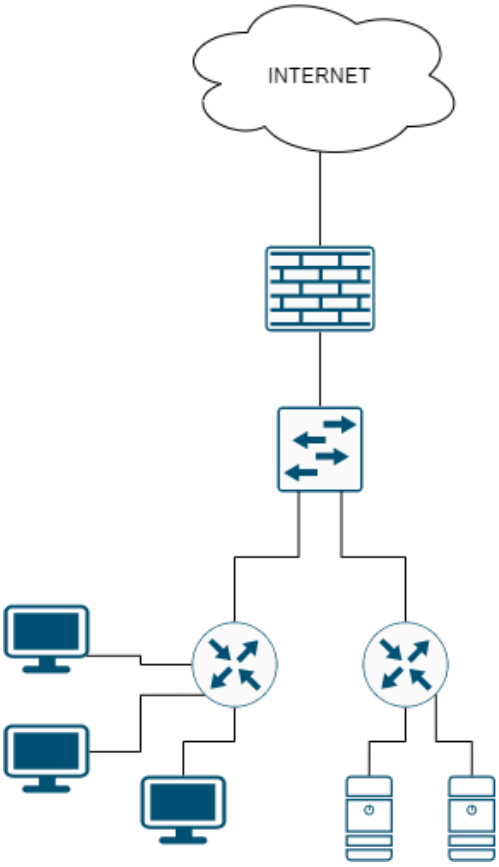

Figura 6. Ejemplo seguridad perimetral

Este tipo de arquitecturas, aunque en su momento fueron bastante útiles fallan al adaptarse a las nuevas tendencias en las comunicaciones, algunos de los fallos que comenten son los siguientes:

- La existencia de ataques sofisticados que penetren el perímetro en cuyo caso con este tipo de arquitecturas el atacante ganaría acceso completo a la red.
- La existencia de redes de invitados en casos de redes abiertas al público.
- La necesidad de conexiones con dispositivos exteriores para trabajadores que se encuentren fuera de las oficinas.
- La posibilidad de ataques por parte de trabajadores descontentos.
- La posibilidad del mal uso por parte de trabajadores no cualificados.

3.1.2 Arquitectura de Zero trust.

Frente a las limitaciones que presenta la arquitectura de seguridad perimetral se desarrolló un nuevo tipo de arquitectura, una en el que la primicia fue que la red es hostil por lo que se tratara de segmentar en diferentes secciones la red interna.

El principio que sigue la arquitectura Zero trust es la de acercar los dispositivos de control a los usuarios, de esta forma pasaríamos de un firewall en la frontera entre internet y la red privada a la segmentación de la red privada en redes más pequeñas que tengan una funcionalidad parecida y a su vez serán más fáciles de monitorizar y más difíciles de acceder por terceros.

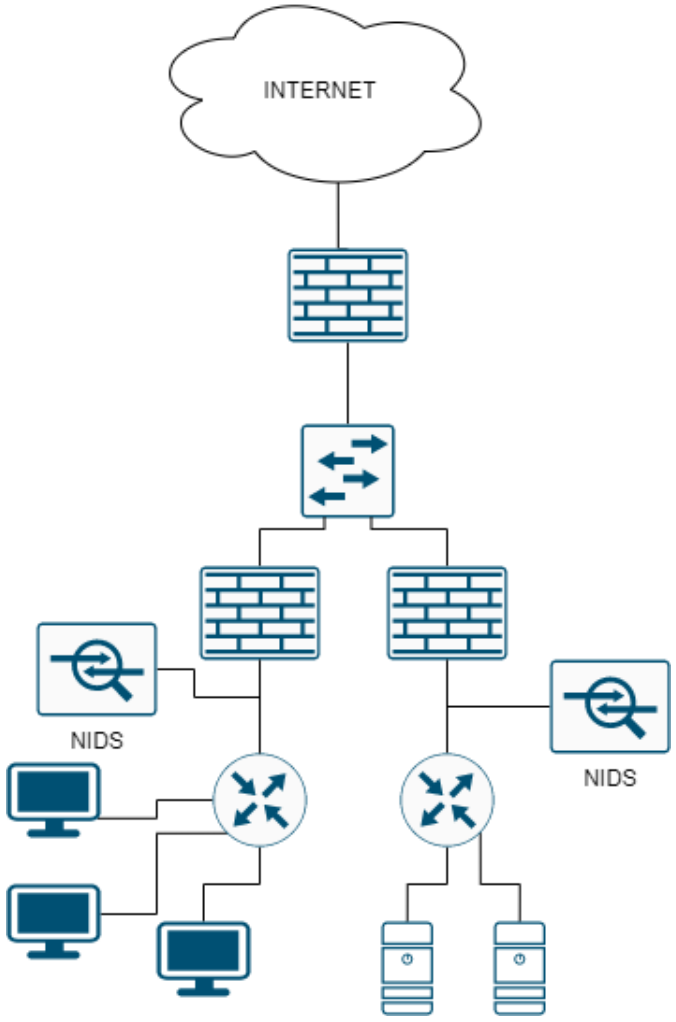

Figura 7. Ejemplo red zero trust

Uno de los objetivos de este tipo de arquitecturas a parte de la autorización inicial a los recursos es la monitorización continua por eso mismo se usan herramientas como las comentadas anteriormente para llevar a cabo dicha tarea.

Esta arquitectura de red tiene claras ventajas sobre la anterior como son, por ejemplo:

- Mayor detección de las amenazas y ataques, así como la mitigación de daños en caso de que este ataque se lleve a cabo.
- Evita el acceso por parte de usuarios no deseados a aplicaciones de alto nivel, como pueden ser las de control o mantenimiento.

3.2 Dispositivos de ciberseguridad

3.2.1 IDS/IPS

Estos dispositivos se basan en la recolección de pequeñas cantidades de información para su posterior análisis y aunque este principio si que es el mismo sus diferencias hacen que sea bueno destacar sus diferencias.

Los llamados sistemas de detección de intrusión tienen la funcionalidad de analizar los paquetes que atraviesan un punto concreto de la red en el que este es instalado, los IDS analizan los paquetes, crean logs de información con los paquetes que lo atraviesan y notifican los potencialmente peligrosos a un supervisor que podrá tomar la decisión pertinente respecto a los datos presentados.

Estos componentes son especialmente útiles a la hora de detectar ciertos tipos de ataques como por ejemplo los ataques DOS.

Los IDS se pueden clasificar respecto a diferentes aspectos bien por la forma de instalación que se diferencian entre HIDS y NIDS (Host IDS y Network IDS) dependiendo de si evalúan las actividades que se llevan a cabo en el dispositivo o si evalúan los paquetes que atraviesan cierto punto de la red.

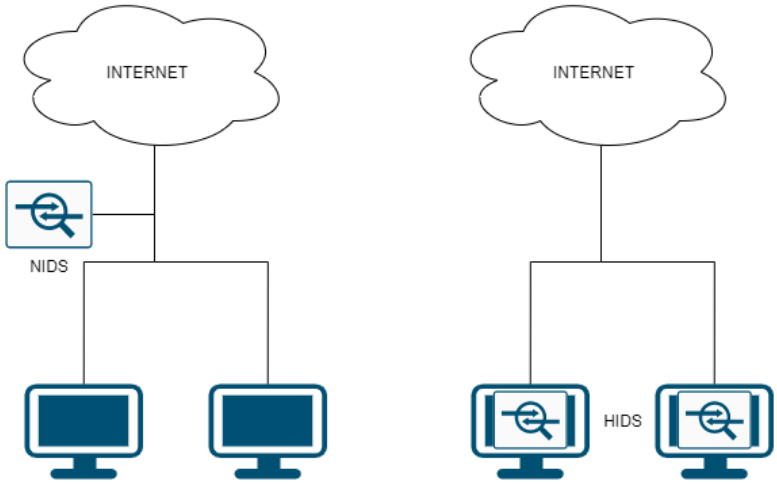

Figura 8. Instalación de NIDS y HIDS.

Los NIDS son buenos componentes para la detección y prevención de ataques DoS, ya que pueden detectar fácilmente el envío masivo de paquetes a través de la red.

Otro aspecto con los que se clasifica es la forma de detectar los ataques, los que analizan la firma de los paquetes y los basados en anomalía, estos IDS se utilizan en diferentes ámbitos y tienen sus ventajas e inconvenientes.

- Los IDS basados en firma tienen la ventaja que reducen el número de falsos positivos, son buenos detectando ataques más habituales y simples, pero por otra parte no pueden detectar ataques que no sean conocidos por lo que variaciones de ataques serán más difíciles de detectar y por tanto se debe mantener actualizado constantemente para conocer ataques recientes.
- Los IDS basados en anomalía son mejores a la hora de detectar ataques no conocidos o que no se conocen todos los detalles, por otra parte, estos IDS también se pueden utilizar combinándose con los basados en firma para una vez detectada una anomalía se conozca la firma, por otra parte los IDS basados en anomalía son más propensos a informar de falsos positivos ya que el comportamiento de los usuarios de la red no siempre se comportan igual y también tardan en ser funcionales ya que tienen que construir un perfil de comportamiento.

Por esta razón lo óptimo en la red es utilizar un IDS hibrido de esta forma los ataques más habituales serian detectados y los comportamientos extraños se analizarían y se podrían añadir como posibles ataques.

La instalación de los IDS se suele hacer en la entrada/salida de la red, es mejor la instalación en ambos extremos de los dispositivos de acceso para poder detectar posibles ataques a los puntos de acceso y monitorizar si estos atraviesan los puntos, y en ciertos componentes importantes de la red, aquellos que son más susceptibles de recibir un ataque.

Los llamados **Intrusion Prevention Systems** son dispositivos con funciones similares a los IDS en el sentido que también analizan los paquetes que circulan por donde está conectado, pero al contrario que los IDS que son elementos pasivos que simplemente informan sobre los posibles ataques los IPS son elementos activos por lo que pueden tomar decisiones sobre los paquetes, como puede ser por ejemplo el bloqueo de dicho paquete, estos dispositivos aunque puedan parecer una mejora de los IDS no siempre es así ya que en algunas ocasiones puede ser muy inconveniente no tener control sobre la acción que se toma en ese momento sobre la información, las ventajas y desventajas de estos dispositivos respecto a los IDS son las siguientes.

Ventajas.

- Un ataque detectado será neutralizado en el momento por lo que prevendrá posibles daños.

Desventajas

- Un falso positivo ya que en caso de que el paquete fuera eliminado podría perderse información importante
- Ralentiza la conexión, aunque esta bajada de rendimiento no es muy grande en ciertos ámbitos como las estructuras criticas esto puede ser muy perjudicial.

Los IPS también se clasifican por el lugar en el que son instalados teniendo así HIPS y NIPS a la vez que tienen diversas formas de funcionamiento iguales a las de los IDS con las mismas ventajas y desventajas.

3.2.2 Firewall.

Los firewalls son los dispositivos de seguridad más utilizados y se utilizan para controlar el flujo de datos entre diferentes redes, para conseguir esto un firewall usa diferentes funciones como son el filtrado de paquetes, el marcado de paquetes o proxy forwarding.

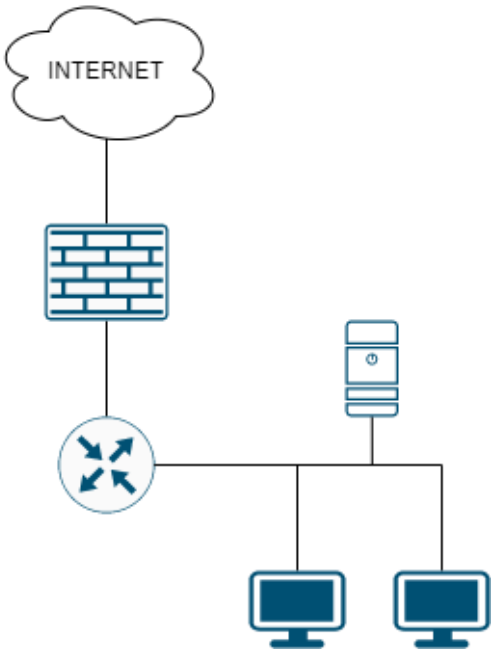

Figura 9. Instalación típica de un firewall

Existen diferentes tipos de firewall y el etiquetado de estos está ligado a la capa OSI sobre la que trabajan.

Firewall de filtrado de paquetes, estos firewalls son los más antiguos y básicos trabajan sobre los puertos, opera en la tercera capa, su función es supervisar determinados aspectos de los paquetes como son su IP destino, protocolo o puerto al que están dirigidos. Funciona con una lista de normas y en caso de que el paquete no corresponda con una norma que tenga el firewall asignada este será bloqueado o descartado.

Stateful Packet Inspection firewalls estos dispositivos actúan en la cuarta capa por lo que analizan los protocolos de transporte que se utilizan durante el establecimiento de la comunicación, al actuar solamente durante el establecimiento estos firewalls dependen de la confianza entre los dos extremos de la comunicación.

Firewall de aplicación estos dispositivos actúan en la séptima capa y controla el acceso a aplicaciones y servicios en la red, este firewall envía la petición a un servidor proxy para que se autorice y en caso de que esto pase le envía una copia de la petición al destinatario original, aunque estos firewalls son muy seguros también ralentizan de forma significante la velocidad de la red.

El funcionamiento de los firewalls se basa en listas de normas en las que se permiten o se prohíben diferentes direcciones IP de origen y destino con ciertos puertos de destino y protocolos del paquete, uno de los métodos más típicos de diseño de normas de los firewalls es prohibir todos los tipos de comunicaciones por defecto salvo las excepciones que se contemplan en la red. A la llegada de un paquete al firewall este comparara sus características con su lista de normas y actuara dependiendo de estas mismas.

Tabla 4. Ejemplo normas firewall

Norma	IP Origen	IP Destino	Puerto Origen	Puerto Destino	Protocolo	Acción
1	192.168.1.0/24	10.0.0.1	*	53	TCP	Accept
2	0.0.0.0/0	0.0.0.0/0	*	*	IP	Deny

Los firewalls más modernos tienden a utilizar una mezcla de tecnología para poder supervisar en diferentes capas y de esta forma proporcionar una defensa en varios niveles.

3.2.3 DMZ

Una zona desmilitarizada (DMZ) es el resultado de usar dos firewalls para aislar una red intermedia entre la red interna y la red externa, normalmente en esta red se llevan a cabo las funciones de comunicación con la red externa, como pueden ser por ejemplo los servicios de correo u otras aplicaciones de comunicación con la red externa, por tanto, se considera una primera línea de defensa frente a los atacantes.

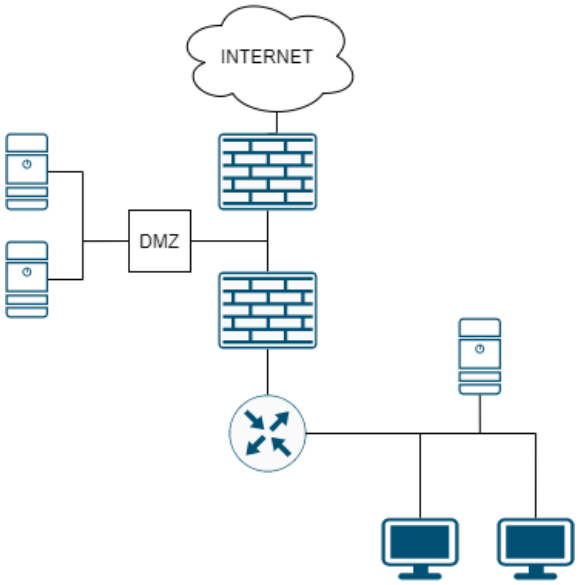

Figura 10. DMZ instalado en la red

3.2.4 Honeypot/Honeynet

Los Honeypot y Honeynets son herramientas de seguridad con gran potencial y a la vez son bastante únicas, en el sentido que son dispositivos preparados para ser atacados para así detectar posibles amenazas para el resto de la red y así mejorar la detección en casos futuros.

La diferencia entre estos dispositivos radica en el tamaño y la complexidad de estos ya que mientras los honeypot son dispositivos individuales, o incluso pueden llegar a ser cosas tan simples como archivos dedicados, las honeynets son redes completas con la única finalidad de ser atacadas y así comprobar cómo se comporta un atacante dentro de esos entornos.

Normalmente se posicionan dentro de las DMZ ya que al ser atacados podrían ser comprometidos y se debe evitar la posible expansión a otros dispositivos, a su vez dentro de la DMZ se deberá asegurar que no pueda pasar a otros dispositivos.

