Marco NormativoHuescaTelecom



Eduardo Villacampa Escartín  
2023

# Introducción

1. **Descripción de la organización**

1.1. Ámbito de negocio

HuescaTelecom empresa dedicada al sector de las comunicaciones. Ofrece servicios de instalación de equipos informáticos y de telecomunicaciones, así como el mantenimiento y reparación de los mismos. Además, es una empresa distribuidora de Movistar, por lo que ofrece los servicios de la misma (altas/bajas de clientes, reparación de equipos de Movistar, atención al cliente, etc).

Para ofrecer el servicio la empresa cuenta con una sede principal, donde se encuentran todos los departamentos de la empresa, así como una tienda de todo tipo de productos relacionados con las telecomunicaciones. A su vez posee 6 sedes secundarias en distintas localidades y un almacén en el que se guardan los bienes de la empresa. Cuenta con un total de 30 empleados.

La empresa cuenta con una página web donde aparece cierta información de la empresa, como: dirección, teléfono de contacto, dirección de correo electrónico, localización, trabajadores de la empresa, trabajos realizados, entidades colaboradoras…

1.2. Organigrama de la empresa

* Departamento de seguridad: Se encarga de la seguridad física y lógica de la empresa. Sobre este recae la total responsabilidad sobre la seguridad de la empresa.
* Departamento de comercio: Se encarga del servicio de cara al público, es decir, controla la venta de los productos en las tiendas, así como el servicio postventa. A su vez se encarga de distribuir la marca Movistar a través de las tiendas y de la página web de la empresa. Gestión de clientes.
* Departamento recursos humanos: Se encarga de la gestión de empleados (altas, bajas, renovaciones, etc). Los trabajadores de este departamento se encargan de el compliance empresarial.
* Departamento de operaciones: Se encarga de controlar todo el trabajo de los instaladores (donde tienen que ir, cuando, a qué…) así como el trabajo del taller. A su vez se encarga de la gestión de la infraestructura de la empresa (mantenimiento, renovación, etc).
* Departamento de finanzas: su función es el control de las compras y ventas de los bienes de la empresa (compra de productos destinados a instalaciones, venta al público, etc) así como la gestión financiera de la empresa (facturas, informes financieros, contratos, proveedores…).
* **Departamento de informática:** se encarga de gestionar tanto el software como el hardware informático utilizado en la empresa. Gestionan el NAS, la página web, las redes internas de la empresa, etc. Parte de este departamento trabaja en la seguridad informática de la empresa bajo el responsable de ciberseguridad.

1.3. Descripción de las sedes

* **Sede principal:** En ella se desarrolla la mayor parte del trabajo de la empresa (sin contar instalaciones). Se encuentran todos los departamentos (Dirección, Compras, Ventas…). Además, cuenta con un taller donde se realiza el mantenimiento de los equipos de los clientes, y una tienda donde se venden los productos y se atiende al cliente.

