Controles Inteligentes sobre el SGSI de la Universidad del Cauca - Fase II Proyecto SGSI UNICAUCA

ANEXO

CARLOS ANDRES RODALLEGA OBANDO
OSCAR RICARDO VALENCIA AGUILAR

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
GRUPO DE I+D EN TECNOLOGÍAS DE LA INFORMACIÓN
LINEA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN, ENERO DE 2013

ANEXOS

ANEXO A: Listado de controles ISO/IEC 27002:2005.

ISO/IEC 27002:2005.

5. POLÍTICA DE SEGURIDAD.

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.

6.1.1 Compromiso de la Dirección con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información.
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
6.1.5 Acuerdos de confidencialidad.
6.1.6 Contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés.
6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.
6.2.2 Tratamiento de la seguridad en la relación con los clientes.
6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos.
7.1.2 Propiedad de los activos.
7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.

7.2.1 Directrices de clasificación.
7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

8.1 Antes del empleo.

8.1.1 Funciones y responsabilidades.
8.1.2 Investigación de antecedentes.
8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.

8.2.1 Responsabilidades de la Dirección.
8.2.2 Concienciación, formación y capacitación en seg. de la informac.
8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.

8.3.1 Responsabilidad del cese o cambio.
8.3.2 Devolución de activos.
8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1 Áreas seguras.
- 9.1.1 Perímetro de seguridad física.
- 9.1.2 Controles físicos de entrada.
- 9.1.3 Seguridad de oficinas, despachos e instalaciones.
- 9.1.4 Protección contra las amenazas externas y de origen ambiental.
- 9.1.5 Trabajo en áreas seguras.
- 9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.
- 9.2.1 Emplazamiento y protección de equipos.
- 9.2.2 Instalaciones de suministro.
- 9.2.3 Seguridad del cableado.
- 9.2.4 Mantenimiento de los equipos.
- 9.2.5 Seguridad de los equipos fuera de las instalaciones.
- 9.2.6 Reutilización o retirada segura de equipos.
- 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.
- 10.1.1 Documentación de los procedimientos de operación.
- 10.1.2 Gestión de cambios.
- 10.1.3 Segregación de tareas.
- 10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.
- 10.2.1 Provisión de servicios.
- 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
- 10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.
- 10.3.1 Gestión de capacidades.
- 10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.
- 10.4.1 Controles contra el código malicioso.
- 10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.
- 10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.
- 10.6.1 Controles de red.
- 10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.
- 10.7.1 Gestión de soportes extraíbles.
- 10.7.2 Retirada de soportes.
- 10.7.3 Procedimientos de manipulación de la información.
- 10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.
- 10.8.1 Políticas y procedimientos de intercambio de información.
- 10.8.2 Acuerdos de intercambio.
- 10.8.3 Soportes físicos en tránsito.
- 10.8.4 Mensajería electrónica.
- 10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.
- 10.9.1 Comercio electrónico.
- 10.9.2 Transacciones en línea.
- 10.9.3 Información públicamente disponible.

10.10 Supervisión.
- 10.10.1 Registros de auditoría.
- 10.10.2 Supervisión del uso del sistema.
- 10.10.3 Protección de la información de los registros.
- 10.10.4 Registros de administración y operación.
- 10.10.5 Registro de fallos.
- 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.
- 11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.
- 11.2.1 Registro de usuario.
- 11.2.2 Gestión de privilegios.
- 11.2.3 Gestión de contraseñas de usuario.
- 11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.
- 11.3.1 Uso de contraseñas.
- 11.3.2 Equipo de usuario desatendido.
- 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.
- 11.4.1 Política de uso de los servicios en red.
- 11.4.2 Autenticación de usuario para conexiones externas.
- 11.4.3 Identificación de los equipos en las redes.
- 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
- 11.4.5 Segregación de las redes.
- 11.4.6 Control de la conexión a la red.
- 11.4.7 Control de encaminamiento (routing) de red.

11.5 Control de acceso al sistema operativo.
- 11.5.1 Procedimientos seguros de inicio de sesión.
- 11.5.2 Identificación y autenticación de usuario.
- 11.5.3 Sistema de gestión de contraseñas.
- 11.5.4 Uso de los recursos del sistema.
- 11.5.5 Desconexión automática de sesión.
- 11.5.6 Limitación del tiempo de conexión.

