*Dockelements*

Incidentes de Ciberseguridad



Antonio Priego Díaz 14/10/2022

Índice

[1. Explicación de los apartados 3](#_Toc119487520)

[2. Ámbito de negocio 3](#_Toc119487521)

[3. Organigrama de la empresa 3](#_Toc119487522)

[Diagrama de Casos de Uso 4](#_Toc119487523)

[4. Descripción de las sedes 5](#_Toc119487524)

[Esquema de red de la sede 5](#_Toc119487525)

[5. Identificación de activos 6](#_Toc119487526)

[Activos críticos 6](#_Toc119487527)

[Activos semicríticos 6](#_Toc119487528)

[Activos no críticos 6](#_Toc119487529)

[7. Plan de seguridad 7](#_Toc119487530)

[Normativa del puesto de trabajo 7](#_Toc119487531)

[Plan de concienciación 7](#_Toc119487532)

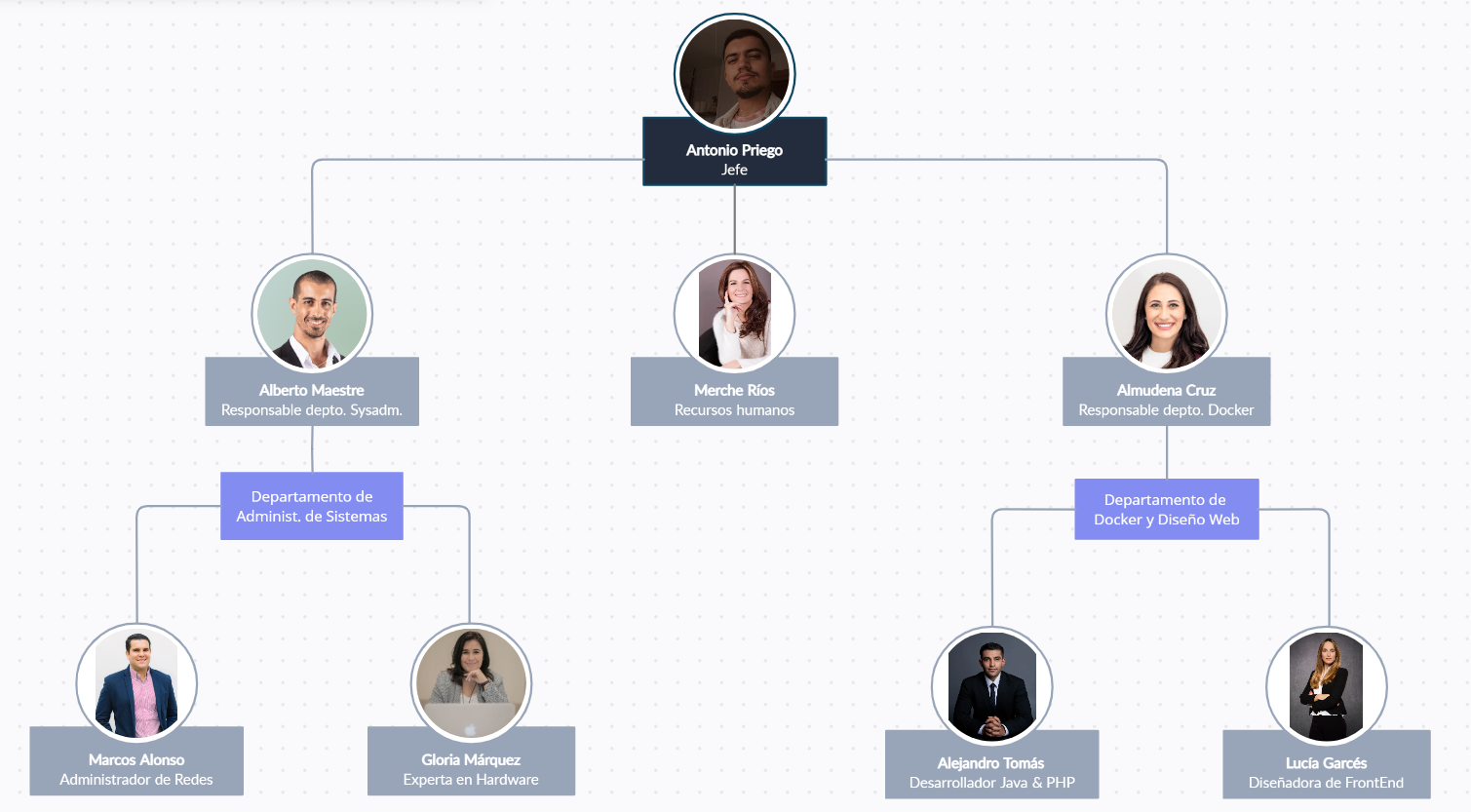
# Explicación de los apartados

lol

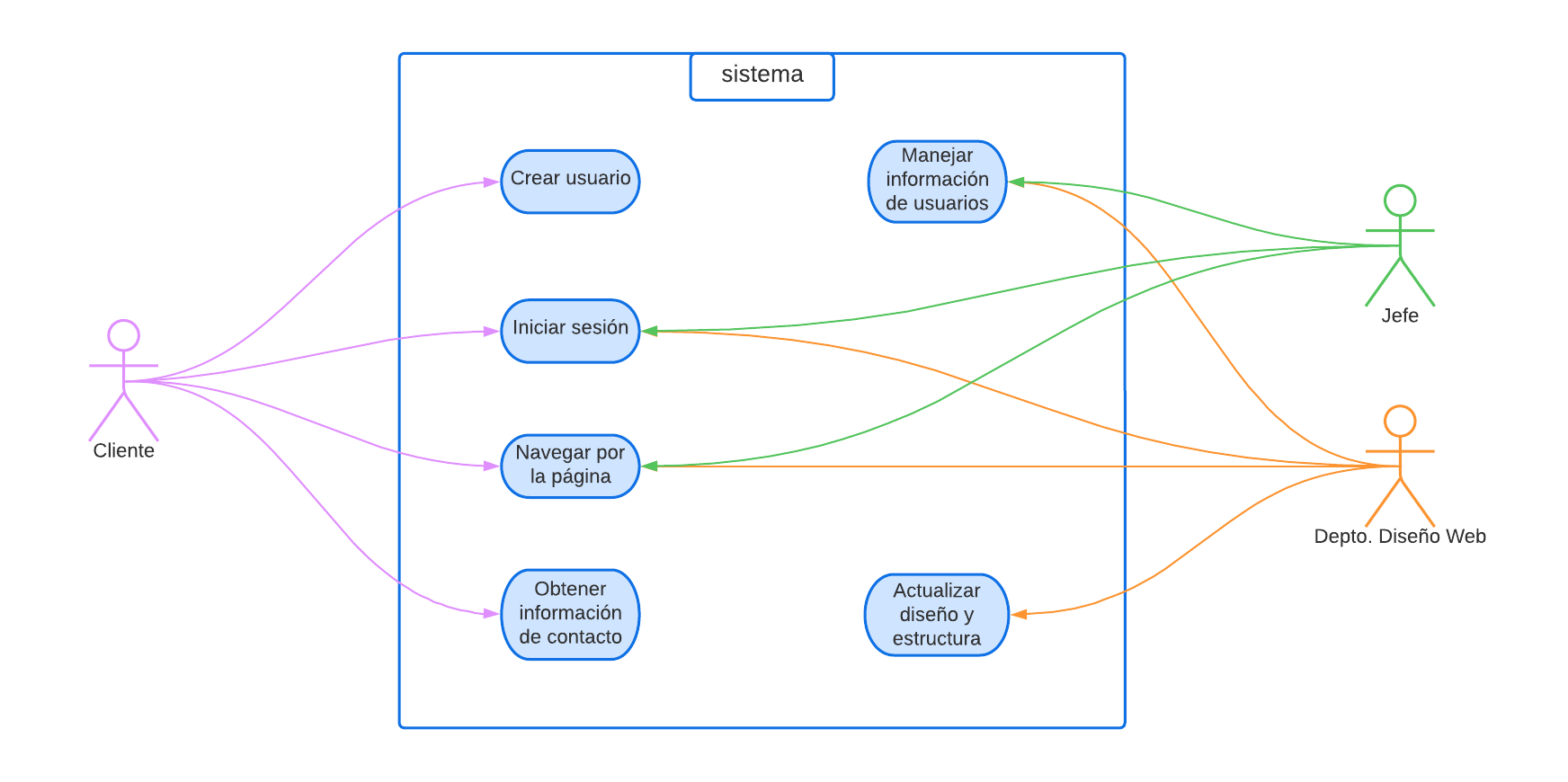
# Ámbito de negocio

* *Dockelements* es una empresa de informática dedicada a la creación, manejo y despliegue de microservicios y contenedores Docker.
