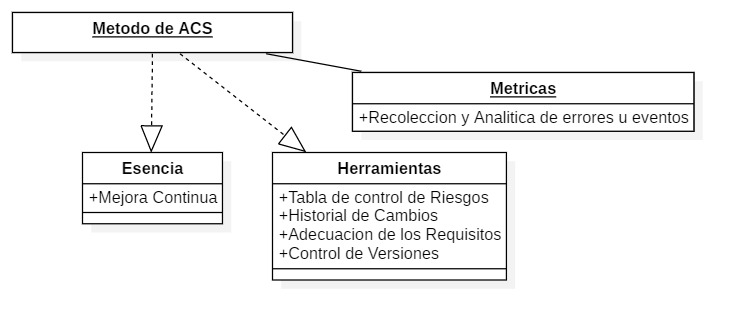
## Método ACS:

Se plantea una metodología capaz de acoplarse a cualquier tipo de desarrollo del software.



### Tabla de Control de Riesgo:

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Categoría** | **Impacto** | **Plan de Acción** |
| Cambio de Gestión | Proyecto | Marginal | Se monitorean las necesidades del nuevo personal, en caso de que haya una adición de requerimientos estos se agendan para el tercer módulo de desarrollo. |
| Cambio de Requerimientos | Proyecto y Producto | Marginal  (Critico depende de la fase de desarrollo) | Se recolecta el o los nuevos requerimientos, acorde a estos se plantea si la solución en desarrollo es viable, o si hay que hacer un cambio en el versionamiento. |
| Retrasos en las Especificaciones | Proyecto y Producto | Critico | Los módulos esenciales del proyecto no se cumplirían en el tiempo planteado originalmente, por lo que se daría prioridad a estos dejando en segundo plano los requisitos no esenciales. |
| Tamaño del Producto | Producto | Critico | El tamaño del proyecto fue subestimado, por lo que se debe priorizar los requisitos fundamentales del software para que este se pueda poner en marcha, dando plazo a actualizaciones posteriores. |
| Cambio en la Tecnología | Producto | Marginal o Critico | Cambios en la tecnología, como OS de un servidor podría afectar sinergia con el producto.  Un efecto como este se podría solventar con mecanismos de virtualización. |

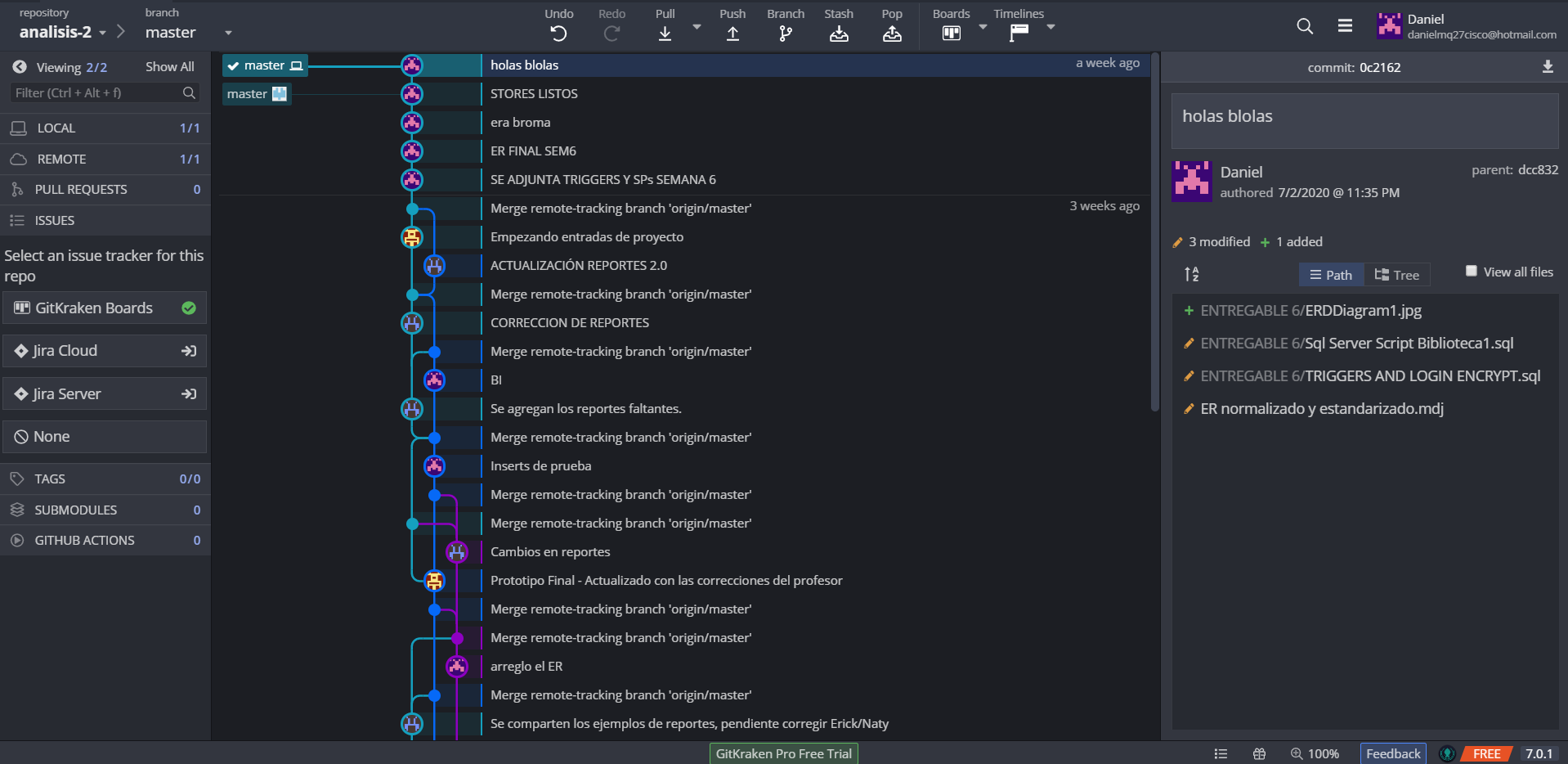
### Historial de Cambio:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Petición** | **# de petición** | **Fecha** | **Prioridad** | **Descripción** |
| Baja del formulario CEDIL | 1 | 10 de mayo 2020 | Despreciable | Se solicita dar de baja al formulario, ya que la información de este ahora debe ser tomada en **Consultas.** |