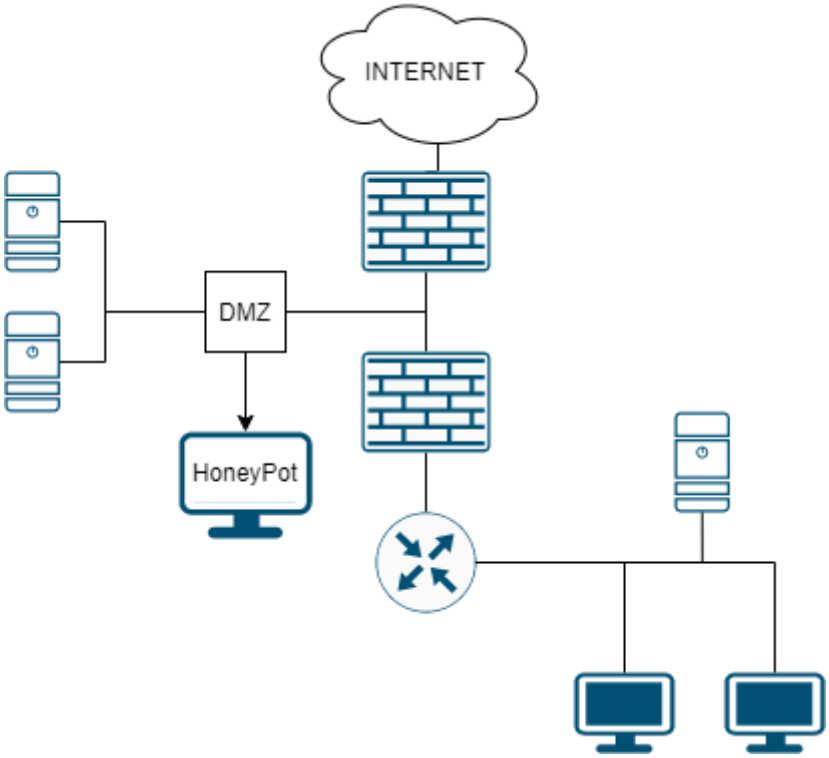

Figura 11. Red con HoneyPot

Las ventajas que presenta colocar estos dispositivos en un sistema son las siguientes:

- Reduce la cantidad de logs creados respecto a otros dispositivos, por lo que los datos son más valiosos y son más fáciles de tratar.
- Reduce los falsos positivos ya que al ser atacadas detectan los patrones de dichos ataques y así posteriormente aumentar la eficiencia de otros dispositivos.
- Detectar falsos positivos, ya que puede ayudar a detectar nuevos tipos de ataques antes de que estos sean conocidos y se disponga de firmas sobre estos.

3.2.5 Antivirus

Los antivirus son software instalados en los dispositivos de los usuarios que se dedican a monitorizar dicho dispositivo, esto requiere una constante actualización para tener disponible una base de datos de los diferentes tipos de ataques que existen y poder identificarlos dentro del sistema en el que son instalados.

Existen diferentes metodologías de escaneo para los antivirus que incluyen el escaneo basado en detección de firmas que buscan trozos de código que puedan ser reconocidos como virus, es decir que se encuentren dentro de la base de datos del programa, escaneo heurístico que analiza patrones de comportamiento de las aplicaciones, este tipo de escaneo se basa más en determinar la posibilidad de que un programa pueda ser un virus y suelen ser supervisados por otra sistema de escaneo, o desencriptado general que funciona creando entornos virtuales para el desencriptado de archivos que puedan ser maliciosos para llevar a cabo una posible infección controlada.

3.2.6 SIEM

Los SIEM (Security Information and Event Management) se encarga de recolectar los datos de diferentes dispositivos analizar dichos datos y comunicar los problemas que se hayan detectado una vez se ha llevado a cabo la acción pertinente el SIEM almacena la información para que sea de ayuda en posibles futuras anomalías, esto se hace mediante la conexión a diferentes tipos de sensores como pueden ser los IDS comentados con anterioridad, firewalls o antivirus instalados

en los dispositivos. Las ventajas de los SIEM es que las fuentes pueden ser de diferentes fabricantes ya que ellos mismos estandarizan los datos que recopilan.

Estos dispositivos pueden ser configurados o bien para actuar simplemente como informantes, es decir que simplemente generan alertas que avisaran a una instancia superior o si son conectados a ciertos dispositivos como los IPS pueden servir como administrador sobre ellos pudiendo incluso eliminar los paquetes que detecte como nocivos.

Los SIEM junto con los dispositivos mentados anteriormente funcionaria de la siguiente manera.

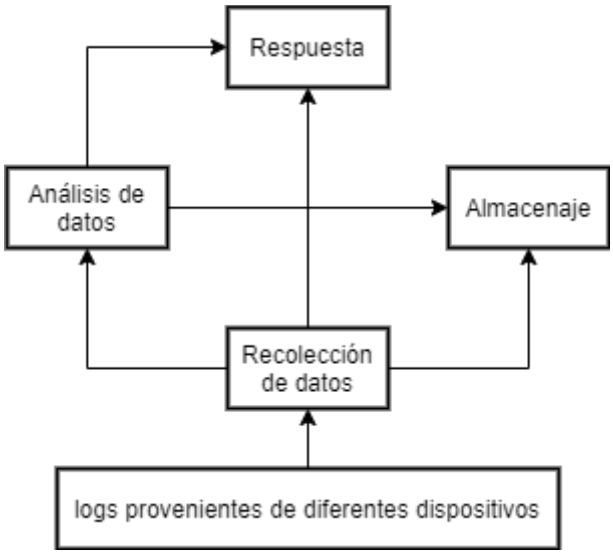

Figura 12. Diagrama de información de los logs.

Donde los diferentes logs de los dispositivos son recogidos por el SIEM para a la vez que se almacenan los datos en crudo estos mismos se analizan, almacenando después el análisis realizado y se lleva a cabo una respuesta dependiendo de los resultados, el guardado de datos se lleva a cabo para poder tener una respuesta más rápido o simplemente tener un perfil más acertado sobre los tipos de ataques.

3.2.7 Romper la Cyber Kill Chain

El objetivo de todos estos dispositivos es el de detectar posibles ataques o parar estos, esto se puede relacionar con el modelo de Cyber Kill Chain, cada uno de estos dispositivos afecta de forma diferente, ya que algunos pueden actuar sobre la fase de envió del programa dañino o cuando este mismo se está expandiendo por la red.

Un resumen de cómo afecta cada dispositivo a la Cyber Kill Chain se muestra en la siguiente tabla.

Tabla 5. Irrupción en la Cyber Kill Chain

	Detección	Prevención	Disrupción	Degradar	Engañar
Reconocimiento	IDS. HoneyPot/net.	IPS Firewall	HoneyPot/Nets IPS		HoneyPot/Nets
Preparación	NIDS. Compartir información sobre amenazas.	NIPS Compartir información sobre amenazas.	Ocultar versiones.		
Entrega	IDS Firewall	NIPS Firewall			HoneyPot/Nets
Intrusión	HIDS	Actualización del sistema			HoneyPot/Nets
Instalación	HIDS	HIPS	Antivirus		HoneyPot/Nets
Comando y control	NIDS SIEM	Firewall	NIPS		HoneyPot/Nets
Acción sobre los objetivos	Análisis de logs				

Como se puede observar en la tabla elementos pasivos como los diferentes tipos de IDS son los que llevan a cabo gran parte de la detección en las diferentes fases del modelo, aunque los IPS también detectarían el ataque al ser elementos activos estos directamente prevendrían que el ataque siguiera a otras fases y el engaño se llevaría a cabo en su totalidad por los HoneyPot y HoneyNets ya que estos podrían dar información errónea sobre los dispositivos vulnerables del sistema al atacante.

Capítulo 4. Seguridad física.

La seguridad física se basa en el control del movimiento de las personas dentro del edificio en cuestión, se pueden dividir en tres secciones el control de acceso, la detección de intrusión y la videovigilancia.

4.1 Control de acceso.

El control de acceso se basa en el posicionamiento de barreras físicas dentro del edificio para impedir el paso de aquellos individuos que no sean autorizados por el sistema. Los dispositivos de control de acceso cuentan normalmente con cierta capacidad de procesado para tener cierta autonomía.

Para llevar a cabo un control de acceso seguro se deberá dividir en zonas las instalaciones a controlar, y modificando el acceso dependiendo de las funciones que tenga cada grupo de acceso, dividiéndose en Tiers de seguridad dependiendo de la importancia de las instalaciones a las que se intentara acceder, cabe destacar que el hecho de que un individuo tengo acceso a una zona de la seguridad más alta no implicará que tenga acceso a otras zonas con la misma seguridad, también se deberá llevar a cabo un control de las salidas de las zonas con mayor seguridad.

Dentro del acceso se deberán ajustar las tecnologías usadas para identificar a los individuos que acceden a cada área, utilizando tecnologías más avanzadas para áreas críticas o con instalaciones más importantes.

Las tecnologías más utilizadas para el control de acceso son las siguientes.

4.1.1 Tokens.

La tecnología de los tokens tal y como indica su nombre son sistemas de credencial material que se asignara individualmente a cada individuo que lo acreditara e identificara para el acceso a las zonas que este tenga disponibles.

Algunos ejemplos son las tarjetas con banda magnética o algún tipo de comunicador de radiofrecuencia.

El funcionamiento de las tarjetas consiste en una comunicación a través de la banda de 13,56MHz a través de la cual se produce una comunicación en el la que se envía de una pequeña cantidad de información desde la tarjeta la cual consiste en la ID asociada de la tarjeta.

Las ventajas de esta tecnología es la facilidad de distribución a los empleados de una empresa, ya que se activan con facilidad y no requieren de intervención por parte del individuo, esto a su vez también es parte de su fallo ya que no se está identificando al individuo, sino que se está comprobando que el token que se está usando está dentro del sistema sin acreditar que aquel que lo porta es quien debería ser.

Esta tecnología cuenta con un sensor de lectura que será el encargado de captar la señal de la tarjeta en cuestión y comunicarse con la base de datos para comprobar que las credenciales son las correctas.

4.1.2 Credenciales de conocimiento.

La tecnología de credenciales de conocimiento utiliza conocimientos del usuario para llevar a cabo el control de acceso, un ejemplo sería que cada usuario tiene un PIN asignado que tiene que introducir para poder acceder a una sala.

Respecto a las anteriores estas mejoran la seguridad en el sentido que la clave de acceso no puede ser sustraída a un individuo sin su consentimiento, aunque presenta el problema que cualquier individuo que conozca la clave puede saltarse el control de acceso sin problemas.

4.1.3 Biometría.

La tecnología biométrica se basa en el uso de facultades físicas de las personas para llevar a cabo la identificación de estas, representa un gran avance ya que es casi imposible falsear las credenciales de un individuo en concreto, la biometría se puede implementar sobre diferentes partes del cuerpo humano, y en los casos de estructuras críticas se buscará una doble autentificación en las partes más sensibles del sistema.

Las diferentes tecnologías de biometría que existen son la lectura de huella dactilar, esta técnica es usada debido a que cada huella dactilar es única, reconocimiento facial, la lectura del iris, debido también a la particularidad de cada iris y escaneo de geometría de la mano.

- La lectura de huella dactilar se basa en la captación de la huella a través de la capacitancia de la huella en la que se consigue una impresión de la huella y se crea un mapa de bits de esta que a continuación será comparado con aquel que se tiene guardado, esta comparación puede ser o bien por correlación es decir buscando puntos concretos de la huella y la basada en minucias en la que se mapea la relación de la huella a partir de encontrar puntos concretos.

Figura 13. Ejemplo mapa de bits de huella dactilar

- El reconocimiento facial se basa en la identificación de un individuo a partir de una imagen o un fotograma de un video, el reconocimiento facial se basa en la métrica facial que consiste en comparar las características principales de una cara como son la distancia entre ojos, nariz y boca o el posicionamiento de estos
- La lectura del iris se basa en la identificación a partir de una imagen del iris, en esta se buscan las diferentes características que componen el iris a partir de las cuales crea un código que será la base de la clave de acceso, para llevar a cabo esta comparación se utiliza la distancia basada en el número de bits de la imagen y si esta no supera un umbral marcado se da por buena.
- La geometría de la mano se basa en la medición de la largaria, ancho, grosor y calcula del área de una mano, este método se usa ya que la mano no varía a partir de cierta edad. Para el escaneo se lleva a cabo el mapeado de la mano para su posterior procesado.

4.2 Detección de intrusión.

La detección de intrusión se encarga de la tarea de detectar cualquier movimiento sospechoso en los sistemas en los que no se debería estar produciendo dicho tipo de movimientos.

Por ejemplo, la apertura de una puerta sin que se encuentre presente ningún empleado acreditado o un movimiento en una sala que se supone que debería estar vacía o se puede generar una alarma cuando una puerta que debería estar cerrada normalmente pasa un tiempo abierta.

Las conexiones de los dispositivos de control de acceso se llevan hasta un panel central de alarma, estas conexiones se llevan a cabo a utilizando buses series debido a que se intercambian pequeñas cantidades de datos, además si se trata de un edificio también se instalan expansores de zonas para poder conectar todos los sensores de intrusión.

4.2.1 Contactos magnéticos.

Los contactos magnéticos son imanes que se instalan en las puertas para que en caso de que esta puerta sea abierta se genere una alarma y en caso de que esta no esté dentro de unos parámetros establecidos se pueda supervisar que está ocurriendo en ese punto.

4.2.2 Detectores de presencia.

Los detectores de presencia son pequeños dispositivos electrónicos cuya función es detectar el movimiento o la presencia de un cuerpo extraño en una sala, existen dos tipos de tecnologías extendidas y utilizadas para diferentes funciones.

- Los detectores de infrarrojos que se basan en la captura de la temperatura del sitio en el que son instalados, estos detectores son muy sensibles a los movimientos normales dentro de su campo de visión, aunque si estos movimientos son pequeños esta tecnología no es muy eficaz.
- Los detectores de ultrasonido utilizan una tecnología más avanzada que los infrarrojos calculando la diferencia entre una onda emitida y la recibida, por esto pueden detectar presencias incluso detrás de objetos que bloqueen el campo de visión del dispositivo, la desventaja de esta tecnología es que es muy sensible a vibraciones de dispositivos.

Las soluciones más avanzadas que encontramos en el mercado son las de tecnología hibrida en la que se usan tanto los infrarrojos como los ultrasonidos.

4.3 Videovigilancia.

La videovigilancia cumple la tarea de poder controlar las zonas de acceso y las habitaciones importantes, el sistema de videovigilancia se suele encontrar centralizado de forma que se puede visionar todas las cámaras del sistema para poder vigilar grandes extensiones desde un solo punto, existen diferentes tipos de cámaras el tipo bala y las domo, a su vez la funcionalidad de las cámaras también es una característica importante ya que no todas las cámaras son estacionarias existen aquellas que se llaman PTZ Pan, Tilt y Zoom que a través de unos controles se puede mover dicha cámara para poder prestar atención sobre posibles anomalías.

Por tanto, se puede entender la videovigilancia como un sistema que mejora el resto de sistema de seguridad, llevando a cabo una vigilancia sobre las zonas de acceso y visionando las habitaciones en caso de alarma generada por los sistemas de detección de intrusión.

- Las cámaras tipo bullet son cámaras apropiadas para exteriores ya que tienen mayor rango de visión y también suelen tener resoluciones mayores, así como alimentación a través de PoE para poder minimizar el cableado de conexión de los dispositivos.
- Las cámaras tipo domo son cámaras usadas en interiores debido a que suelen ser cámaras con menor rango de visión y con resoluciones más pequeñas, pero cuentan con mayor ángulo de visión por lo que se puede llevar a cabo la vigilancia sobre los pasillos, también suelen tener las funciones PTZ para en caso de ser necesario hacer un seguimiento de la posible amenaza.

4.4 Conexión de elementos.

4.4.1 Detección de intrusión.

Primero definiremos la estructura de red de los diferentes dispositivos de control de acceso, estos dispositivos están conectados a un panel central que a su vez se conecta a través de la red IP al centro de seguridad desde el que se supervisaran las diferentes alarmas creadas, si las distancias son muy grandes se usan expansores junto con las PSU (power suply units) para llevar la conexión a los dispositivos lejanos.

A continuación, se muestra un ejemplo de conexión de una red con dos expansores de zona.