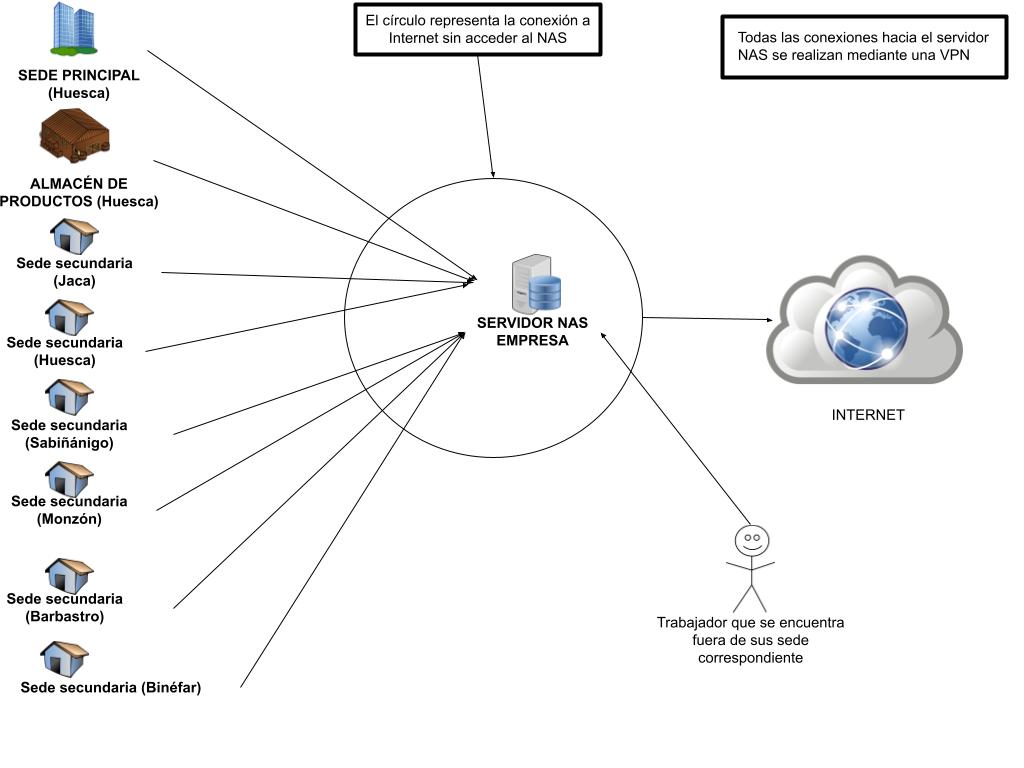
En ella se encuentra la sala en la que se almacena toda la información de la empresa, tanto en papel como en formato digital. A esta sala se accede mediante una tarjeta RFID que identifica a la persona que accede a ella. Dependiendo del puesto de trabajo del mismo, este tendrá acceso o no a cierta información.

Los documentos en formato papel se encuentran almacenados en unos armarios con cerradura. Dependiendo la información que contienen estos documentos estarán localizados en un armario u otro, facilitando así su forma de acceso y evitando que ciertos trabajadores tengan acceso a información que no necesitan saber.

En esta sala también se encuentran los elementos que controlan el CCTV de la sede principal (grabadores, monitores, discos duros…). Las grabaciones son almacenadas tanto en el grabador como en la nube, donde permanecen almacenadas un total de 7 días. Pasado este tiempo, las imágenes se borran automáticamente salvo que se quiera que no se borren, algo que solo puede decidir el director de la empresa. Únicamente tienen acceso a los discos duros con las grabaciones el director general y el director de operaciones.

* **Sedes secundarias:** Total de 6. Son tiendas de Movistar, donde se venden teléfonos móviles y se da servicio al cliente de Movistar. Permiten la recogida de equipos para su reparación (estos productos se envían a la sede principal para ser reparados). Poseen un CCTV y alarmas conectadas a la policía.
* **Almacén:** En ella se almacenan los equipos y elementos destinados a las distintas instalaciones, así como los vehículos de los instaladores de la empresa. Posee un CCTV y alarma conectada a la policía.

1.4. Esquema de sedes

A continuación se observa un esquema de red de las sedes que componen la empresa, y posteriormente se describen los servicios que ofrece cada una de ellas:

SERVICIOS QUE OFRECE CADA SEDE:

* Sede principal: En ella se gestionan todos los departamentos de la empresa. Posee un taller para arreglar equipos averiados, una tienda para venta de productos electrónicos y ofrecer el servicio de Movistar. A su vez posee la sala que se encarga de alojar toda la documentación de la empresa, tanto en formato digital como en formato papel.
* Sedes secundarias: Son tiendas en las que se venden productos electrónicos, se ofrece el servicio de Movistar y donde los clientes pueden dejar equipos averiados para ser arreglados en el taller de la sede principal.
* Almacén: Se almacenan tanto los vehículos usados por los instaladores y comerciales como los equipos destinados a las instalaciones y a la venta directa al público mediante las tiendas.