11.7 Ordenadores portátiles y teletrabajo.
- 11.7.1 Ordenadores portátiles y comunicaciones móviles.
- 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.
- 12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.
- 12.2.1 Validación de los datos de entrada.
- 12.2.2 Control del procesamiento interno.
- 12.2.3 Integridad de los mensajes.
- 12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.
- 12.3.1 Política de uso de los controles criptográficos.
- 12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.
- 12.4.1 Control del software en explotación.
- 12.4.2 Protección de los datos de prueba del sistema.
- 12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.
- 12.5.1 Procedimientos de control de cambios.
- 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 12.5.3 Restricciones a los cambios en los paquetes de software.
- 12.5.4 Fugas de información.
- 12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la cont. del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistem. de información.

15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

ANEXO B: Listas de chequeo.

Tabla B.1: Lista Chequeo para identificación del servicio crítico del portal institucional.

Entrevistado: Ing. Fabián Mera Fecha: 14 – Junio - 2012

Entidad: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca (TIC).

LISTA DE CHEQUEO PARA IDENTIFICAR LOS SERVICIOS CRITICOS				
	Test para verificar los servicios críticos	SI	NO	Observaciones
1	¿Si el servicio falla afecta el funcionamiento de otros servicios?	X		
2	¿Existen servicios que dependen del servicio seleccionado?	X		
3	¿Existen políticas claras para el servicio seleccionado?	X		
4	¿Existe algún proceso de organización interna para este servicio? Ejemplo: Coordinación de roles, acuerdos de confidencialidad, revisiones de implantación de la seguridad de toda la información etc.		X	
5	¿Existe información de alta confidencialidad en ese servicio?		X	
6	¿Este servicio es capaz de trabajar de modo independiente?		X	
7	¿Existen controles, alarmas o algún seguimiento de administración sobre este servicio crítico?	X		
8	¿Existe un procedimiento documentado sobre cómo se debe llevar a cabo el servicio?	X		
9	¿Se genera algún registro por la prestación o no del servicio crítico?	X		

¿Cuánto es el tiempo máximo que puede estar por fuera el servicio crítico?

El tiempo máximo que puede estar fuera de servicio son 12 horas.

¿Existen datos estadísticos de cuantas interrupciones del servicio crítico ocurren al día, al mes, al año?

Los informes de disponibilidad son proporcionados por NAGIOS.

¿Cuántas personas intervienen en el proceso de la prestación de ese servicio crítico?

Editores Web, desarrolladores y área de SSI.

¿Qué tipo de privilegios tienen cada una de las cuentas de las personas que prestan ese servicio?

Dependen del rol existen:

- Administrador de contenido.
- Desarrollador Web.
- Ingenieros Administradores de servidores.

Comparten una cuenta de administrador donde se almacena el login de la persona que la está usando.

Tabla B.2: Lista Chequeo para identificación del servicio crítico del correo electrónico.

Entrevistado: Ing. Fabián Mera Fecha: 14 – Junio - 2012

Entidad: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca (TIC).

LISTA DE CHEQUEO PARA IDENTIFICAR LOS SERVICIOS CRITICOS				
	Test para verificar los servicios críticos	SI	NO	Observaciones
1	¿Si el servicio falla afecta el funcionamiento de otros servicios?	X		
2	¿Existen servicios que dependen del servicio seleccionado?	X		
3	¿Existen políticas claras para el servicio seleccionado?	X		
4	¿Existe algún proceso de organización interna para este servicio? Ejemplo: Coordinación de roles, acuerdos de confidencialidad, revisiones de implantación de la seguridad de toda la información etc.		X	
5	¿Existe información de alta confidencialidad en ese servicio?	X		
6	¿Este servicio es capaz de trabajar de modo independiente?	X		
7	¿Existen controles, alarmas o algún seguimiento de administración sobre este servicio crítico?	X		
8	¿Existe un procedimiento documentado sobre cómo se debe llevar a cabo el servicio?	X		
9	¿Se genera algún registro por la prestación o no del servicio crítico?	X		

¿Cuánto es el tiempo máximo que puede estar por fuera el servicio crítico?

El tiempo máximo que el servicio puede estar fuera de servicio es de 12 horas.

¿Existen datos estadísticos de cuantas interrupciones del servicio crítico ocurren al día, al mes, al año?
Proporcionadas por NAGIOS.