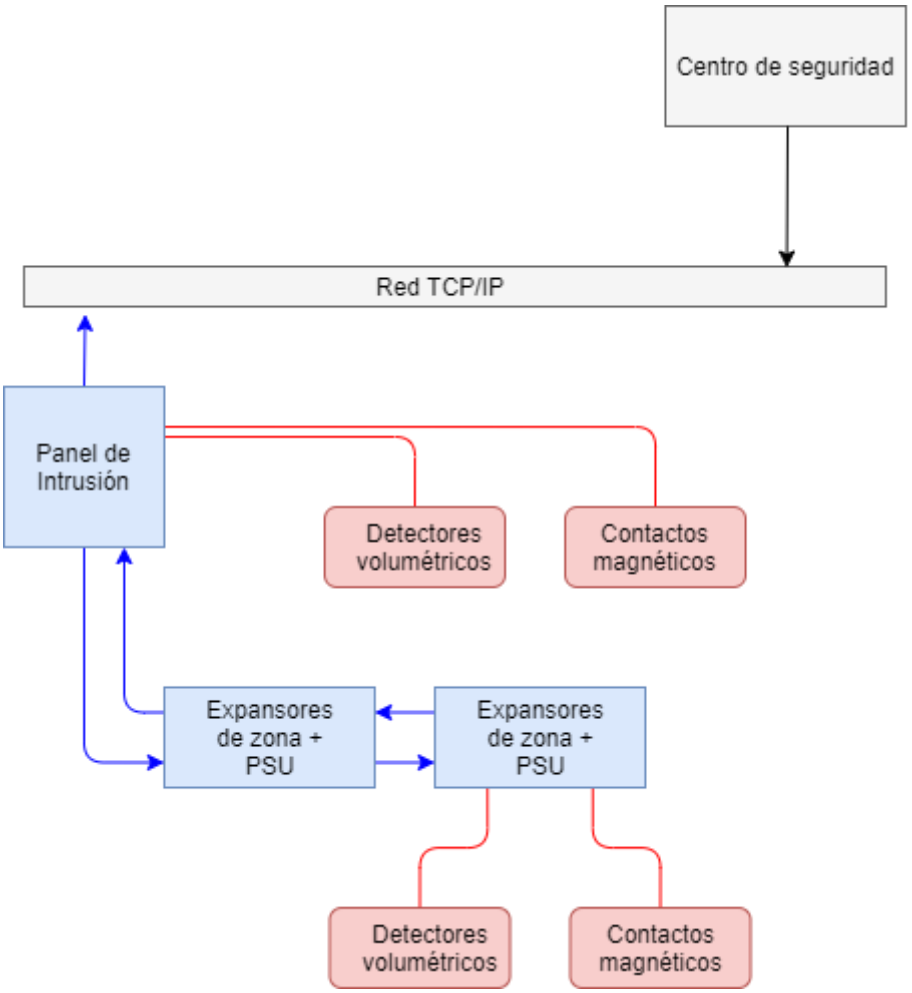

Figura 14. Esquema instalación intrusión.

4.4.2 Control de acceso.

Los dispositivos de control de acceso se instalan normalmente junto a un panel individual que gestione cada uno de estos dispositivos, a su vez también se conectan los diferentes componentes como las cerraduras eléctricas para abrir y en caso de que exista control de acceso en una puerta cabe la opción de instalar el contacto magnético en el panel.

A continuación, se muestra el ejemplo de una puerta con doble control de acceso entra y salida y con el contacto magnético conectado.

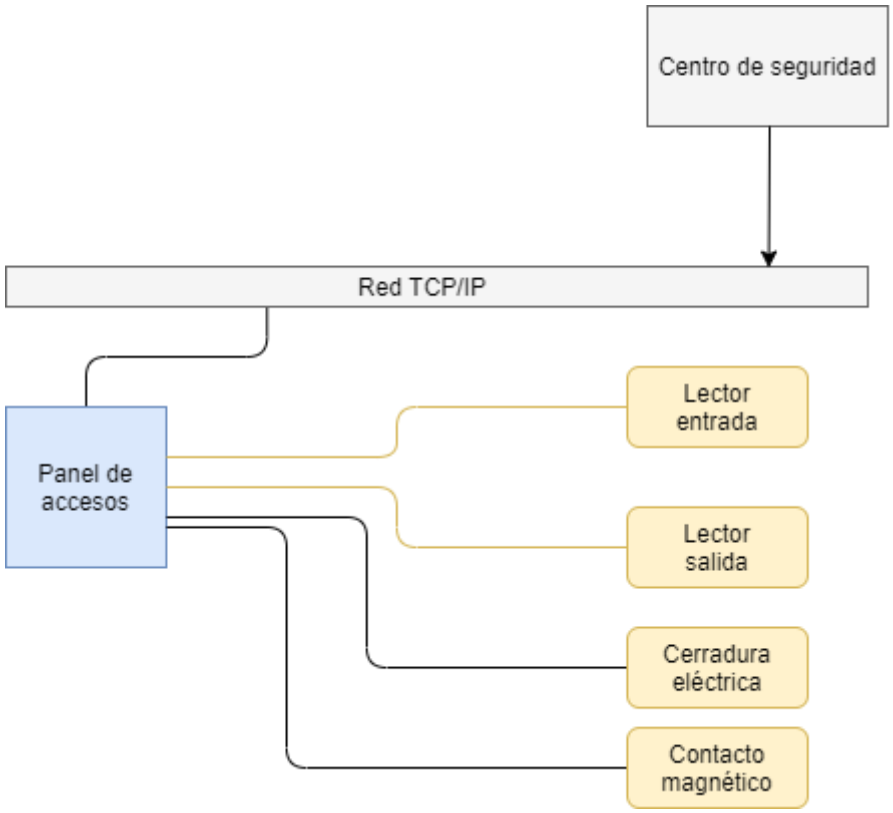

Figura 15. Esquema instalación Control de acceso.

4.4.3 Videovigilancia.

Los sistemas de videovigilancia constan de dos elementos de conexión, primero un videograbador en el que se almacenan las imágenes que captan el CCTV y segundo se conecta a un dispositivo en el que se podrá visualizar la imagen en de las cámaras de manera centralizada. Casi todas las cámaras cuentan con opción de alimentación a través de PoE por lo que su conexión debe ser a través de un dispositivo que soporte dicho protocolo.

A continuación, se muestra el esquema de una red CCTV alimentada a través de PoE que cuenta con un videograbador.

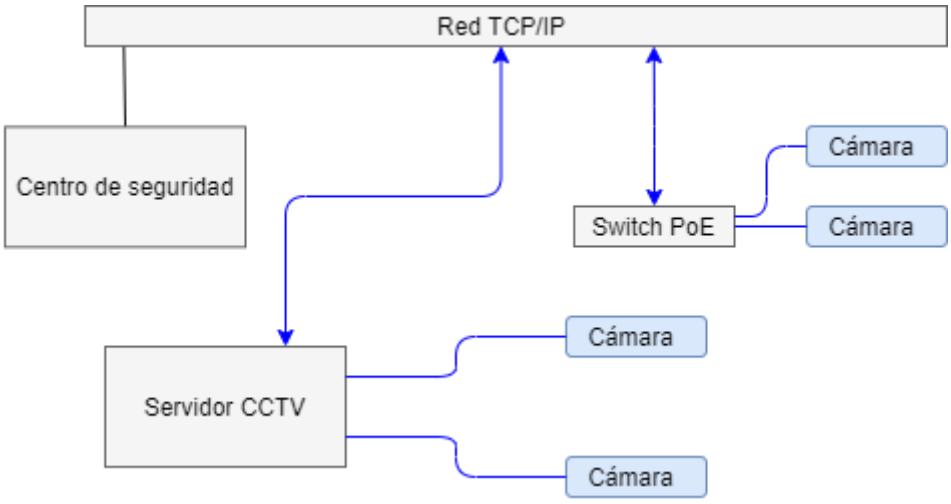

Figura 16. Esquema instalación CCTV.

Capítulo 5. Desarrollo del proyecto.

5.1 Situación inicial

La red del centro de control consta de un nodo principal el cual se encuentra conectado a internet a través de un firewall perimetral y una DMZ en la cual se encuentran las conexiones con servicios de las redes exteriores, de este nodo principal cuelgan tres redes LAN las cuales cada una tiene una función diferente que son las siguientes.

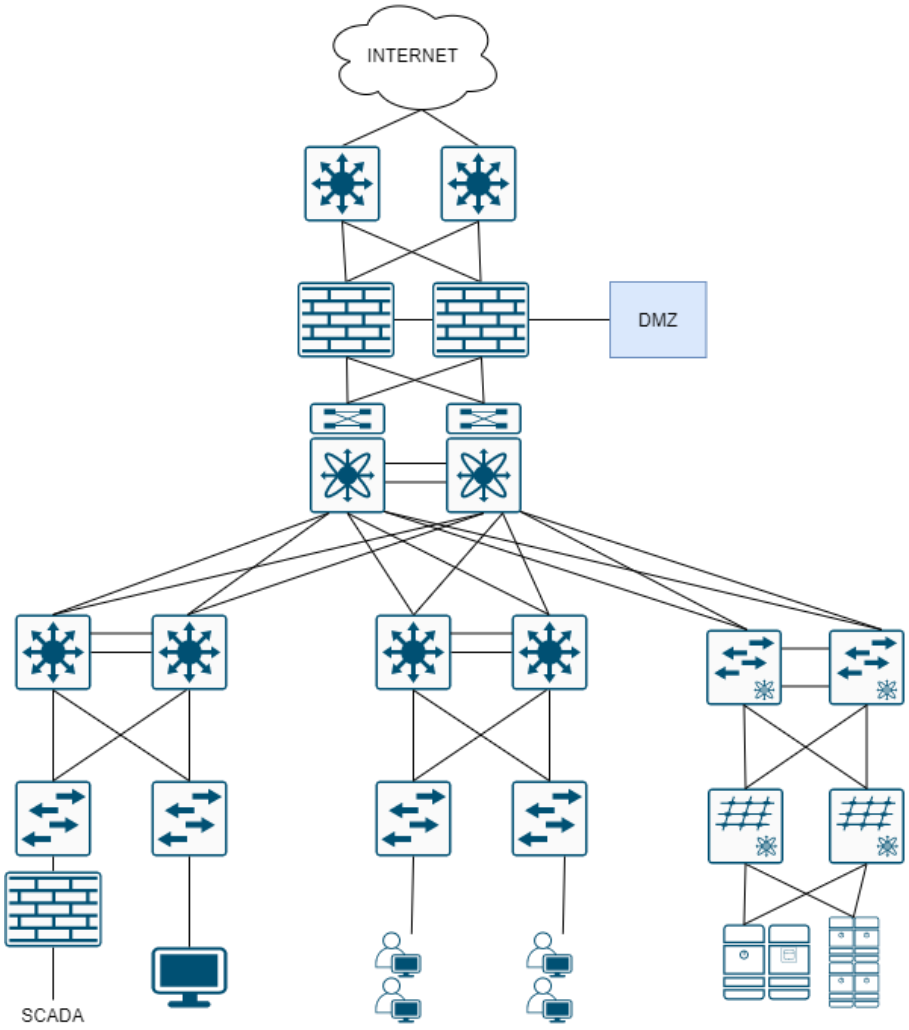

Figura 17. Red centro de control

La LAN del centro de control la cual contendrá un SCADA, así como la supervisión del tráfico, a su vez estará conectada con las redes equivalentes de otros centros de control a través de VPN gestionadas de manera privada a través de la red pública.

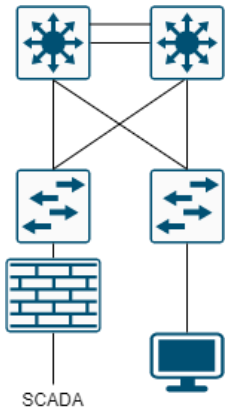

Figura 18. LAN centro de control

La LAN de las instalaciones del edificio la cual contendrá una red de oficina típica con tráfico de voz y datos.

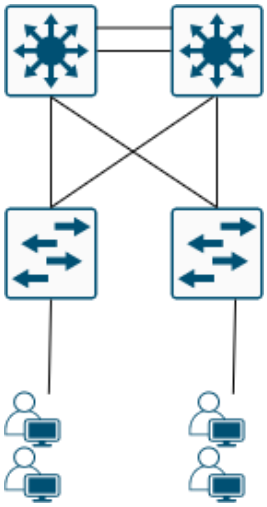

Figura 19. LAN oficinas

La LAN del CPD la cual contendrá los servidores en los que se encontraran las aplicaciones necesarias para el normal funcionamiento del centro, esta red será accesible desde las otras LAN, pero con servicios diferenciados.

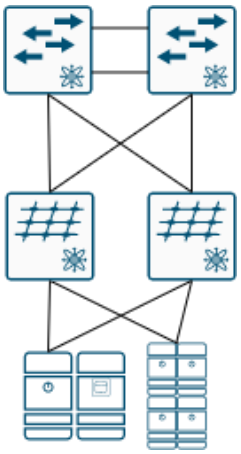

Figura 20. LAN CPD

Como se puede observar esta red presenta como medidas de seguridad un firewall en la entrada salida y su DMZ correspondiente, esta estructura es lo que llamamos una arquitectura perimetral, por lo que el tráfico interno no tiene ningún tipo de control.

Para solucionar esto analizaremos cada una de las LAN que componen la red y viendo sus necesidades ajustaremos los dispositivos que supervisan dicha red.

5.2 Análisis Ciberseguridad

5.2.1 LAN de oficinas.

La LAN de oficinas está compuesta por puestos de trabajo, no más de unos 30 puestos, que requieren solamente de voz y datos.

Aunque la LAN de oficinas a primera vista pueda parecer la más simple también se trata de las más vulnerable ya que la gran mayoría de ataques empiezan con ingeniería social, es decir a través de por ejemplo correos maliciosos usando phishing, por lo que se debe controlar tanto el tráfico entrante como el saliente ya que este puede tratarse en algunos casos de tráfico no deseado.

A su vez podría ser importante poder bloquear posibles paquetes dañinos que salgan de la red por lo que será importante usar un IPS basado en firmas evitar que aquellos paquetes que sean ataques conocidos sean bloqueados, aunque se podría optar por uno basado en anomalías esto aumentaría los falsos positivos y podría llegar a entorpecer mucho el tráfico habitual. A su vez también se instalará un Firewall para tener un doble control sobre el tráfico entrante y saliente, y se instalará un SIEM para controlar los logs provenientes de los diferentes dispositivos mentados anteriormente, así como de los antivirus instalados en los ordenadores de los empleados de la oficina.

Se combinará la instalación de un NIPS en la parte interna de la LAN con la instalación de un NIDS basado en anomalía en la parte exterior de la LAN, de esta forma se podrán detectar ataques adicionales, aunque estos no sean detenidos en el momento.

Se respetará la normativa por la que los dispositivos frontera y los de conexión deberán ser con redundancia para evitar posibles fallos en estos mismos.

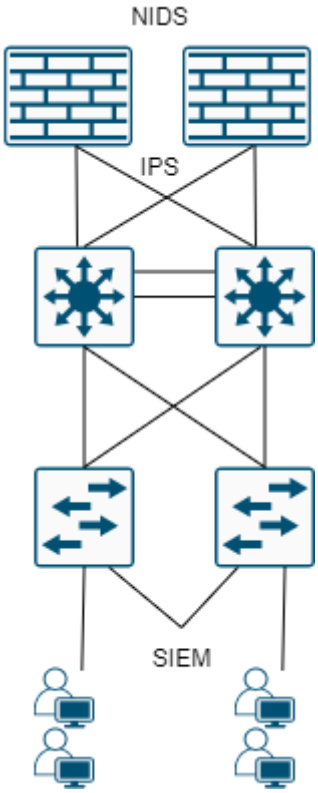

Figura 21. LAN centro de control resultante

También se podría tomar la alternativa de instalar HIDS en los dispositivos de trabajo de los trabajadores, aunque por las características de la red general no se guardara información de valor dentro de los dispositivos de esta LAN.

5.2.2 LAN centro de control

La LAN de centro de control está compuesta por puestos de trabajos de técnicos, que serán un numero bastante reducido, una sala de control desde el que se tendrá acceso a los diferentes dispositivos de seguridad instalados en la red de transporte y un tendrá conectado un SCADA en un principio conectado a través de un firewall a la red que se comunicará con los sensores de la red.

Para llevar a cabo la mejora en seguridad de esta red se tendrá que atender a que el objetivo de esta red es el continuo funcionamiento, por lo que se deberán de evitar los dispositivos que posiblemente den falsos positivos que afecten a las comunicaciones con el exterior de la red, por lo que se optara por no instalara ningún IPS y se instalaran NIDS basados en anomalía, ya que las tareas que se llevaran a cabo en esta red son concretas y conocidas, así como resguardarlo de la red exterior mediante un sistema de firewalls redundados, ya que minimizara los ataques que se puedan llevar a cabo contra esta LAN y así como la instalación de HIDS en los dispositivos conectados que junto con el antivirus evitaran la manipulación de los archivos que se encuentran en los dispositivos por terceras partes. Se instalará un SIEM para controlar los diferentes logs creados dentro de la LAN, los NIDS se instalarán tanto a la entrada de los firewalls como a su salida y a la frontera de conexión con el SCADA para poder detectar posibles ataques contra el SCADA.

A su vez para mejorar la seguridad de comunicaciones entre el SCADA y la red interna se instalará una DMZ para llevar a cabo las comunicaciones entre ambas.