1. **ACTIVOS DE LA EMPRESA**

* ACTIVOS DE ALTO NIVEL
* Los **documentos de la empresa** están almacenados tanto en formato papel (en una sala localizada en la sede principal de la empresa, donde se accede mediante una tarjeta que identifica a quien accede a ella) como en formato digital en un NAS (localizado en la misma sala) al que los diferentes trabajadores se conectan mediante una VPN con sus credenciales. Dependiendo del puesto del trabajador este tiene acceso a determinada información.
* Los **equipos destinados a instalaciones** se encuentran localizados tanto en el almacén como en la sede principal. El almacén cuenta con una alarma conectada a la policía.
* Los **equipos destinados a la venta** al consumidor se localizan en sus tiendas correspondientes, y en menor medida, en el almacén de la empresa.
* Los **vehículos** que utilizan los instaladores se encuentran en el almacén. Llevan un GPS instalado por el que se puede saber la localización de estos en tiempo real.
* El **software** creado para realizar el inventario de los bienes de la empresa, la gestión de averías, las altas y bajas de clientes de Movistar, la emisión de facturas… Este software se encuentra instalado en el NAS de la empresa.
* La **sala** donde se almacena la información, el NAS, los elementos del CCTV y los servidores de la red corporativa de la empresa.. Es la parte que requiere más seguridad de la empresa, ya que en ella se encuentran todos los documentos confidenciales de la empresa. Esta sala no permite la entrada de agua y fuego, y además cuenta con detectores y sensores anti-incendios, anti-intrusión, control de acceso, sensores de temperatura y humedad, etc. El director general posee control remoto sobre esta sala. Hay un SAI que en caso de fallo eléctrico permite funcionar al NAS y al sistema de seguridad de la empresa.

1. **TIPOS DE EMPLEADOS Y SUS ROLES**

* Director general: Posee el poder total sobre la empresa. Tiene acceso a todos los documentos de la empresa.
* Responsable de seguridad: Es el encargado de la seguridad física de la empresa.
* Responsable de ciberseguridad: Es el encargado de la seguridad informática de la empresa. Cuenta con varios trabajadores del departamento de informática para esta gestión. Es el responsable de la gestión de los datos informáticos de la empresa.
* Directores de departamentos: Se encuentran en este grupo los directores de cada departamento. Poseen un acceso superior a los datos que la mayoría de los empleados, pero no superan al director general. Dependiendo el ámbito (económico-operaciones) tiene acceso a diferente tipo de información), por ejemplo: El director financiero tiene acceso a todas las cuentas de la empresa, pero no puede saber la ubicación de los instaladores, cosa que el director de operaciones puede hacer. En cambio, el director de operaciones no puede revisar las cuentas.

Para acceder a información privilegiada deberán solicitar permiso al director general.

* Instaladores: Poseen un nivel bajo en cuanto a acceso a la información de la empresa. Pueden crear altas y bajas de averías, emitir facturas… En caso de ser necesario que accedan a información no permitida deberá solicitar permiso al equipo de dirección del departamento pertinente.
* Equipo de tienda: Son los trabajadores encargados de realizar el trabajo en las tiendas. Se encargan principalmente de la venta de productos al consumidor, la gestiones relacionadas con Movistar, la recogida de equipos para su reparación, etc. Tienen un nivel de acceso a la información similar al de los instaladores. En caso de ser necesario que accedan a información no permitida deberá solicitar permiso al equipo de dirección del departamento pertinente.
* Seguridad: Son los trabajadores que se encargan de la seguridad física de la empresa, en la sede principal y en el almacén. Su función es garantizar la máxima seguridad de los activos de la empresa. Para ello tienen acceso a las grabaciones del CCTV de la empresa, y al resultado de los sensores localizados en la sala donde se guardan los documentos y el NAS.

1. **PLAN DE SEGURIDAD DE LA EMPRESA**

* Análisis de riesgos

El análisis de riesgos según los activos y las amenazas se encuentra en el documento que se adjunta: [Activos y Análisis de riesgo](https://docs.google.com/spreadsheets/u/0/d/1pyrpFWqOOSYoIcgjA2maNGAHl_eElDQePhzaVsRkaJA/edit)

* Normativa en el puesto de trabajo

Para evitar lo máximo posible los incidentes de seguridad en la empresa, todos los trabajadores de la misma deberán cumplir con una serie de normas que ayudarán a reducir la posibilidad de que se produzca un incidente de seguridad. Estas normas son, entre otras::