¿Cuántas personas intervienen en el proceso de la prestación de ese servicio crítico?
2 Administradores de servidores.

¿Qué tipo de privilegios tienen cada una de las cuentas de las personas que prestan ese servicio?
Comparten una cuenta de administrador donde se almacena el login de la persona que la está usando.

Tabla B.3: Lista Chequeo para identificación del servicio crítico SIMCA y SIMCAS.
Entrevistado: Ing. Fabián Mera Fecha: 14 – Junio - 2012
Entidad: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca (TIC).

LISTA DE CHEQUEO PARA IDENTIFICAR LOS SERVICIOS CRITICOS				
	Test para verificar los servicios críticos	SI	NO	Observaciones
1	¿Si el servicio falla afecta el funcionamiento de otros servicios?	X		Procesos académicos
2	¿Existen servicios que dependen del servicio seleccionado?	X		
3	¿Existen políticas claras para el servicio seleccionado?		X	
4	¿Existe algún proceso de organización interna para este servicio? Ejemplo: Coordinación de roles, acuerdos de confidencialidad, revisiones de implantación de la seguridad de toda la información etc.		X	En proceso de elaboración
5	¿Existe información de alta confidencialidad en ese servicio?	X		
6	¿Este servicio es capaz de trabajar de modo independiente?		X	
7	¿Existen controles, alarmas o algún seguimiento de administración sobre este servicio crítico?	X		Monitoreo por parte de NAGIOS y la herramienta AWStats
8	¿Existe un procedimiento documentado sobre cómo se debe llevar a cabo el servicio?		X	En proceso de elaboración

9	¿Se genera algún registro por la prestación o no del servicio crítico?		X	Se generan informes pero no porque se pidan.

¿Cuánto es el tiempo máximo que puede estar por fuera el servicio crítico?

Se exige disponibilidad 24/7. Esta montado sobre un clúster de alta disponibilidad. El mayor tiempo que se encontró fuera de servicio este año de forma planeada fue de un tiempo máximo de 5 minutos.

¿Existen datos estadísticos de cuantas interrupciones del servicio crítico ocurren al día, al mes, al año?

Se realizan por medio de NAGIOS y AWStats

¿Cuántas personas intervienen en el proceso de la prestación de ese servicio crítico?

2 personas

¿Qué tipo de privilegios tienen cada una de las cuentas de las personas que prestan ese servicio?

Comparten una cuenta de administrador donde se almacena el login de la persona que la está usando.

Tabla B.4: Lista Chequeo para identificación del servicio crítico LDAP.

Entrevistado: Ing. Fabián Mera Fecha: 14 – Junio - 2012

Entidad: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca (TIC).

LISTA DE CHEQUEO PARA IDENTIFICAR LOS SERVICIOS CRITICOS				
	Test para verificar los servicios críticos	SI	NO	Observaciones
1	¿Si el servicio falla afecta el funcionamiento de otros servicios?	X		
2	¿Existen servicios que dependen del servicio seleccionado?	X		
3	¿Existen políticas claras para el servicio seleccionado?		X	
4	¿Existe algún proceso de organización interna para este servicio? Ejemplo: Coordinación de roles, acuerdos de confidencialidad, revisiones de implantación de la seguridad de toda la información etc.		X	
5	¿Existe información de alta confidencialidad en ese	X		

	servicio?			
6	¿Este servicio es capaz de trabajar de modo independiente?	X		
7	¿Existen controles, alarmas o algún seguimiento de administración sobre este servicio crítico?	X		Faltan controles a nivel interno.
8	¿Existe un procedimiento documentado sobre cómo se debe llevar a cabo el servicio?		X	
9	¿Se genera algún registro por la prestación o no del servicio crítico?	X		Realizado por NAGIOS.

¿Cuánto es el tiempo máximo que puede estar por fuera el servicio crítico?

Se exige disponibilidad 24/7. Alta disponibilidad.

¿Existen datos estadísticos de cuantas interrupciones del servicio crítico ocurren al día, al mes, al año?

Se realiza por medio de NAGIOS.

¿Cuántas personas intervienen en el proceso de la prestación de ese servicio crítico?

Es administrado por 2 personas pero hay 3 clientes que pueden gestionar información.