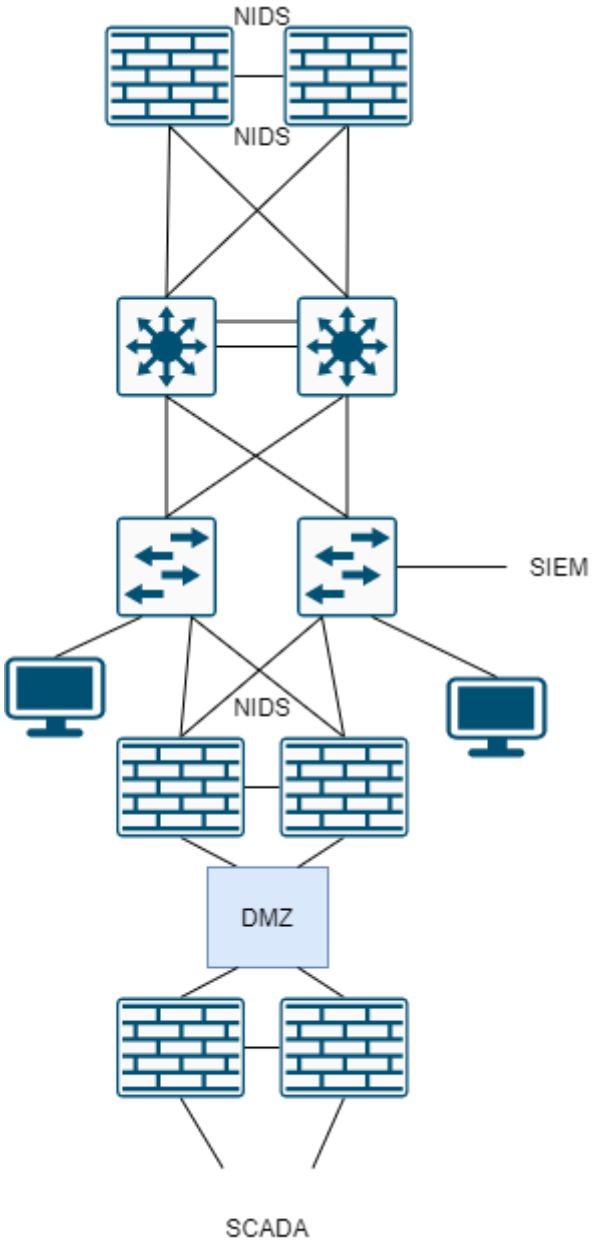

Figura 22. LAN centro de control resultante

Cabe destacar la importancia del NIDS de entrada/salida a la DMZ del SCADA ya que se debe tener muy en cuenta cualquier tráfico anómalo generado en esta dirección, por lo que el SIEM deberá prestar especial atención a este tráfico.

Se instalarán los NIDS tanto en la entrada como en la salida de los firewalls que resguardan la LAN para poder notar la diferencia entre el tráfico que llega al firewall y aquel que entra en la LAN.

5.2.3 LAN centro procesado de datos.

En la LAN del centro de procesado de datos se encuentran los servidores con las aplicaciones y los documentos, esta LAN tendrá comunicación constante con las otras LAN por tanto es especialmente vulnerable ya que es un objetivo muy importante dentro de la red del centro de control, esta red no cuenta con puestos de trabajo tradicionales por lo que la mayoría del tráfico será dirigido a diferentes LAN.

Para llevar a cabo la mejora en seguridad se tendrá que tener en cuenta la importancia de los servidores, por lo que se optara por instalar HIDS basados en firma en los servidores para evitar que los ataques proliferen dentro del propio servidor, a su vez se resguardara la LAN detrás de unos firewalls respecto a las otras redes para mejorar el control de acceso de paquetes a la red y se instalaran NIDS basados en anomalía para poder detectar ataques que los firewalls no puedan detectar fácilmente, se instalara a su vez un SIEM para controlar los sensores que se encuentran instalados en la red, igual que en las LAN anteriores, pero en este se instalara también un centro de gestión de ciberseguridad que centralizara toda la seguridad de la red interna. Esto se instala en esta LAN debido a que el funcionamiento de las oficinas es compartido con otra institución y la red del centro de control ya tiene un funcionamiento muy específico, por lo tanto, es mejor instalarlo dentro de la LAN del CPD.

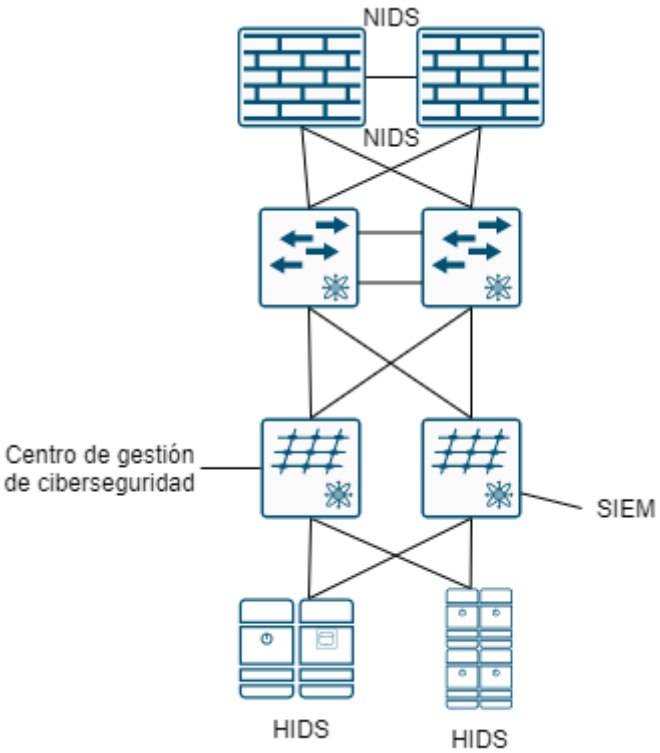

Figura 23. LAN CPD resultante

5.2.4 DMZ

En la DMZ de conexión a red externa se cumplirá la normativa sobre la redundancia de los sistemas fronteras y a su vez se instalarán unos NIDS para poder llevar a cabo el análisis de los paquetes que atraviesen los firewalls, esto tiene cierto peligro debido a que uno de estos se encuentra cerca de la red externa y podría ser alterado por lo que se debería tener especial cuidado con las alertas que este dispositivo genere.

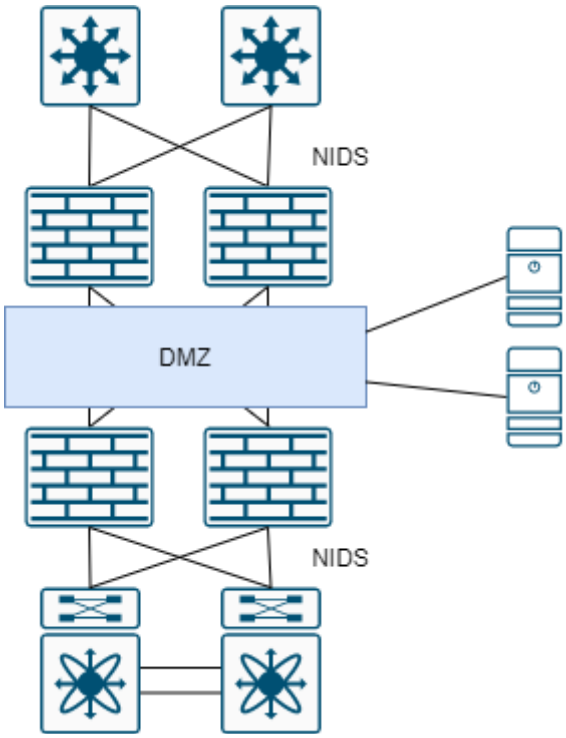

Figura 24. DMZ entrada a la red

5.2.5 Red resultante.

Por tanto, la red resultante, con los cambios mencionados anteriormente seria la siguiente.

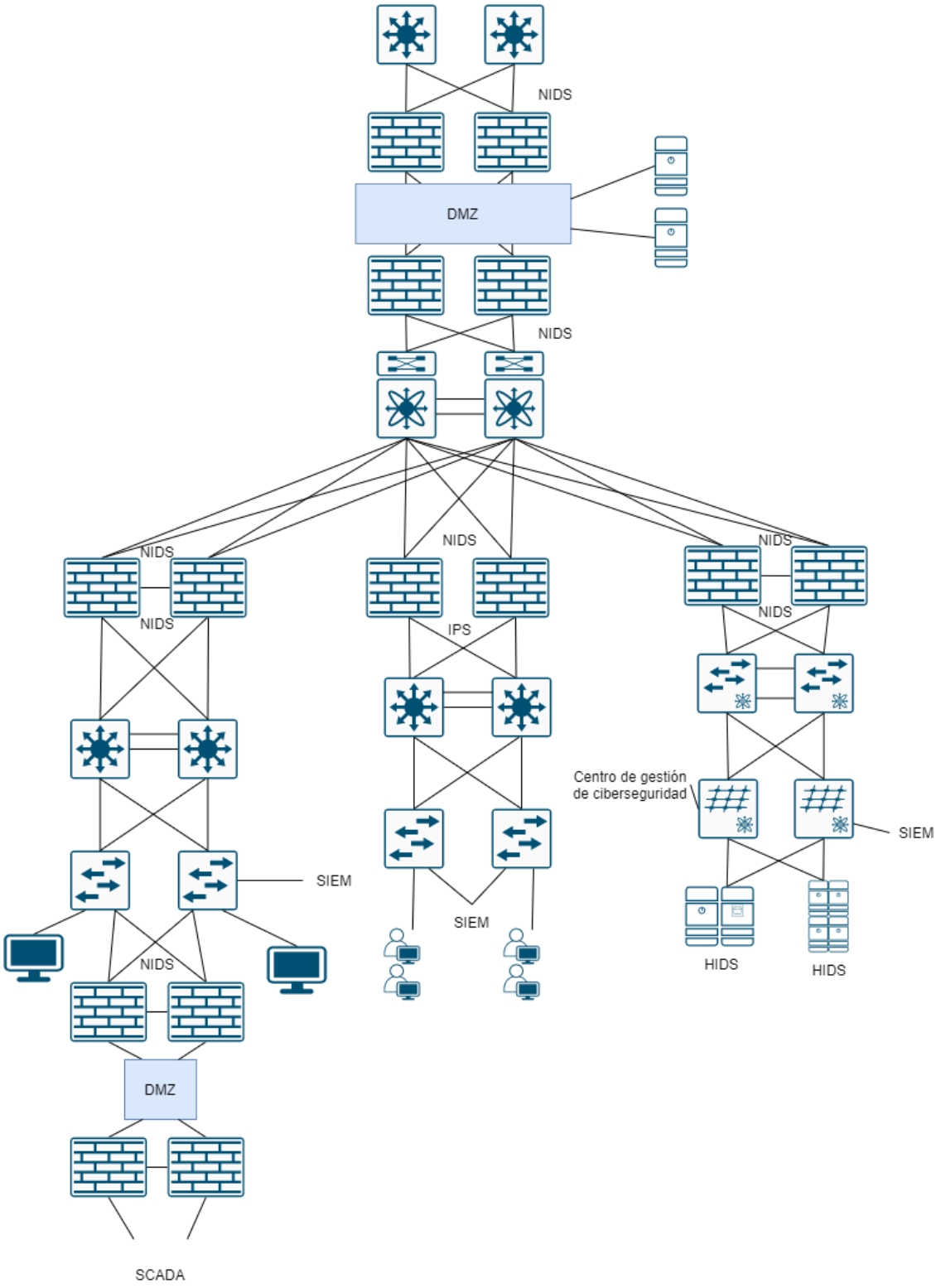

Figura 25. Red centro de gestión resultante

Se puede observar que respecto a la red original que era una estructura de perímetros esta red presenta una estructura de Zero Trust en la que los dispositivos de defensa se han acercado a los dispositivos de los usuarios a la vez que se han instalado diferentes dispositivos para monitorizar tráficos.

5.3 Análisis seguridad física.

Para llevar a cabo un análisis sobre la seguridad física del edificio primero deberemos analizar los diferentes pisos de este asignando a cada una de las plantas y habitaciones de la planta los equipos requeridos y de esta forma delimitar las diferentes zonas de acceso.

La primera planta del edifico consta de la entrada al mismo y la entrada a su vez de las diferentes instalaciones que requiere un edificio para su funcionamiento normal, así cuenta con una sala en la que se supervisara las instalaciones de seguridad del edificio y una recepción que a su vez funcionara como un primer control de acceso.

La segunda planta es una planta en la que se encontraran las oficinas del edificio en la que podemos encontrar una sala de formación y diferentes despachos, así como una zona de trabajo normal.

En la tercera planta encontramos el centro de procesado de datos, de ahora en adelante CPD, las instalaciones del CPD se dividen en tres zonas, una sala para el trabajo de ingeniería del personal, una sala contigua que se utilizara para almacén de los diferentes componentes de repuesto del CPD y una sala separada en la que se encontraran los servidores, una peculiaridad de esta planta es que cuenta con dos entradas de baja tensión, tal y como se encuentra estipulado en la normativa para las instalaciones críticas del sistema.

La cuarta y quinta planta pertenecen a la parte del centro de control del edificio, en la cuarta planta encontramos el acceso a la sala de control, esta sala es de doble altura, mientras que en la quinta planta encontramos las diferentes instalaciones desde la atención de llamadas de emergencia hasta una sala de manejo de crisis para situaciones que requieran una reunión del personal técnico.

A continuación, se muestran los planos de las plantas descritas anteriormente.