### Adecuación de Requisitos:

|  |  |  |
| --- | --- | --- |
|  | **CRUD del formulario CIIE** |  |
|  | Calificación 10 - 1 |  |
| Correcto | # | Incorrecto |
| Completo | # | Incompleto |
| Útil | # | Despreciable |
| Verificable | # | No verificable |
| Modificable | # | No modificable |

### Control de Versiónamianto:



### Métricas:

* Especificaciones erróneas o incompletas.
* Errores de comunicación con el cliente.
* Violación de los estándares de programación.
* Errores en la integridad de los datos.
* Interfaz gráfica inconsistente.
* Documentación errónea.
* Interfaz ambigua.

Formula de medición:

Errores \* 100

X= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 100 – X = VALOR DE LA METRICA

Especificaciones totales

Donde lo ideal es mantener un porcentaje superior a 70 en cada una de las métricas. Cualquier valor cercano a 70 o debajo de este indica una requerida atención en esa área.

### Pruebas de Software:

De forma manual se realizará el siguiente esquema de pruebas:

|  |  |  |
| --- | --- | --- |
| **Área** | **Descripción** | **Cantidad** |
| CRUD de formularios | Por cada campo de los CRUD se hará un ingreso completo del mismo, validando las restricciones de cada uno de los campos.  Ejemplo: En el formulario CIIE el espacio correspondiente al número de teléfono solo debe aceptar valores numéricos. Por lo que la prueba consiste en intentar ingresar caracteres, espacio nulo y valores alfanuméricos. De esta forma se podrán validar las diferentes respuestas que debe dar el sistema. | En este caso las pruebas serian en relación a la cantidad de campos multiplicados por la cantidad de validaciones que requiera cada uno de ellos. |
| Permisos de Roles | En este segmento se tienen que probar los accesos a las diferentes vistas acorde a cada rol. De manera tal que un rol sin permiso administrativo no pueda acceder a funciones como la gestión de los demás usuarios. | La cantidad de pruebas se realizarían sobre los 3 distintos tipos de roles planteados, verificando una a una sus funcionalidades dentro del sistema. |
| Generación de Reportes | La información almacenada en la base de datos debe ser transformada y mostrada en forma de reporte, esta sección debe validar la integridad de los datos, donde la información contenida en la base debe ser la misma reflejada en los reportes. | Luego de hacer al menos 50 ingresos por formulario, se extraerán los reportes múltiples veces, permitiendo validar que estos datos se mantienen en valores reales, aprobada esta parte se realizaran modificantes a los datos desde el sistema y se repetirá el paso anterior, este ciclo debe hacerse al menos 10 veces. Reflejando reportes de aproximadamente 500 ingresos al sistema (incluyendo modificaciones). |

### Seguridad Perimetral:

* Física:

1. Cámaras de Vigilancia.
2. Cuartos de Sistemas bajo llave

(Esto del lado de la Asamblea Legislativa)

* Lógica:

1. Firewalls con filtrado de datos en ambas partes (Asamblea y Proveedor de servicio).
2. Acceso a las computadoras por medio de claves de usuario. (Asamblea)
3. Seguridad de puertos de red. Solo la maquina destinada a ese puerto puede darle uso, validación mediante la MAC. (Asamblea)
4. ACL’s. (Asamblea y Proveedor de servicio)

### Seguridad de Red y WEB:

* Evaluación de riesgo ante las entradas por parte de los usuarios, en este caso las computadoras cuentan con antivirus, como método de escaneo para los datos que pueda descargar o inyectar un usuario a los equipos computacionales.
* Implementación del Cifrado SSL.
* Diseño de un sistema seguro para el restablecimiento de las contraseñas. Los datos o transacciones de estas no serán visualizables dentro del HTML.
* Segmentación de redes mediante VLAN, esto incluye los puntos de acceso inalámbricos.
* CDP y LLDP desactivados en la configuración de los dispositivos de red.
* Uso de Tunneling GRE para la comunicación de la Asamblea y el proveedor.

### Seguridad de los Datos:

* Encriptación de campos relevantes. (privados)
* Respaldo de información relevante mediante tablas de respaldo y back ups programados de la base de datos.
* Encriptación de los Back Ups mediante TDE.
* Respaldos y protocolos de recuperación contratados con el proveedor.

### Seguridad Contractual:

En esta área el proveedor debe cumplir con los siguientes aspectos por los que es contratado:

* Seguridad Física de los sistemas donde ese encuentra la información.
* Protección ante ataques como la denegación de servicios.
* Dualidad en la información, de manera que se permita la recuperación de los sistemas en caso de algún tipo de perdida total o parcial sobre el servidor.
* Back ups sobre los datos almacenados en el servidor.
* Los tiempos en la caída de los servicios no puede ser mayor a 30 min, en caso de ser así aplican multas.