* Los trabajadores no podrán acceder a la red en su puesto de trabajo a través de equipos personales (excepto previa autorización).
* Se evitará el acceso al correo electrónico u otros servicios con cuentas personales. Se deberá acceder con las cuentas que la empresa ha creado para sus trabajadores.
* Los trabajadores no podrán dejar el ordenador con la cuenta abierta cuando se ausenten de su puesto de trabajo.
* Evitar acceder a links sospechosos recibidos por correo electrónico. Para ello se deberá revisar la dirección a la que lleva el link, ya que podría tratarse de un phishing.
* Las credenciales de cada trabajador son privadas e intransferibles.
* Se evitará utilizar la conexión de dispositivos USB, teléfonos u otros dispositivos personales en los ordenadores de la empresa, ya que podrían estar infectados.
* No se compartirá información confidencial de la empresa a través de una conversación por teléfono.
* Las tarjetas RFID que dan acceso a la sala del NAS son personales e intransferibles.
* Se evitará la descarga de software desde páginas web sospechosas.
* Plan de concienciación

Para concienciar a los empleados en materia de ciberseguridad, se realizarán diferentes acciones:

* Se realizarán charlas informativas en materia de ciberseguridad, donde deberán acudir todos los trabajadores. Se buscará informar en mayor parte a los directivos y jefes de departamento de la empresa, ya que estos poseen acceso a mayor cantidad de información, por lo que supone un riesgo mayor que estos sean víctima de algún intento de robo de credenciales.
* Se realizarán actividades donde se simulará un posible incidente de ciberseguridad, donde los empleados deberán responder adecuadamente.
* Se contratarán hackers para que ataquen a los empleados mediante ingeniería social (siempre con la autorización de la empresa) con el objetivo de hacer ver a los empleados que es algo que es muy fácil que ocurra y qué consecuencias tendría.
* Se realizarán auditorías para comprobar la seguridad de la empresa.
* Se entregará a los empleados información de INCIBE relacionada con ciberseguridad en empresas.
* Los empleados deberán conocer la normativa en el puesto de trabajo respecto a la ciberseguridad.
* A final de año se realizarán estudios internos sobre la seguridad de la empresa, donde se mostrará a los trabajadores los incidentes ocurridos, los evitados, como se ha actuado, por qué, etc.
* En caso de incidente de seguridad, se informará a los empleados de cómo deben actuar, cómo ha afectado, cómo se va a solucionar, etc.
* Política de seguridad
  + Las redes utilizadas en las distintas sedes de la empresa serán únicamente accesibles por los equipos utilizados por los trabajadores para desarrollar su trabajo. Para ello se realiza un filtrado MAC en las distintas redes de la empresa.
  + Dependiendo del estatus empresarial de cada trabajador, este tendrá acceso a determinada información. Para ello se ha creado un usuario a cada trabajador que utilice un dispositivo conectado a la red de la empresa. De esta forma cada trabajador tendrá acceso a la información que le corresponde. En caso de querer acceder a información a la que no tiene acceso, deberá pedir permiso a su superior, y este le enviará la información.
  + Se realizarán charlas informativas sobre ciberseguridad a los trabajadores de la empresa, sea cual sea el puesto que cubren, con el objetivo de concienciar a estos de como se puede producir un incidente de ciberseguridad y su importancia. Se buscará informar en mayor parte a los directivos y jefes de departamento de la empresa, ya que estos poseen acceso a mayor cantidad de información, por lo que supone un riesgo mayor que estos sean víctima de algún intento de robo de credenciales.
  + Los documentos de la empresa estarán alojados en una sala de alta seguridad. Esta sala cuenta con control de accesos, monitorización de su estado (temperatura, humedad…), sistema anti incendios, sistema anti intrusión, grabación permanente…
  + Los documentos en formato papel están almacenados en unos armarios con una cerradura digital que únicamente podrán abrir los trabajadores autorizados. En cuanto a los documentos digitales, estos se encuentran almacenados en un NAS.
  + Para acceder al NAS los trabajadores tendrán que entrar con un usuario y contraseña que los identifique. A través de esta identificación se podrá monitorizar quién ha accedido, la fecha y hora del acceso, la localización, el tiempo que ha estado conectado, etc.
  + Las grabaciones de todos los CCTV de la empresa son almacenados en los discos duros situados en la sala de máxima seguridad. Estas grabaciones permanecerán almacenadas durante 7 días y posteriormente serán enviadas a un servidor en la nube.
  + Todas las sedes cuentan con un SAI que permitirá que, en caso de fallo eléctrico, funcionen sus respectivos sistemas de seguridad (CCTV, sistemas anti incendios, sistemas anti intrusión, etc).

# 