

Descripción de la
organización

Incidentes de Ciberseguridad

Eduardo Villacampa Escartín

Fecha



Introducción

1. **Descripción de la organización**

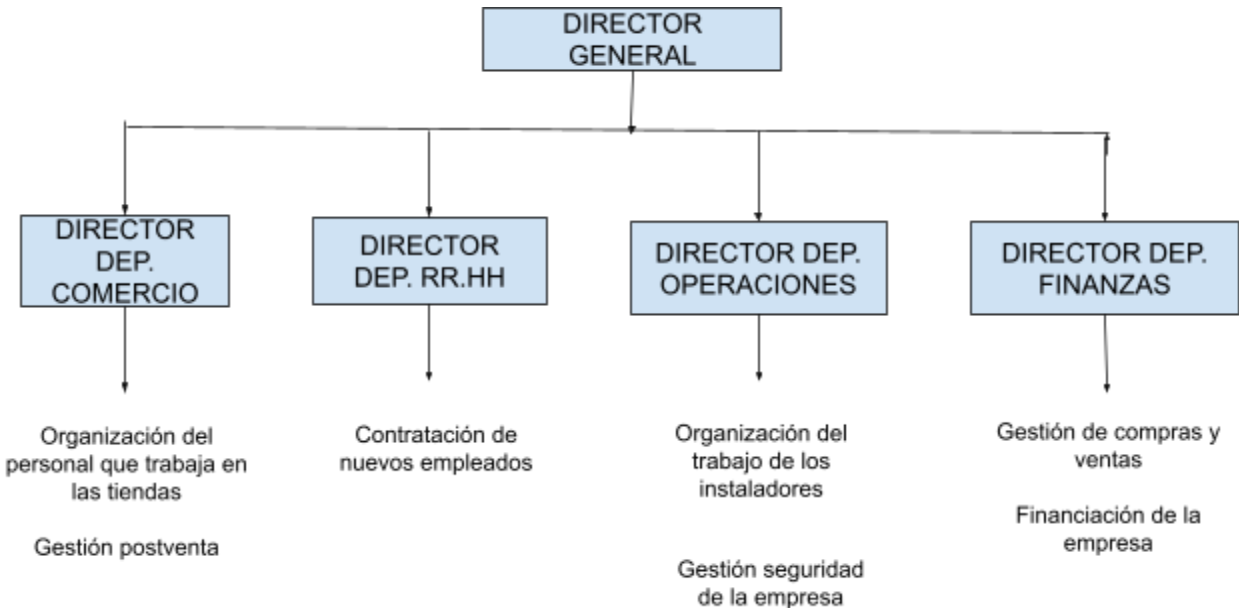
1.1. Ámbito de negocio

Se trata de una 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 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 contratación de nuevos empleados.
- 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.
- Departamento de finanzas: su función es el control de las compras y ventas de los bienes de la empresa, así como la gestión financiera de la empresa (facturas, informes financieros, contratos...).

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.

2. ACTIVOS DE LA EMPRESA

ACTIVOS CRÍTICOS

- 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...
- La **sala** donde se almacena la información, el NAS y los elementos del CCTV. 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 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.

-

3. TIPOS DE EMPLEADOS Y SUS ROLES

- Director general: Posee el poder total sobre la empresa. Tiene acceso a todos los documentos 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.

4. PLAN DE SEGURIDAD DE LA EMPRESA

➤ 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).