  + También ofrece planes de administración de sistemas y diseño web.
* La empresa es relativamente pequeña, puesto que cuenta con 7 integrantes.

# Organigrama de la empresa



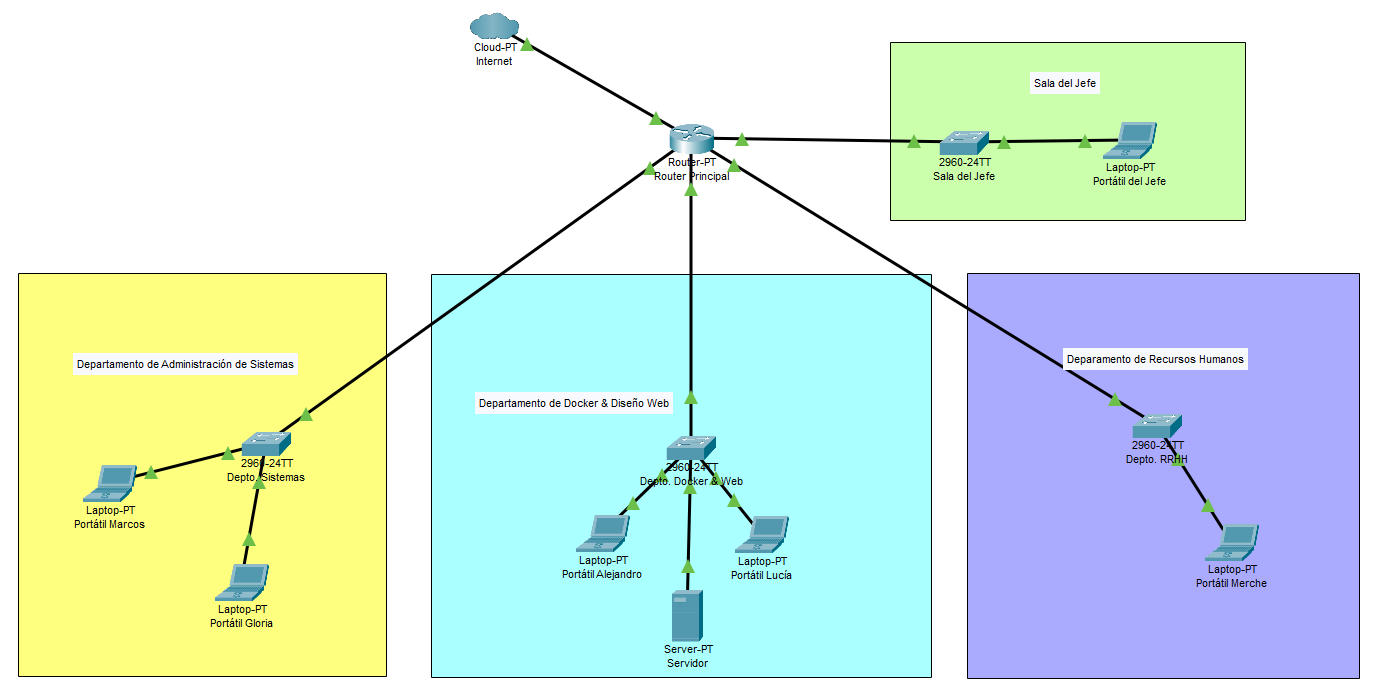
## Diagrama de Casos de Uso



# Descripción de las sedes

* La empresa posee con una sede física en Huesca, aunque los trabajadores pueden optar por teletrabajar desde donde se encuentren.
* La sede cuenta con una sala separada para cada departamento, una oficina para el jefe, un área común y un baño.