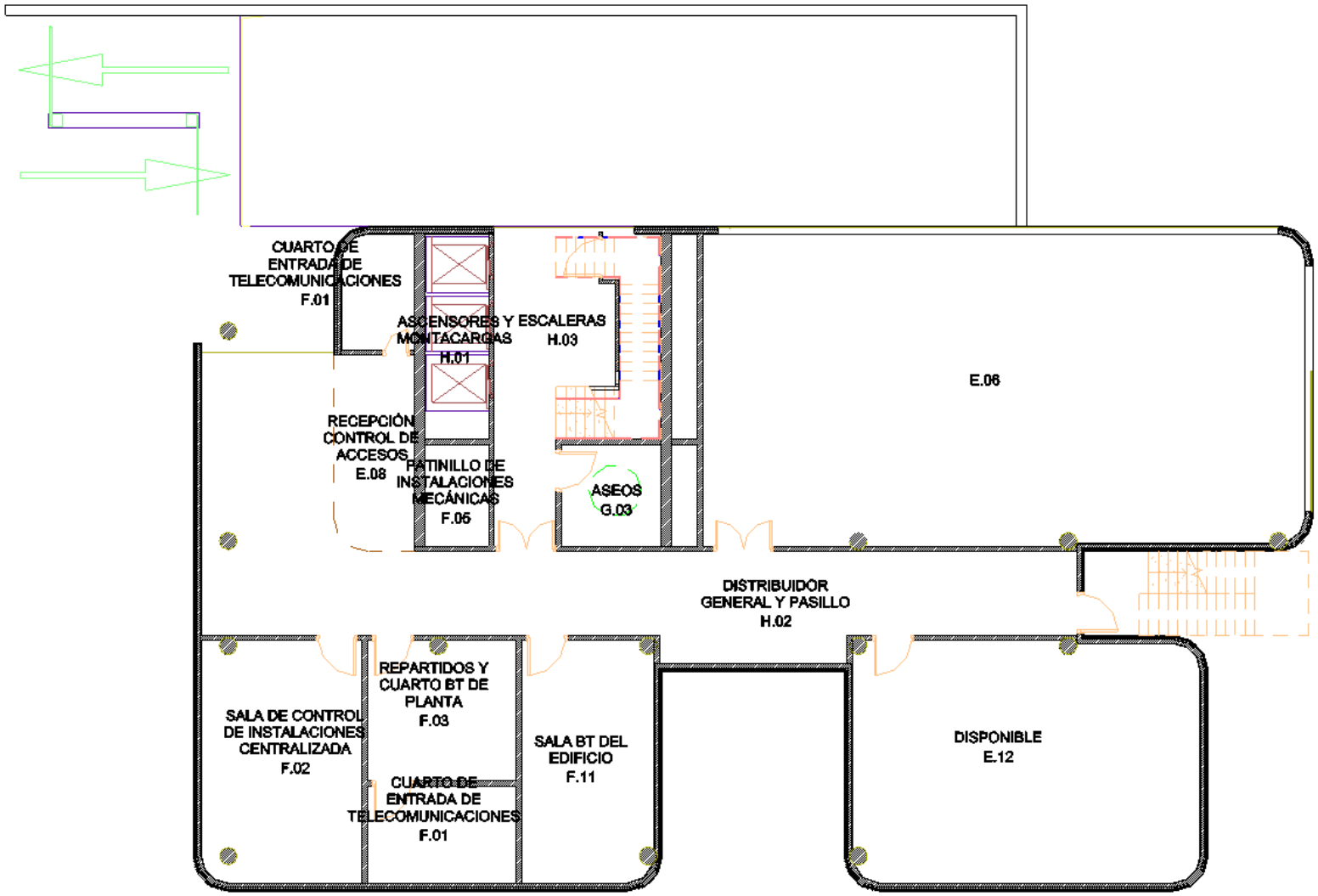

Figura 26. Plano Planta Baja

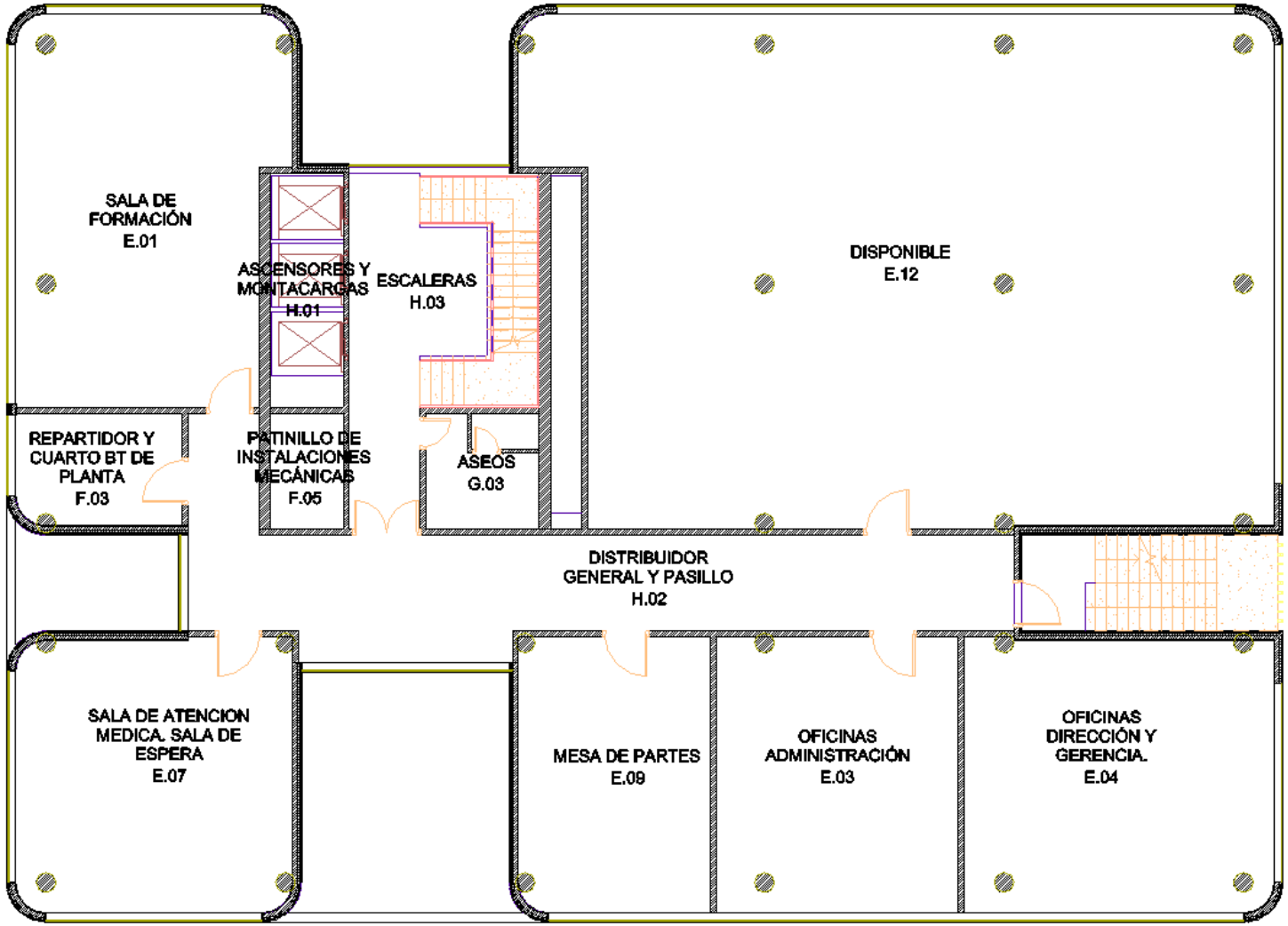

Figura 27. Plano oficinas

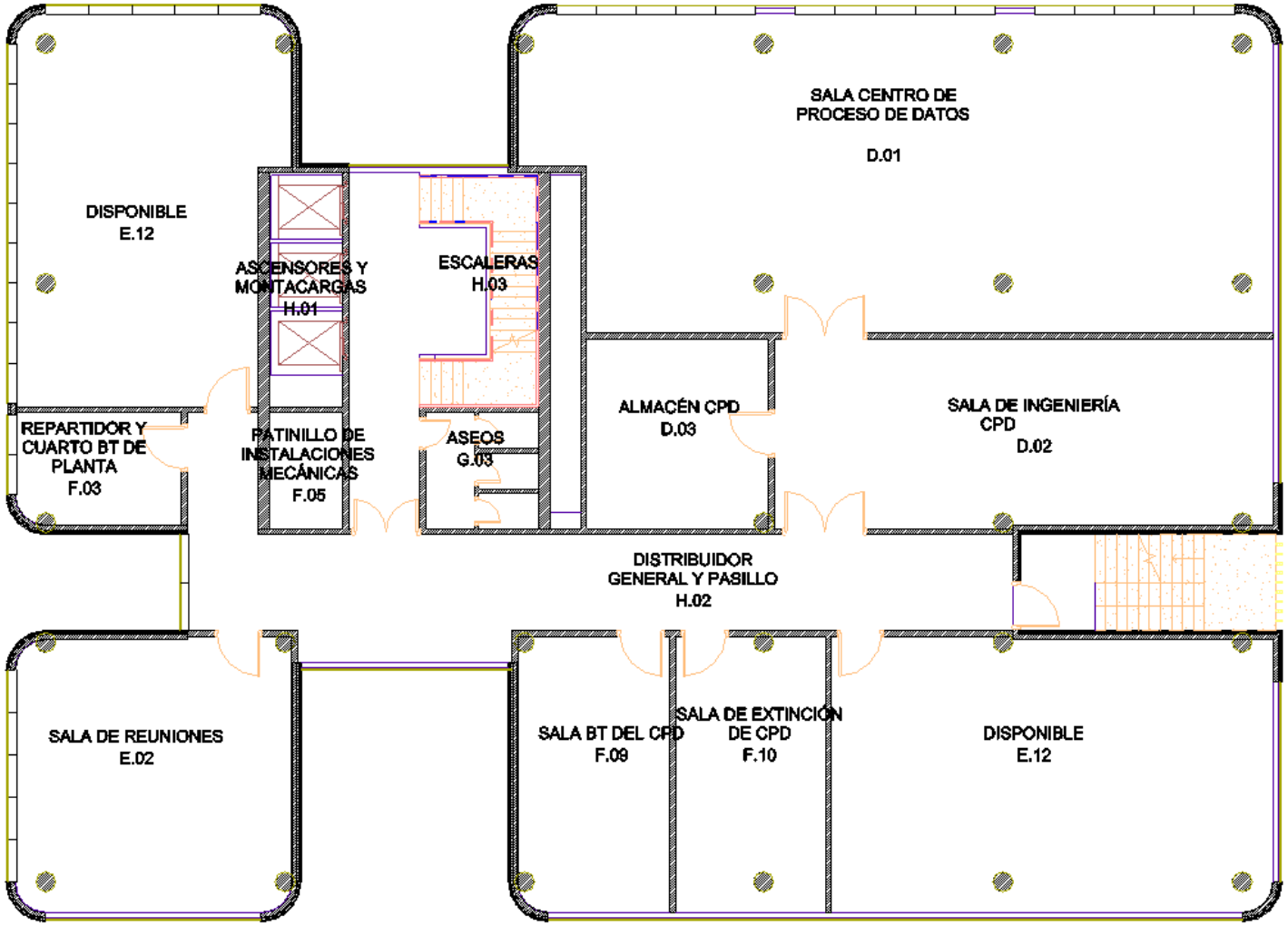

Figura 28. Plano CPD

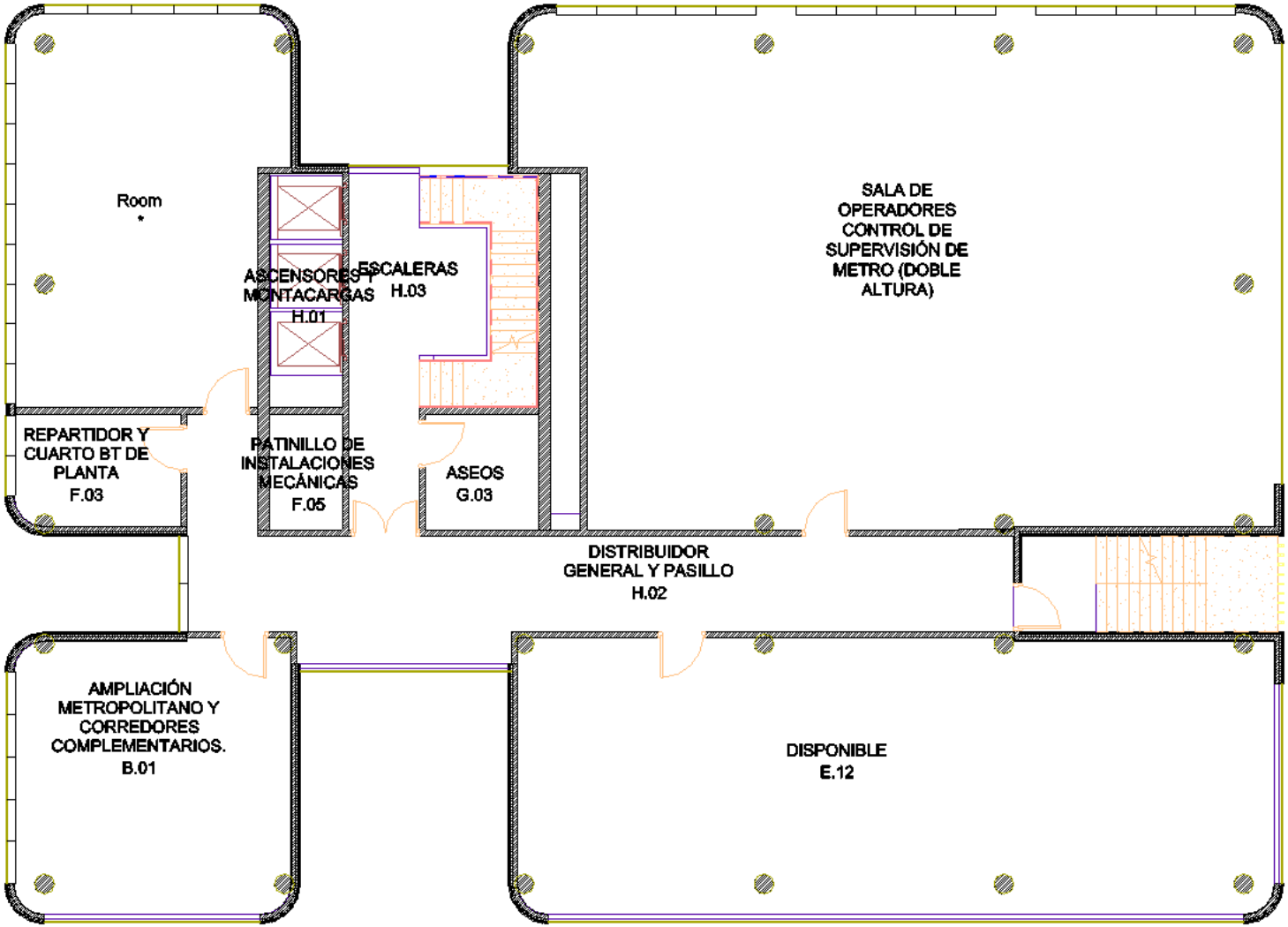

Figura 29. Plano centro de control 1

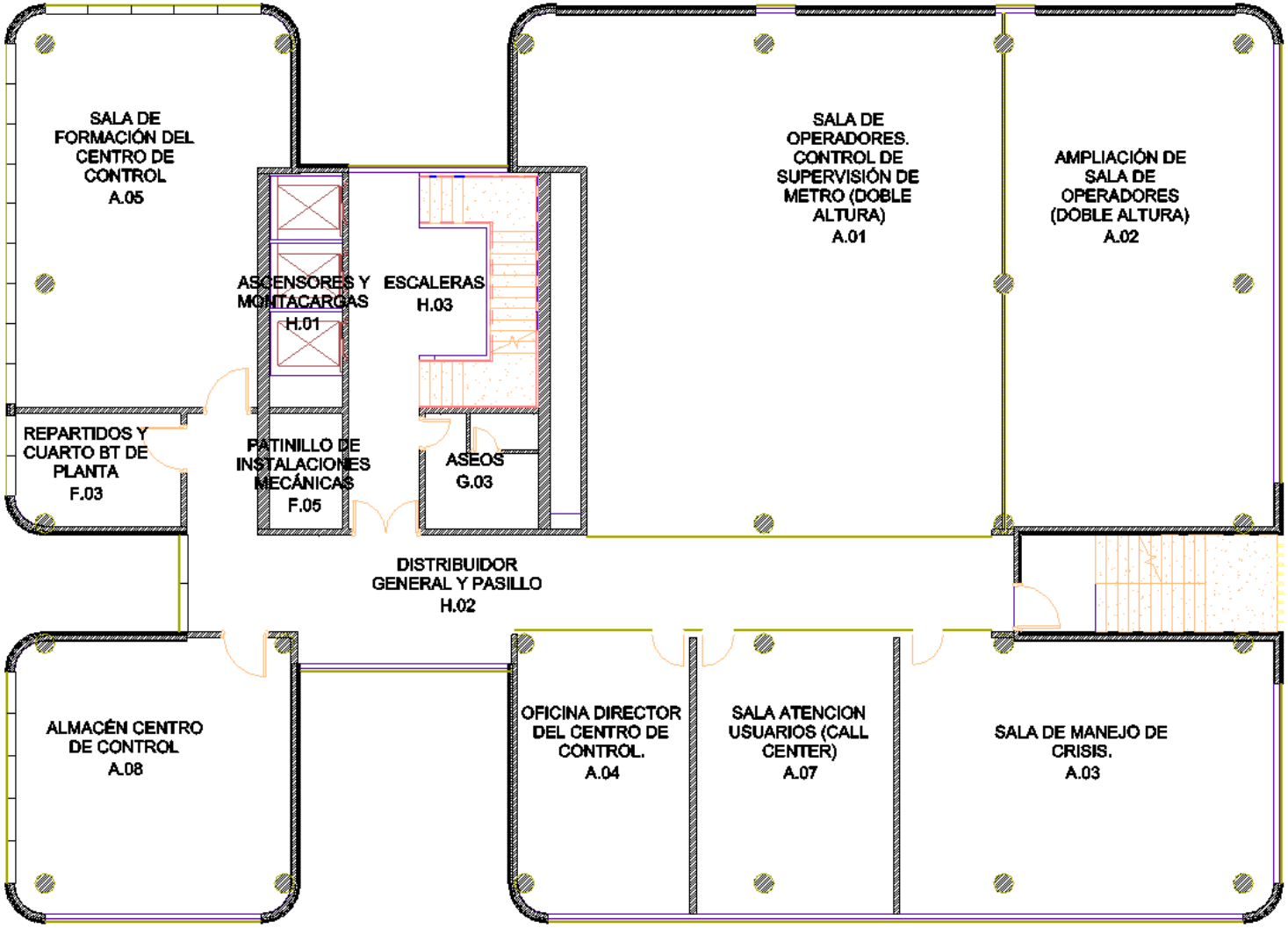

Figura 30. Plano centro de control 2

5.3.1 Definición de zonas.

El paso siguiente es dividir las diferentes plantas del edificio en zonas de seguridad, las clases se dividen en 4 grupos siendo el primero zonas de acceso público o semipúblico, la segunda permitiendo el acceso a personal autorizado por la institución, se le asignara a las oficinas y demás habitaciones de uso común, la tercera se requiere la identificación de los usuarios y se asignara a las diferentes habitaciones de los aparatos de conexión de cada planta y por último la cuarta clase que se reserva a las instalaciones más técnicas, como son el CPD y su almacén y el centro de control y su almacén, este tipo de zonas también requerirá el control de acceso.

El acceso a una zona de nivel alto no significa que se tenga acceso a todas las zonas de clases inferiores.

En la primera planta encontramos que casi toda la planta es de clase 1 ya que este edificio es de acceso semipúblico, dentro de la misma planta encontramos las habitaciones de entrada de las instalaciones de telecomunicaciones y las salas de reparto de equipos y la sala de gestión de seguridad que serán de clase 3 ya que no se encuentran abiertas al público en general ni a todos los trabajadores de las instalaciones.

