

**UNIVERSIDAD TECNOLOGICA DE PEREIRA**

**FACULTAD DE INGENIERIAS**

**Programa Ingeniería de Sistemas y Computación**

**Ingeniería del software**

**Documento de requisitos**

**Proyecto de gestión de información de usuarios**

**Presentado por:**

LUISA FERNANDA HENAO MAYA

1.088.353.505

YEISON AGUIRRE GALLEGO

1.104.675.098

**Presentado a:**

RICARDO BERMUDEZ

**septiembre**

Pereira / Risaralda

2019

**HISTORIAL DE VERSIONES**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **FECHA** |  |  | **VERSIÓN** |  |  | **DESCRIPCIÓN** |  |  | **AUTOR** |  |  | **EMPRESA** |  |
|  |  |  |  |  |  |  |  |  |  |
| 25/09/2016 | |  | 1.0 | |  |  | Creación del documento | |  | Luisa Fernanda Henao Maya  Yeison Aguirre Gallego | |  | UNIVERSIDAD TECNOLOGICA DE PEREIRA |  |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Elaborado por:** |  |  | **Revisado por:** |  |  | **Aprobado por:** |  |
|  |  |  |  |  |  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |  | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |  | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |  |
|  | **LUISA HENAO** | |  | **RICARDO BERMUDEZ** | |  |  |  |
|  | **YEISSON AGUIRRE** | |  |  | |  | **Cliente** | |
|  |  | |  |  |  |  |  |  |

**Requisitos no funcionales**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| **Código** | RNF001 | **Versión** | 1 | **Fecha** | Septiembre 25/2019 |
| **Fuente** | Protocolo Kerbeos | | | | |
| **Prioridad:** | Alta | | | **Módulo:** | Autenticación de usuarios |
| **Descripción:** | | | | | |
| Para la autenticación de los usuarios se debe de tener en cuenta que las contraseñas deben ser encriptadas y de esta forma almacenadas en la base de datos para así brindar una seguridad para cada usuario. | | | | | |
|
| **Observaciones:** | | | | | |
| Tener en cuenta que la contraseña tiene una caducidad trimestral | | | | | |
|
| Reglas: | | | | | |
| La contraseña debe de tener mínimo 8 alfanuméricos y carácter especial | | | | | |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| **Código** | RNF002 | **Versión** | 1 | **Fecha** | Septiembre 25/2019 |
| **Fuente** |  | | | | |
| **Prioridad:** | Alta | | | **Módulo:** | Autenticación de usuarios |
| **Descripción:** | | | | | |
| El usuario debe de estar seguro que cuenta con una contraseña y un usuario el cual se encuentra creado en la base de datos con su respectivo protocolo. | | | | | |
|
| **Observaciones:** | | | | | |
| Tener en cuenta que el usuario puede ser el correo o un código de usuario elegido por el mismo | | | | | |
|
| **Reglas:** | | | | | |
| Un usuario debe de ser único e irrepetible | | | | | |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| **Código** | RNF003 | **Versión** | 1 | **Fecha** | Septiembre 25/2019 |
| **Fuente** |  | | | | |
| **Prioridad:** | Alta | | | **Módulo:** | Autenticación de usuarios |
| **Descripción:** | | | | | |
| Método de recuperación de contraseña | | | | | |
| **Observaciones:** | | | | | |
| El usuario deberá tener el correo el cual registró en el sistema o su número de teléfono para así recibir un mensaje de autenticación | | | | | |
|
| **Reglas:** | | | | | |
| El usuario solo podrá intentar autenticarse 2 veces, en la 3ra se enviará notificación de alerta. | | | | | |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| **Código** | RNF004 | **Versión** | 1 | **Fecha** | Octubre 01/2019 |
| **Fuente** |  | | | | |
| **Prioridad:** | Alta | | | **Módulo:** | Autenticación de usuarios |
| **Descripción:** | | | | | |
| Seguridad de la contraseña de accedo muy alta | | | | | |
| **Observaciones:** | | | | | |
| El usuario deberá registrar una contraseña la cual debe contener letras mayúsculas, minúsculas números y símbolos para garantizar la seguridad. | | | | | |
|
| **Reglas:** | | | | | |
| Que la cantidad de caracteres no supere los 15 dígitos | | | | | |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| **Código** | RNF004 | **Versión** | 1 | **Fecha** | Octubre 01/2019 |
| **Fuente** |  | | | | |
| **Prioridad:** | Alta | | | **Módulo:** | Autenticación de usuarios |
| **Descripción:** | | | | | |
| Protección de datos | | | | | |
| **Observaciones:** | | | | | |
| Como se maneja información personal como correos, nombres, datos de contacto, etc, se deben regir mediante la Ley Orgánica de Protección de Datos de Carácter Personal. | | | | | |
|
| **Reglas:** | | | | | |
| mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales en Colombia. | | | | | |
|