## Esquema de red de la sede



# Identificación de activos

* En primer lugar, distinguiremos entre activos críticos, semicríticos y no críticos.
  + Los activos críticos son aquellos que deben estar en marcha para que la actividad de la empresa funcione. El rendimiento es menos importante que si el activo está en funcionamiento o no.
  + Los activos semicríticos son los que, en caso de fallo, no tienen por qué detener la producción, pero sí ralentizan el rendimiento.
  + Por último, los activos no críticos son aquellos que no afectan a la capacidad de la empresa para generar ingresos, da igual cual sea su precio, tamaño o complejidad.

## Activos críticos

* Los servidores que almacenan recursos y la página web de la empresa, router, switches.
* Los documentos que contengan información importante, sea de los clientes o de la propia empresa.

## Activos semicríticos

* Los portátiles que usan los empleados para trabajar, el software CRM para gestionar los datos de los clientes.

## Activos no críticos

* Periféricos (monitores, ratones, teclados), sillas de oficina.

# 7. Plan de seguridad

## Normativa del puesto de trabajo

* No activar la opción de “Autocompletar contraseñas” en el navegador. Para gestionar las contraseñas, se usará un gestor dedicado a ello, como Bitwarden.
  + Preferiblemente, se usará la funcionalidad de autogenerar contraseñas, para una mayor seguridad. En caso de no usarla, la contraseña generada por el usuario deberá cumplir con unos requisitos de complejidad y longitud (Uso de mayúsculas, números, símbolos…)
* El antivirus de Windows Defender debe encontrarse activado en todo momento.
* El software que se instale en los equipos debe ser lícito, queda prohibida la descarga de cualquier programa pirata, o de origen dudoso.
* Cada empleado se llevará su portátil a su domicilio antes de empezar el fin de semana. En caso de que se irrumpa en la oficina en este lapso de tiempo, los equipos no se encontrarán allí.
* La información de carácter sensible que se maneje (documentos, contraseñas, etc.) se debe mantener siempre organizada y cuidada.
* Para realizar el trabajo correspondiente a la organización, priorizar el uso de los equipos y materiales otorgados por la empresa.
* No manejar información en canales que no sepamos que son 100% seguros.
* Los archivos y materiales de relevancia deben tener una redundancia, es decir, deben encontrarse duplicados (copias de seguridad).
* Cuando la información sensible con la que trabajemos deje de ser relevante, se destruirá, garantizando que no vuelva a ser accesible.
* En la medida de lo posible, ignorar los correos sospechosos que contengan enlaces externos, o documentos adjuntos. Se deberá comprobar que el remitente del mismo sea fiable.

## Plan de concienciación

El plan de concienciación de la empresa se diseña acorde al estatus de la misma (PYME). Por ello, el presupuesto será más limitado, pero se tratará de ajustar lo máximo posible al ámbito de la empresa (informática).

* El objetivo principal es que los empleados sean conscientes de los problemas que podrían provocar las brechas o amenazas de seguridad.
* Se propondrá un taller sobre ciberseguridad, de curso no mandatorio, pero sí premiado (recompensas aún por designar).
* En la oficina de la empresa se colgarán posters con imágenes diseñadas para concienciar en aspectos concretos. Se tratará de rotar el contenido de éstos cada mes, o máximo cada 2 meses. (Parte del Kit de Concienciación de INCIBE).
* En relación con la temática de los pósters, el primer miércoles de cada mes se tratará de exponer la presentación correspondiente al tema mensual, para que los empleados estén más formados. (Parte del Kit de Concienciación de INCIBE).
* Una vez al año (en fechas “aleatorias”, pero planificadas), se llevará a cabo el simulacro de “Gophish”, para poner a prueba los conocimientos de los empleados en materia de ciberseguridad. (Parte del Kit de Concienciación de INCIBE).