En la segunda planta encontramos las oficinas por lo que se marcaran como clase 2 ya que, aunque no se encuentran abiertas de normal al público general este puede entrar si es acompañado por alguien responsable que tenga acceso a esta planta, en esta planta solo encontramos una zona de clase 3 que es la sala de reparto de la planta a la que se encontraran conectados los diferentes equipos de la planta.

En la tercera planta encontramos el centro de procesado de datos en la que se encuentra varias zonas de clase 4 siendo las salas de instalaciones de baja tensión y la sala de extinción del centro de control para casos de incendios, por otra parte encontramos las diferentes salas del CPD dividiéndose en la sala de ingeniería en la que se llevara a cabo las diferentes tareas relacionadas con el centro, también se encuentra el almacén y también la misma habitación en la que se encuentra los servidores del CPD, también encontramos una sala de reparto de la planta que será de clase 3, además de esto se encuentran las oficinas del CPD que se corresponden a la clase 2.

En la cuarta planta encontramos el centro de control que cuenta con unas oficinas que se marcaran con clase 2 así como la sala de reparto de equipos de la planta que se marcara con la clase 3, por otra parte, tenemos la sala de supervisión del centro de control que se corresponde con la clase 4 ya que desde este punto se llevaran a cabo operaciones por personal muy especializado.

En la quinta y última planta encontramos más oficinas del centro de control que se corresponderán con una zona de clase 2, aparte también encontramos la sala de reparto que se marcara como clase 3 y también encontramos el almacén del centro de control en el que se encontrarán los recambios del centro de control, esta habitación se corresponde con una clase 4.

A continuación, se muestran los diferentes planos con las zonas explicadas anteriormente.

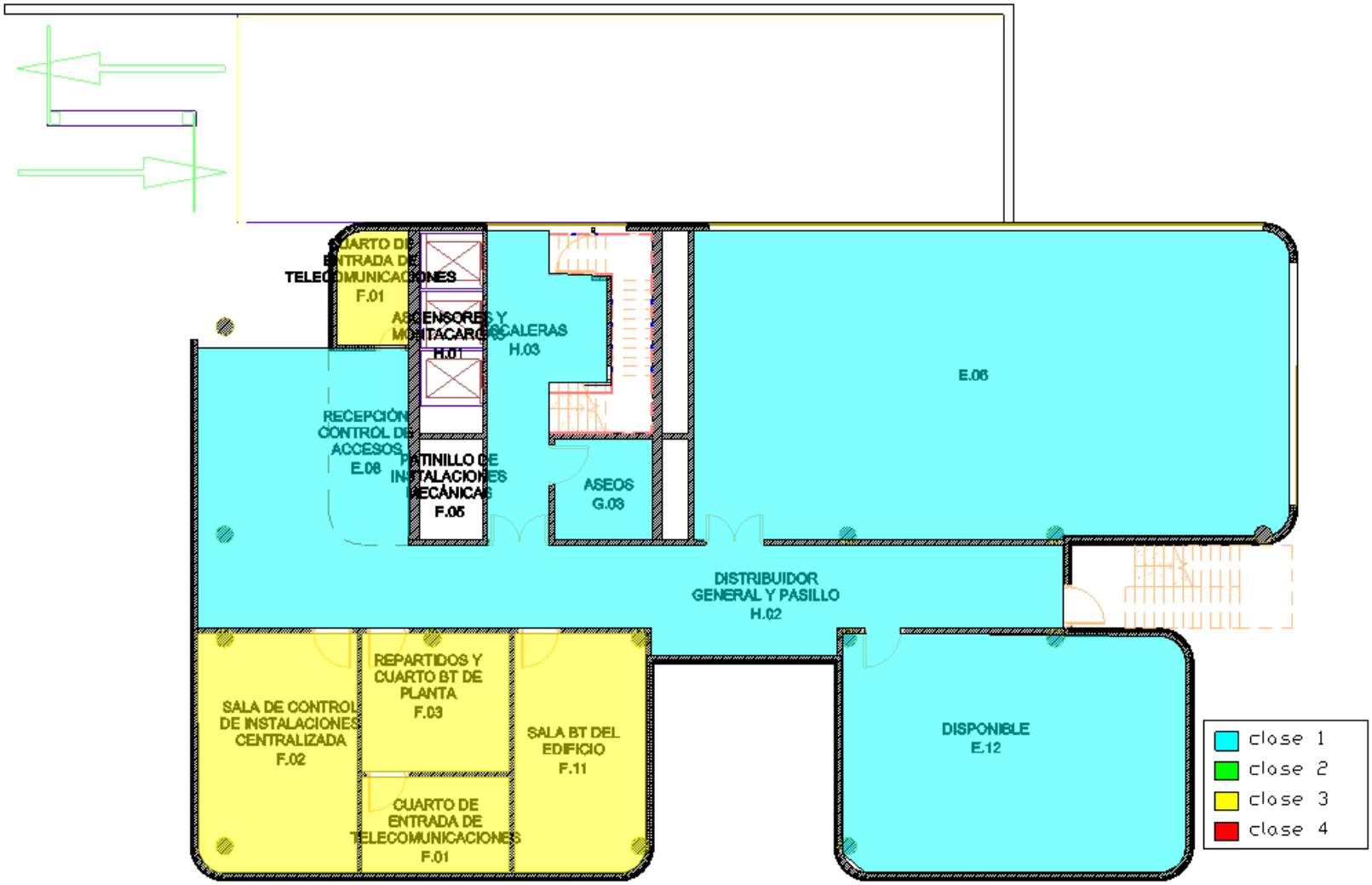

Figura 31. Plano zonas de seguridad planta baja

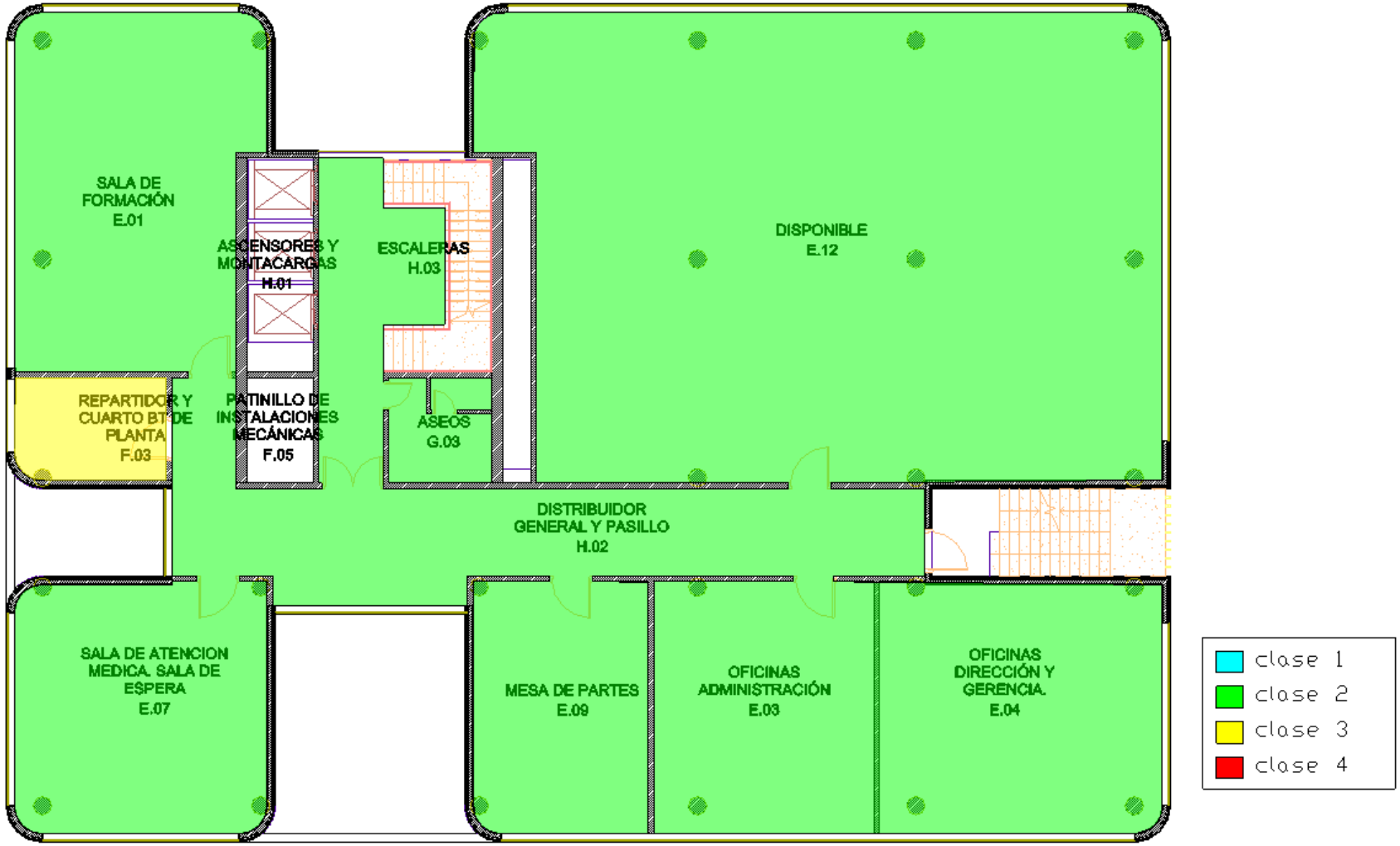

Figura 32. Plano zona oficinas.

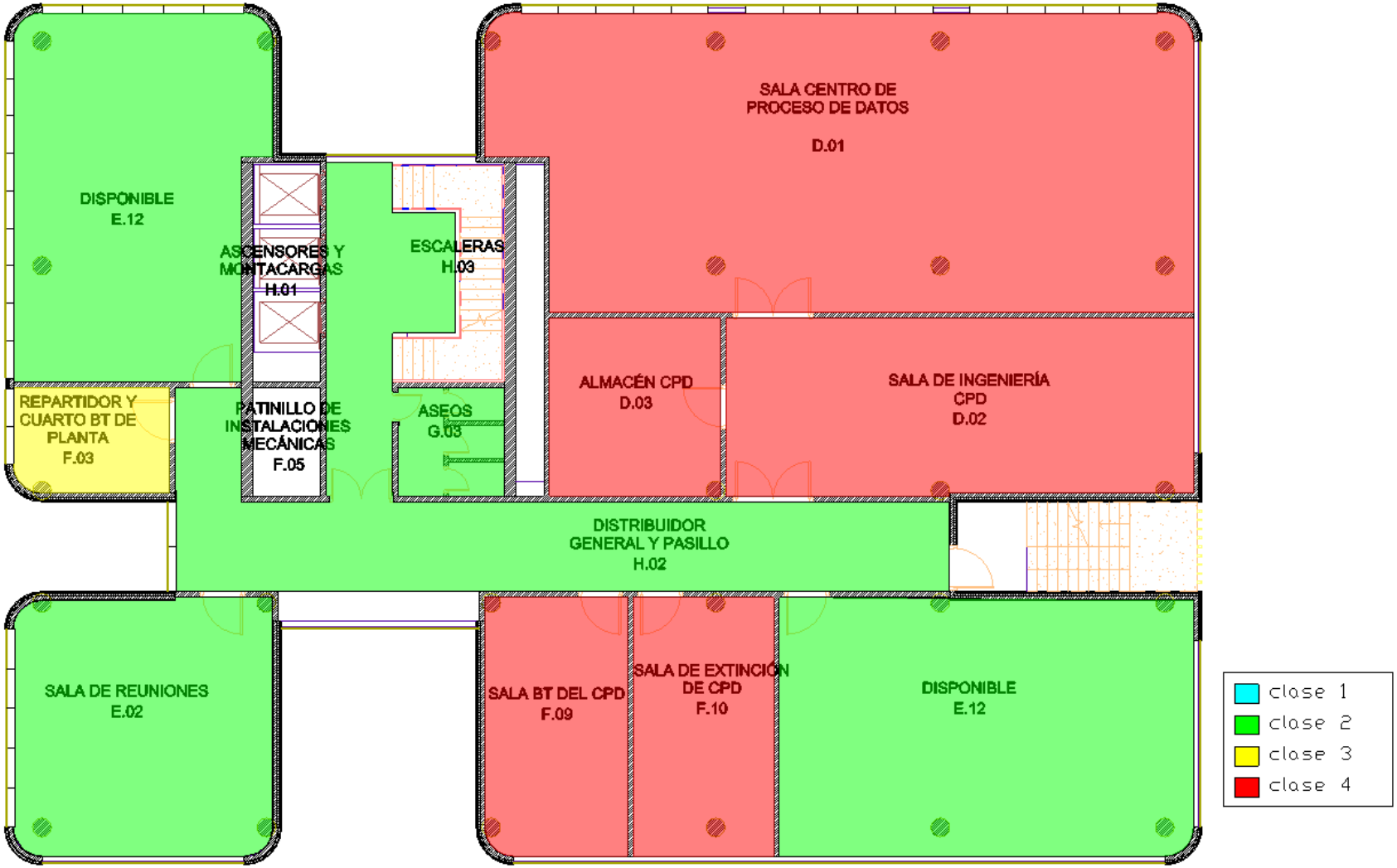

Figura 33. Plano zonas CPD

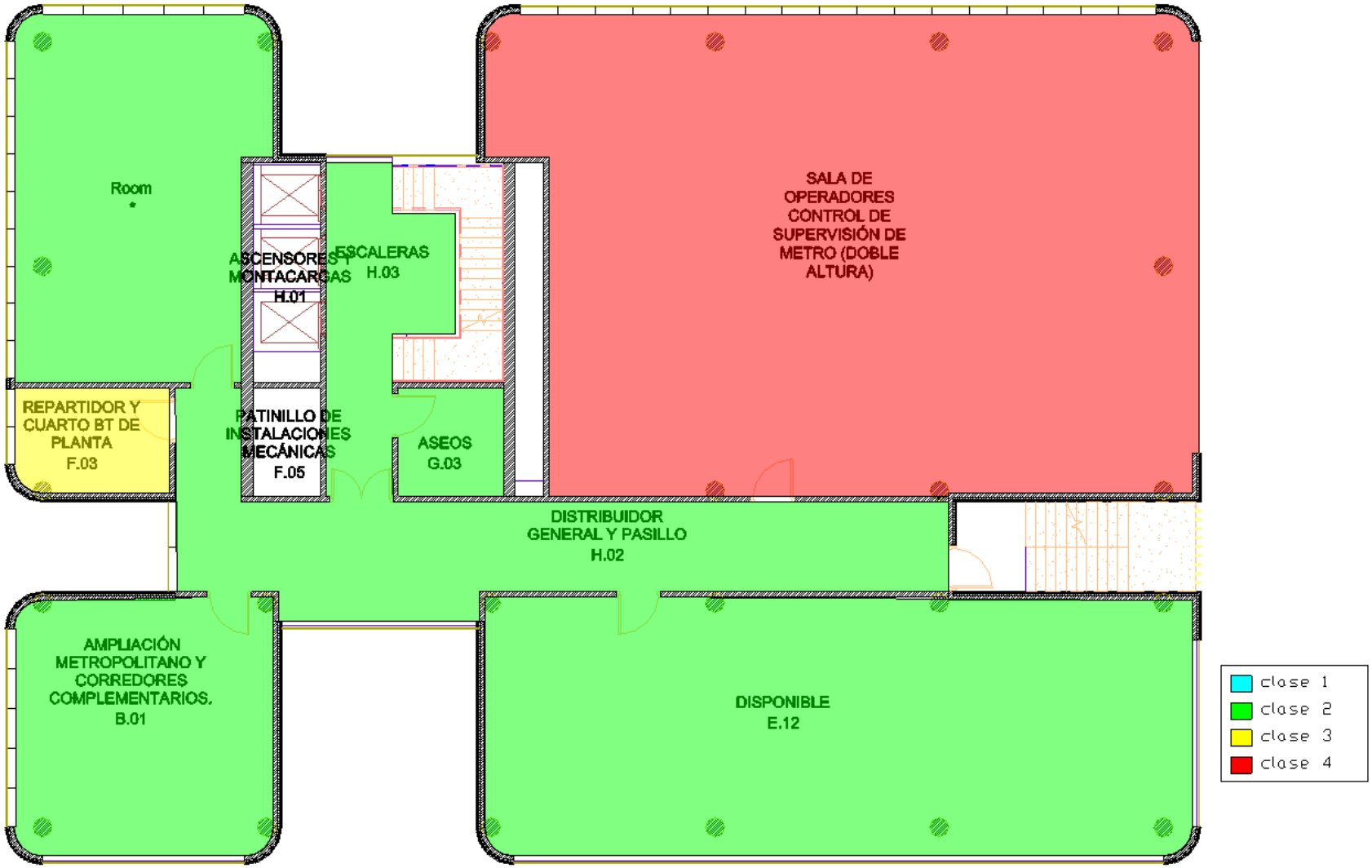

Figura 34. Plano zonas centro de control 1

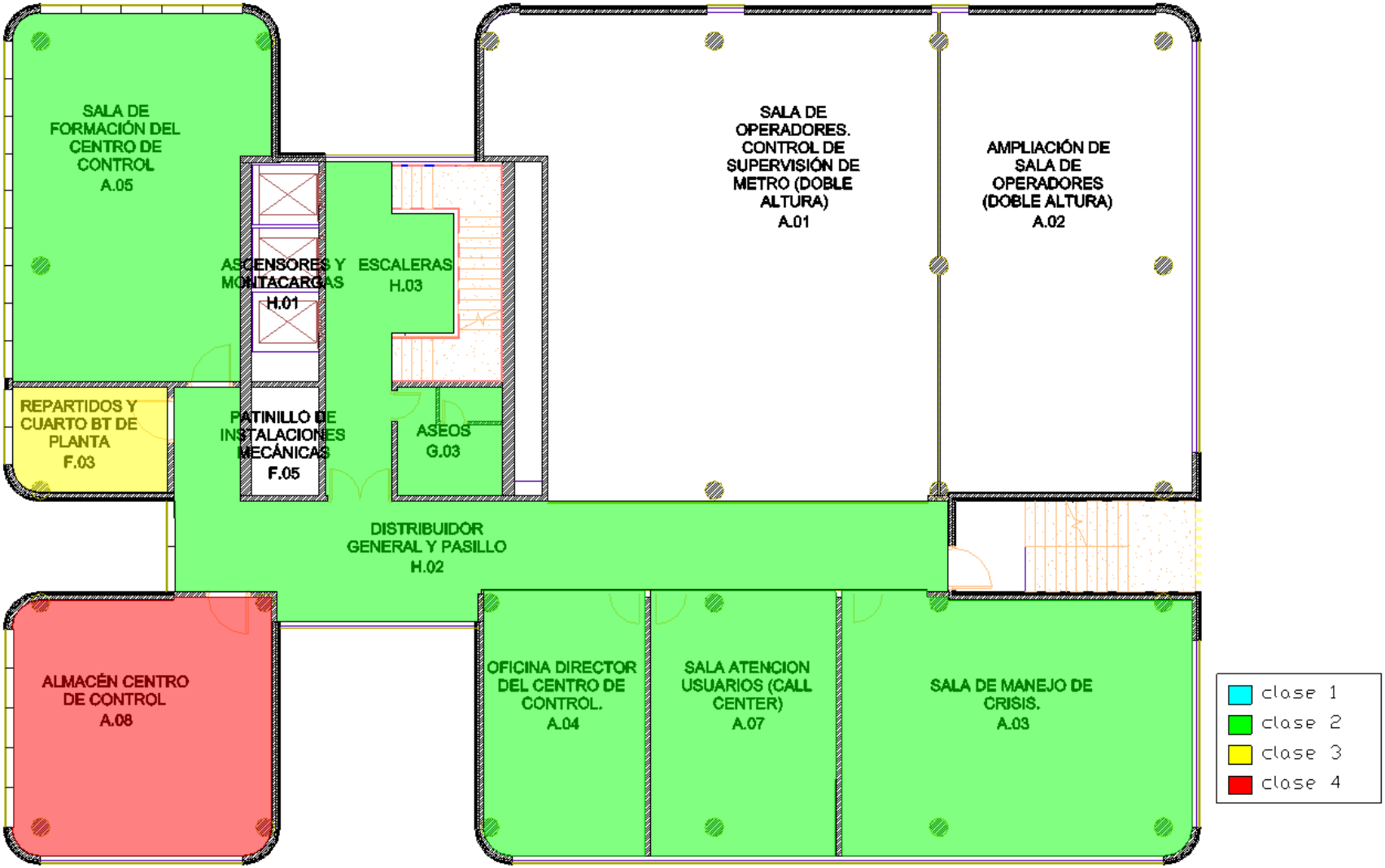

Figura 35. Plano zonas centro de control 2

5.3.2 Equipos instalados.

Los diferentes equipos instalados se dividen en tres grupos, los equipos de control de acceso en los que se encuentran los dispositivos de lectura y los paneles de acceso, en este caso los dispositivos son de dos tipos lectores de tarjetas magnéticas y lectores biométricos, los equipos de CCTV tratándose de cámaras tipo domo al ser instaladas en interiores que se instalaran para vigilar las zonas de tránsito y los equipos de detección de intrusión que se componen de contactos magnéticos para las puertas y detectores volumétricos. Todos estos dispositivos se conectan a través de cableado a el panel de la planta y a su vez estos se encuentran conectados al panel central que se encuentra en la planta baja.

En la primera planta encontramos contactos magnéticos en las puertas de acceso a habitaciones técnicas, así como detectores volumétricos en dichas habitaciones y las demás habitaciones, así como en el pasillo que da acceso a las escaleras, encontramos lectores de tarjeta en las puertas de acceso a los cuartos técnicos y cámaras en la entrada al edificio, el pasillo de acceso a las instalaciones y en las escaleras.

En la segunda planta encontramos detectores volumétricos en las diferentes habitaciones de oficinas y encontramos un contacto magnético junto con un detector volumétrico en la habitación de reparto de la planta, por parte del control de acceso solamente encontramos un lector de tarjetas en la misma habitación de reparte y por último encontramos las cámaras vigilando los diferentes puntos de paso de las escaleras y los pasillos de entrada a las habitaciones.

En la tercera planta nos encontramos con el centro de procesado de datos, esta planta contara con contactos magnéticos tanto en la entrada a la sala de ingeniería del CPD como a su almacén y la sala de servidores, también encontraremos la misma configuración en la sala de extinción y la sala de baja tensión propia del CPD así como en la sala de reparto, encontraremos control de acceso por biometría a las diferentes salas del CPD, estos lectores se instalaran tanto a la entrada como a la salida de las salas y serán independientes unos de otros, las salas de baja tensión, de reparto y extinción se controlara el acceso con tarjeta y las cámaras se instalaran en las zonas de transito de acceso a las diferentes salas , en las escaleras, en la zona del almacén del CPD y se llevara a cabo la instalación en la sala de servidores de dos cámaras para poder conseguir una visión en caso de cualquier detección de movimiento por parte de los sensores volumétricos.

En la cuarta planta encontramos contactos magnéticos y detectores volumétricos en todas las habitaciones, en el control de acceso se instalará un control de acceso a la sala de reparto con lector de tarjetas y un lector biométrico para el acceso a la sala de control, este último será tanto de entrada como de salida y se instalaran cámaras en las diferentes zonas de tránsito.

En la quinta planta encontramos contactos magnéticos en las habitaciones y en la puerta de entrada a la planta, esto se instalara junto a un lector de tarjetas debido a la existencia de una zona acristalada desde la que se puede observar el centro de control, se llevara a cabo también la instalación de un lector de tarjetas en la habitación de reparto y un lector biométrico en el almacén del centro de control y se instalaran cámaras en las zonas de tránsito y en dicho almacén.

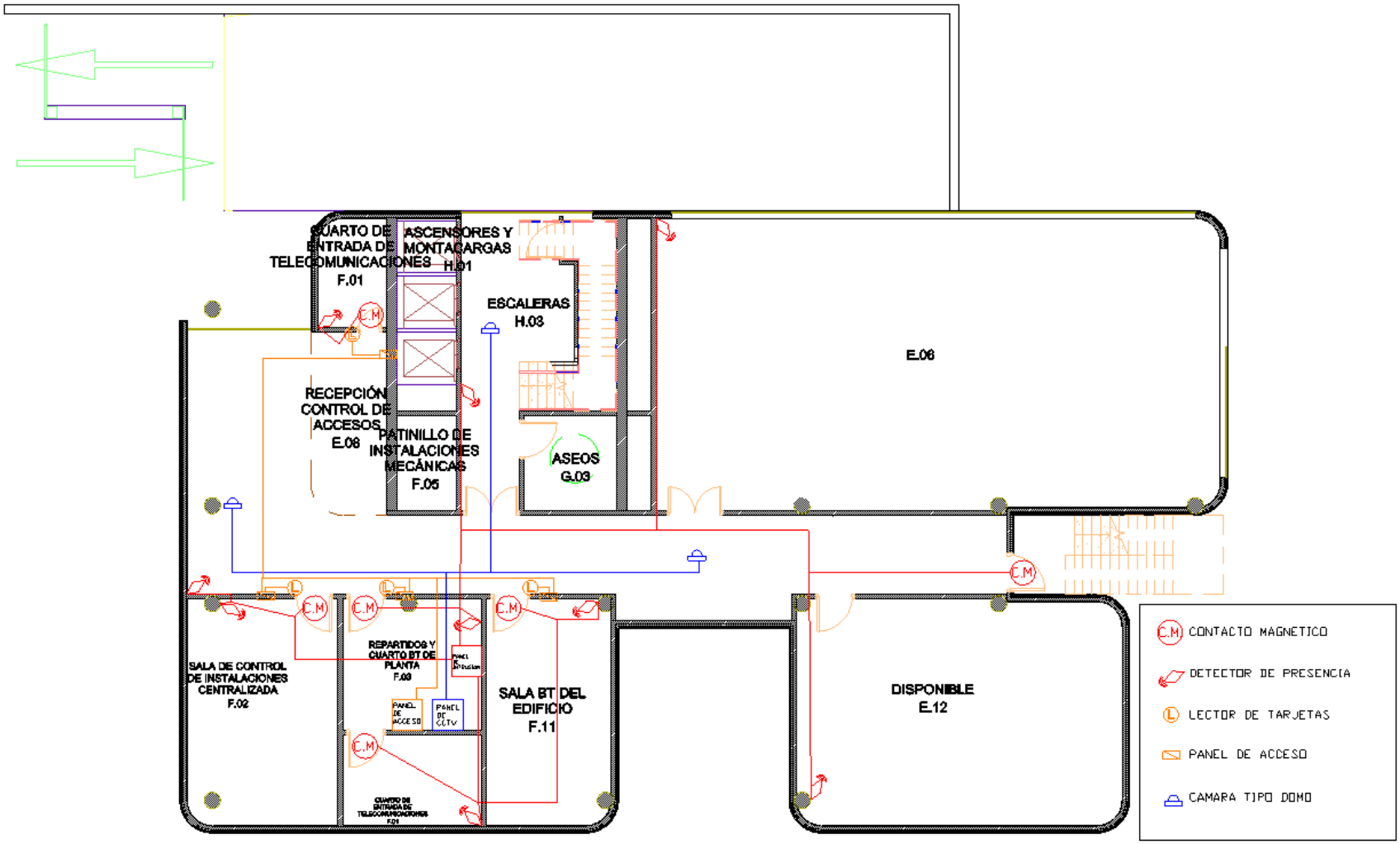

Figura 36. Plano dispositivos planta baja

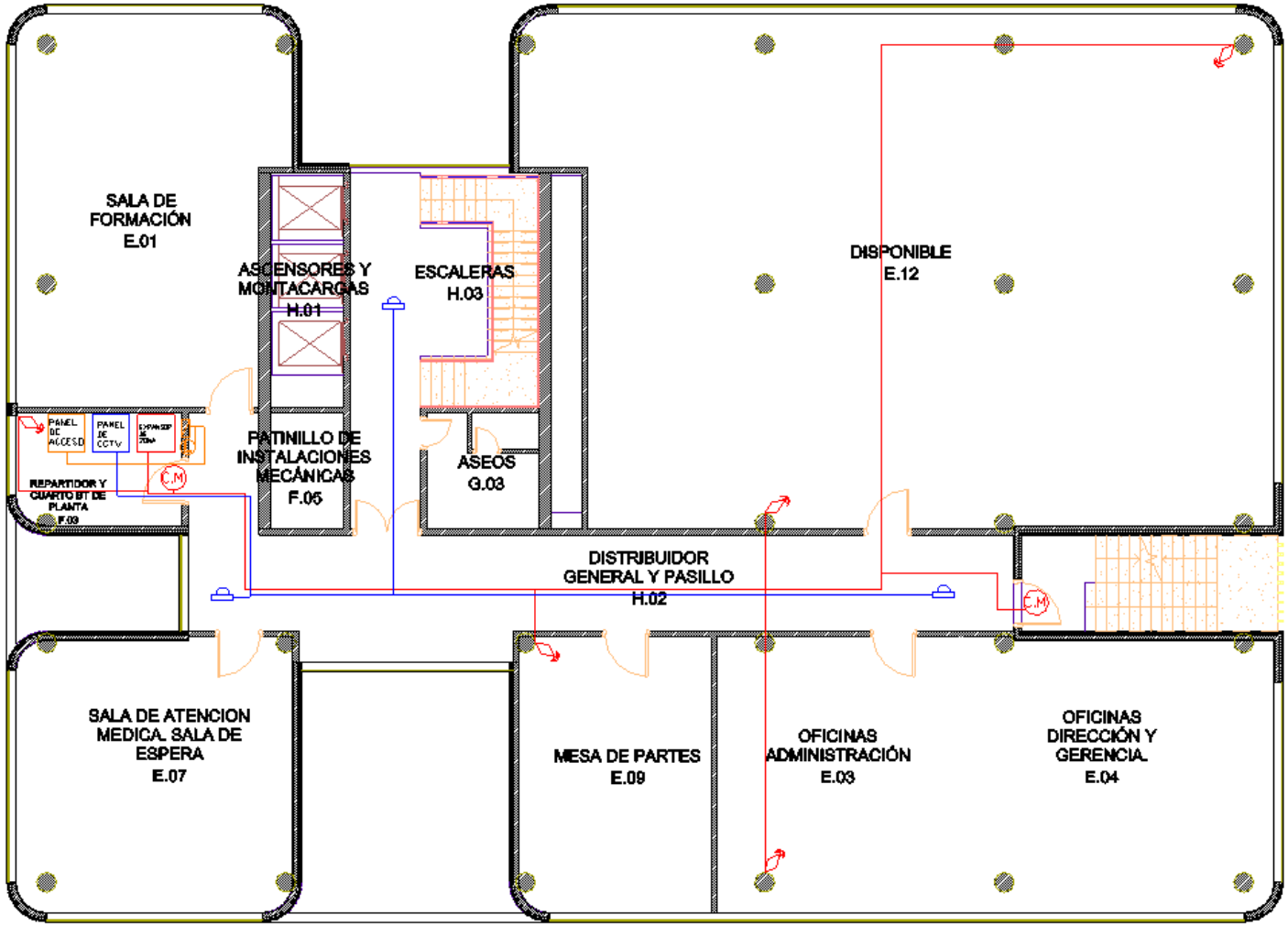

Figura 37. Plano dispositivos oficinas

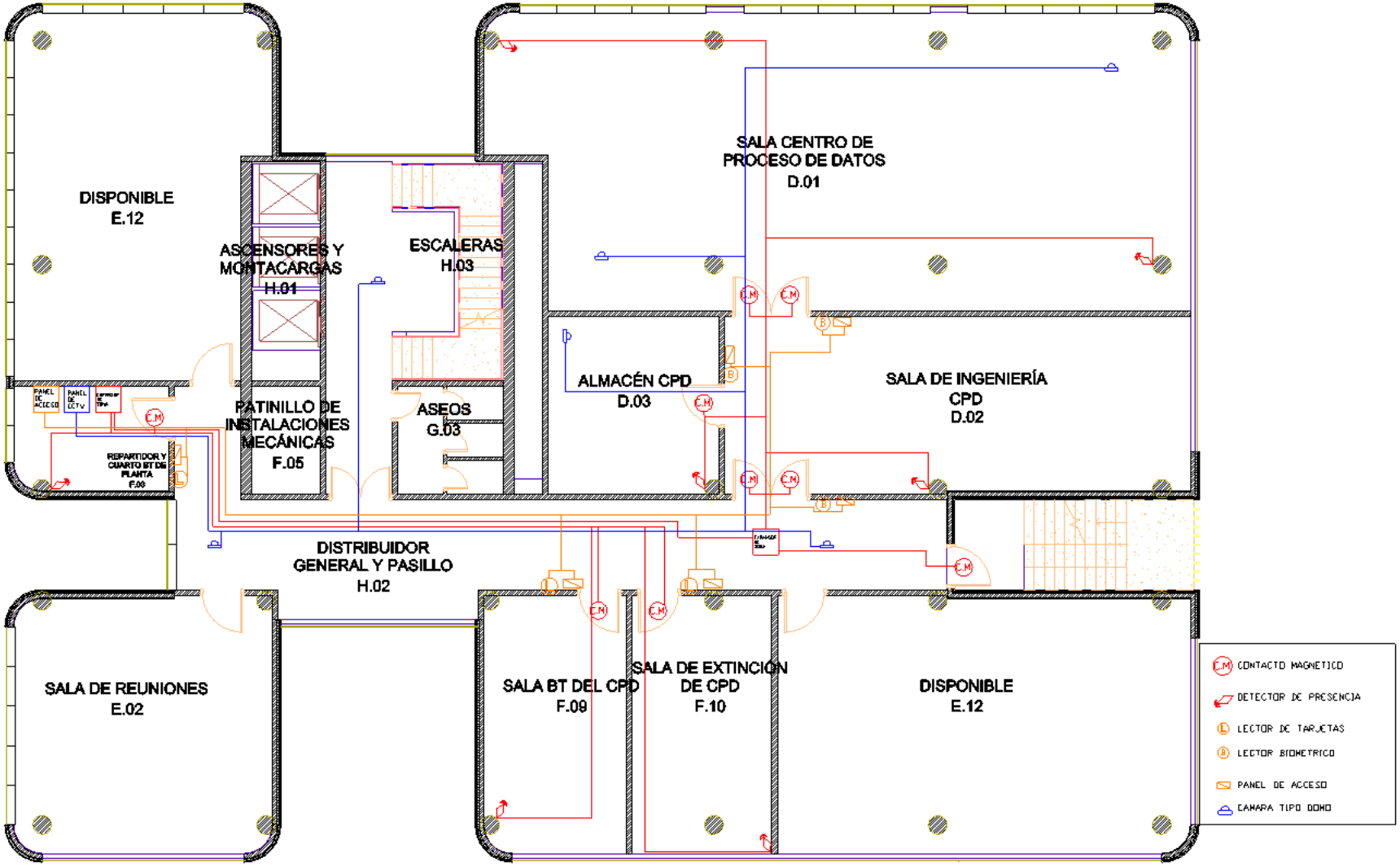

Figura 38. Plano dispositivos CPD

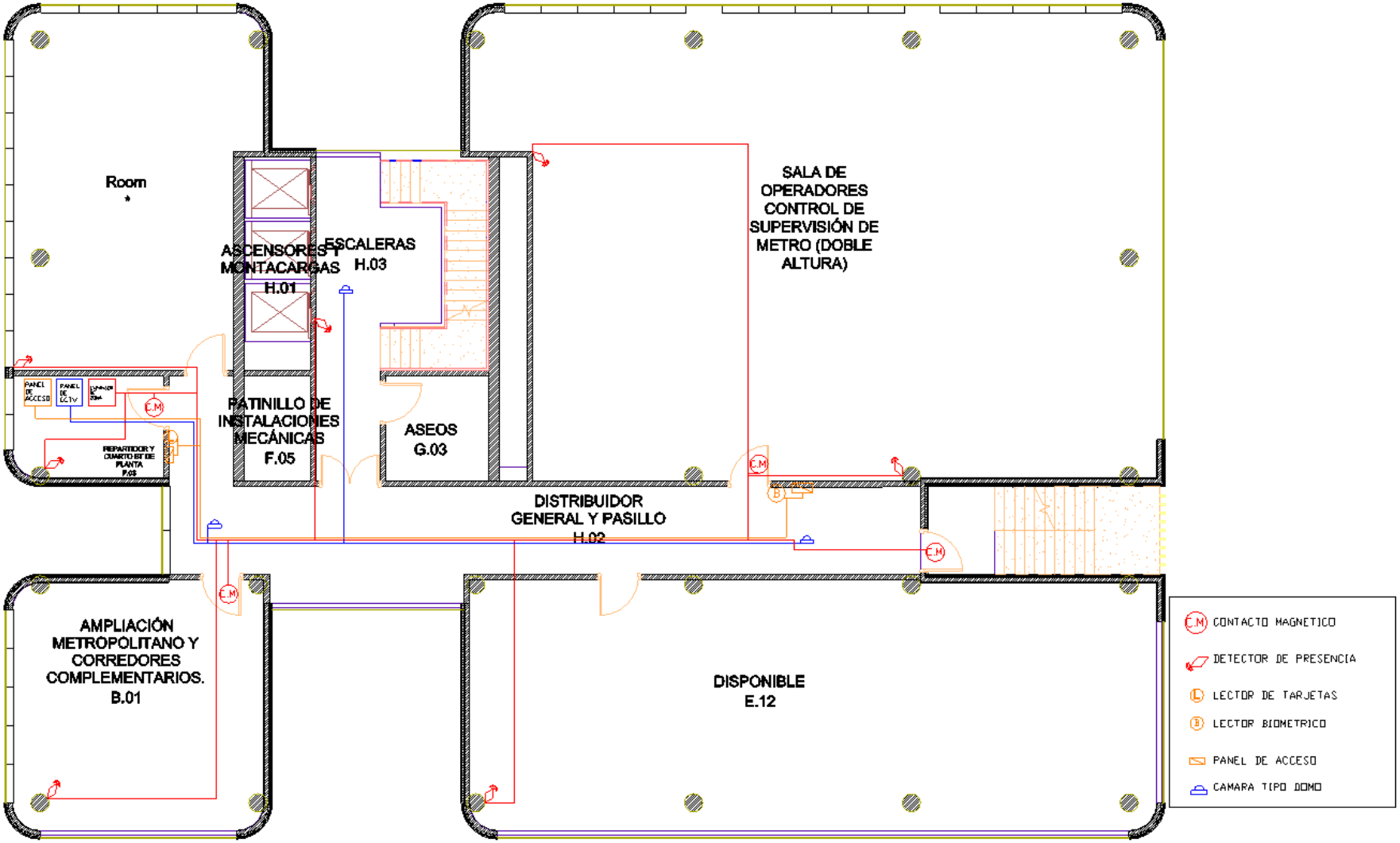

Figura 39.Plano dispositivos centro de control 1

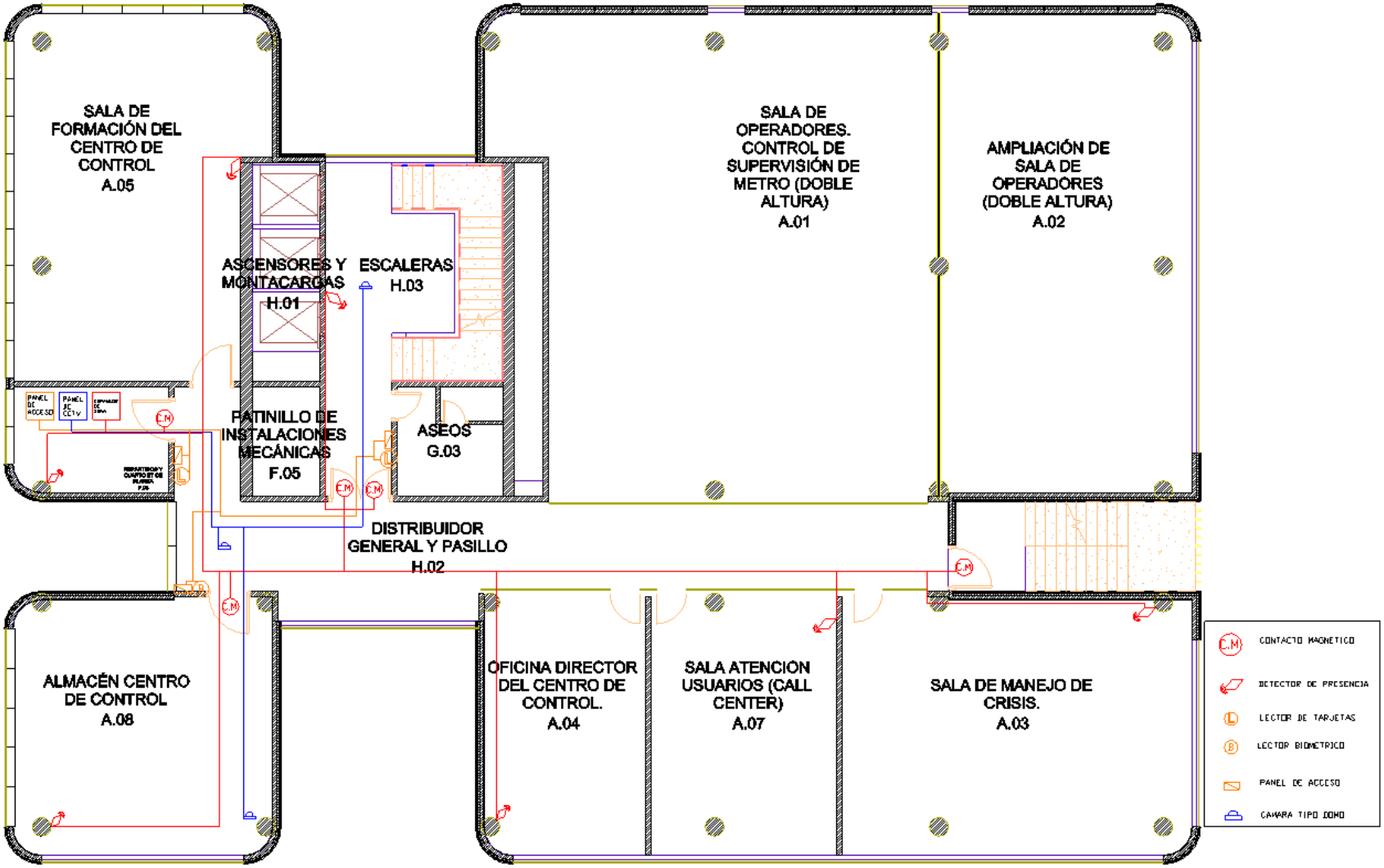

Figura 40. Plano dispositivos centro de control 2

Capítulo 6. Futuro trabajo.

Una vez confirmado que el sistema funciona correctamente se tendría que continuar implementando continuamente el bucle PHVA, uno de los dispositivos más importante a desarrollar una vez se ha establecido el funcionamiento correcto del sistema es una HoneyPot o una HoneyNet, esto se hace posteriormente al funcionamiento del sistema debido a la peculiaridad de estos sistemas, ya que en caso de no funcionar correctamente el sistema presentaría problemas graves de seguridad.

Por tanto, en un futuro se podría llevar a cabo el diseño de una HoneyNet que intente engañar a los posibles atacantes de la red interna.

Estos dispositivos serian instalados en la DMZ de conexión con la red externa.

Capítulo 7. Bibliografía

[1] Asociación Española de Normalización y Certificación, "tecnología de la información – Infraestructuras e instalaciones de centros de datos- Parte 2-5: Sistemas de seguridad".

[2] Centro criptológico nacional CN-CERT, "Ciberamenazas y Tendencias". https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html

[3] Gobierno de españa ministerio de la presidencia, relaciones con las cortes e igualdad, "Estrategia nacional de ciberseguridad". https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf

[4] Ozgur Depren; Murat Topallar; Emin Anarim; M. Kemal Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks" https://doi.org/10.1016/j.eswa.2005.05.002.

[5] H. Ling-Fang, "The Firewall Technology Study of Network Perimeter Security," 2012 IEEE Asia-Pacific Services Computing Conference, Guilin, 2012, pp. 410-413, doi: 10.1109/APSCC.2012.23.

[6] G. A. Marin, "Network security basics," in IEEE Security & Privacy, vol. 3, no. 6, pp. 68-72, Nov.-Dec. 2005, doi: 10.1109/MSP.2005.153.

[7] Rafeeq Ur Rehman. "Intrusion Detection Systems with Snort" https://books.google.es/books?id=1WKrLbh23LAC&lpg=PA1&dq=IDS%20systems&lr&hl=ca&pg=PP1#v=onepage&q=IDS%20systems&f=false

[8] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E.Vazquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges. https://doi.org/10.1016/j.cose.2008.08.003

[9] I. Kotenko and A. Chechulin, "Common Framework for Attack Modeling and Security Evaluation in SIEM Systems," *2012 IEEE International Conference on Green Computing and Communications*, Besancon, 2012, pp. 94-101, doi: 10.1109/GreenCom.2012.24.

[10] M. Ali Aydin, A. Halim Zaim, K. Gökhan Ceylan. "A hybrid intrusion detection system design for computer network security" https://doi.org/10.1016/j.compeleceng.2008.12.005

[11] Guillermo Suarez-Tangil, Esther Palomar, Arturo Ribagorda, Ivan Sanz. "Providing SIEM systems with self-adaptation" https://doi.org/10.1016/j.inffus.2013.04.009

[12] S. Bhatt, P. K. Manadhata and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," in *IEEE Security & Privacy*, vol. 12, no. 5, pp. 35-41, Sept.-Oct. 2014, doi: 10.1109/MSP.2014.103

[13] E. Novikova and I. Kotenko, "Analytical Visualization Techniques for Security Information and Event Management," 2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, Belfast, 2013, pp. 519-525, doi: 10.1109/PDP.2013.84.

[14] M. Khonji, Y. Iraqi and A. Jones, "Phishing Detection: A Literature Survey," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091-2121, Fourth Quarter 2013, doi: 10.1109/SURV.2013.032213.00009.

[15] Cesario Di sarno, Alessia Garofalo, Ilaria Matteucci, Marco Vallini. "A novel security information and evento management system for enhancing cyber security in a hydroelectric dam". https://doi.org/10.1016/j.ijcip.2016.03.002.

[16] Cisco Systems, "Firewall Fundamentals". https://books.google.es/books?hl=ca&lr=&id=meUzVLMQMJ4C&oi=fnd&pg=PT28&dq=fire

wall+types&ots=yECQhpZxxD&sig=-ltPuKdLSGc4fu0nKAXtESo5gZ8&redir_esc=y#v=onepage&q&f=false

[17] Mohamed G. Gouda, Alex X. Liu, "Structured firewall design". https://doi.org/10.1016/j.comnet.2006.06.015

[18] C. L. Schuba and E. H. Spafford, "A reference model for firewall technology," Proceedings 13th Annual Computer Security Applications Conference, San Diego, CA, USA, 1997, pp. 133-145, doi: 10.1109/CSAC.1997.646183.

[19] Srinivas Mukkamala, Andrew Sung, Ajith Abraham. "Cyber-Security Challenges: Designing Efficient Intrusion Detection Systems and Anti-Virus Tools". https://books.google.es/books?hl=ca&lr=&id=egnOBQAAQBAJ&oi=fnd&pg=PA125&dq=antivirus+software+%22intrusion+detection+systems%22&ots=kJfTmTH4yF&sig=OkfmUS0Id_Nw8GMN-xLGdCOn2tg&redir_esc=y#v=onepage&q=antivirus%20software%20%22intrusion%20detection%20systems%22&f=false

[20] Haining Wang, Danlu Zhang and K. G. Shin, "Change-point monitoring for the detection of DoS attacks," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 4, pp. 193-208, Oct.-Dec. 2004, doi: 10.1109/TDSC.2004.34.

[21] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, 2011, pp. 380-388, doi: 10.1109/iThings/CPSCom.2011.34.

[22] Cisco Systems. "Cisco Router Firewall Security". https://books.google.es/books?hl=ca&lr=&id=s2GVAwAAQBAJ&oi=fnd&pg=PT36&dq=firewall+security&ots=5SQsmXGT5Z&sig=Rx_gGCm0tSNCovi3qvspCXMHVYY&redir_esc=y#v=onepage&q=firewall%20security&f=false

[23] A. Nicholson, S.Webber, S.Dyer, T. Patel, H. Janicke, "SCADA security in the light of Cyber-Warfare". https://doi.org/10.1016/j.cose.2012.02.009

[24] Colin Tankard, "Advanced Persistent threaths and how to monitor and deter them". https://doi.org/10.1016/S1353-4858(11)70086-1

[25] Georg Disterer. "ISO/IEC 27000, 27001 and 27002 for Information Security Management". https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf

[26] Ireneusz Tarnowski "How to use cyber kill chain model to build cybersecurity?". https://www.eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf

[27] Michael J. Assante, Robert M. Lee "The Industrial Control System Cyber Kill Chain". https://scadahacker.com/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf

[28] COIT y AEIT, "bit. Ciberseguridad Tecnología segura para un mundo en cambio continuo"

https://www.coit.es/sites/default/files/bit217.pdf

[29] L. Spitzner, "Honeypots: catching the insider threat," 19th Annual Computer Security Applications Conference, 2003. Proceedings., Las Vegas, NV, USA, 2003, pp. 170-179, doi: 10.1109/CSAC.2003.1254322.

[30] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html

[31] A. C. Weaver, "Biometric authentication," in *Computer*, vol. 39, no. 2, pp. 96-97, Feb. 2006, doi: 10.1109/MC.2006.47. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1597098&isnumber=33586

[32] Debnath Bhattacharyya, "Biometric Authentication: A review". https://www.biometrie-online.net/images/stories/dossiers/generalites/International-Journal-of-u-and-e-Service-Science-and-Technology.pdf