¿Qué tipo de privilegios tienen cada una de las cuentas de las personas que prestan ese servicio?

Existe una cuenta de administrador y usuarios con privilegios (administrador de cuentas).

Tabla B.5: Lista Chequeo para identificación del servicio crítico DNS.

Entrevistado: Ing. Fabián Mera Fecha: 14 – Junio - 2012

Entidad: División de Tecnologías de la Información y la Comunicación de la Universidad del Cauca (TIC).

LISTA DE CHEQUEO PARA IDENTIFICAR LOS SERVICIOS CRITICOS				
	Test para verificar los servicios críticos	SI	NO	Observaciones
1	¿Si el servicio falla afecta el funcionamiento de otros servicios?	X		
2	¿Existen servicios que dependen del servicio seleccionado?	X		
3	¿Existen políticas claras para el servicio seleccionado?		X	

4	¿Existe algún proceso de organización interna para este servicio? Ejemplo: Coordinación de roles, acuerdos de confidencialidad, revisiones de implantación de la seguridad de toda la información etc.		X	
5	¿Existe información de alta confidencialidad en ese servicio?		X	
6	¿Este servicio es capaz de trabajar de modo independiente?	X		
7	¿Existen controles, alarmas o algún seguimiento de administración sobre este servicio crítico?	X		Alarmas que dependen de NAGIOS
8	¿Existe un procedimiento documentado sobre cómo se debe llevar a cabo el servicio?		X	Parcialmente.
9	¿Se genera algún registro por la prestación o no del servicio crítico?	X		Estadísticas de NAGIOS, estas no se revisan todo el tiempo.

¿Cuánto es el tiempo máximo que puede estar por fuera el servicio crítico?

Se exige que se encuentre 24/7. Se tiene un margen de 1hora fuera de servicio por cortes de energía, pero por razones de mantenimiento 12 horas cada año, tarda aproximadamente 20 minutos en volver a estar disponible.

¿Existen datos estadísticos de cuantas interrupciones del servicio crítico ocurren al día, al mes, al año?

Estadísticas realizadas por NAGIOS

¿Cuántas personas intervienen en el proceso de la prestación de ese servicio crítico?

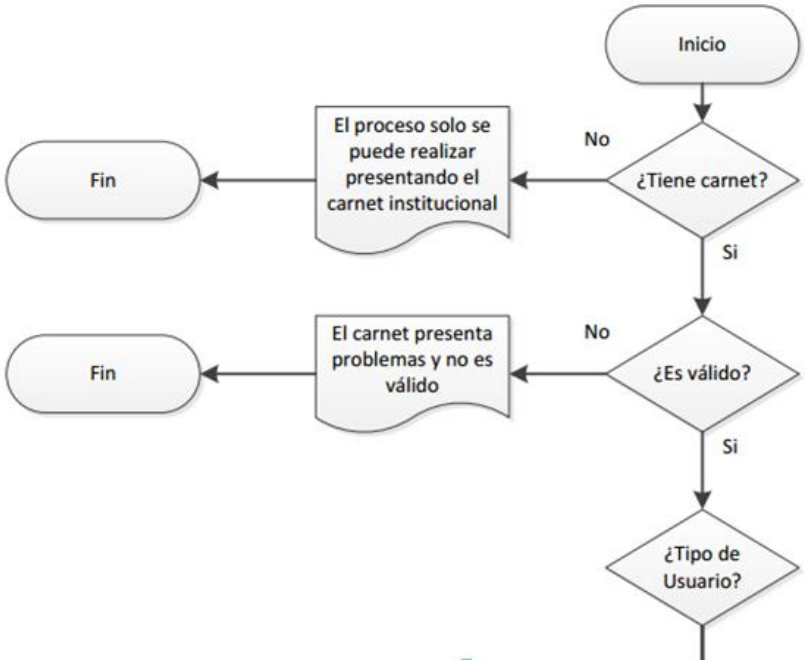
2 personas

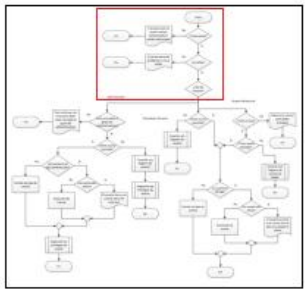
¿Qué tipo de privilegios tienen cada una de las cuentas de las personas que prestan ese servicio?

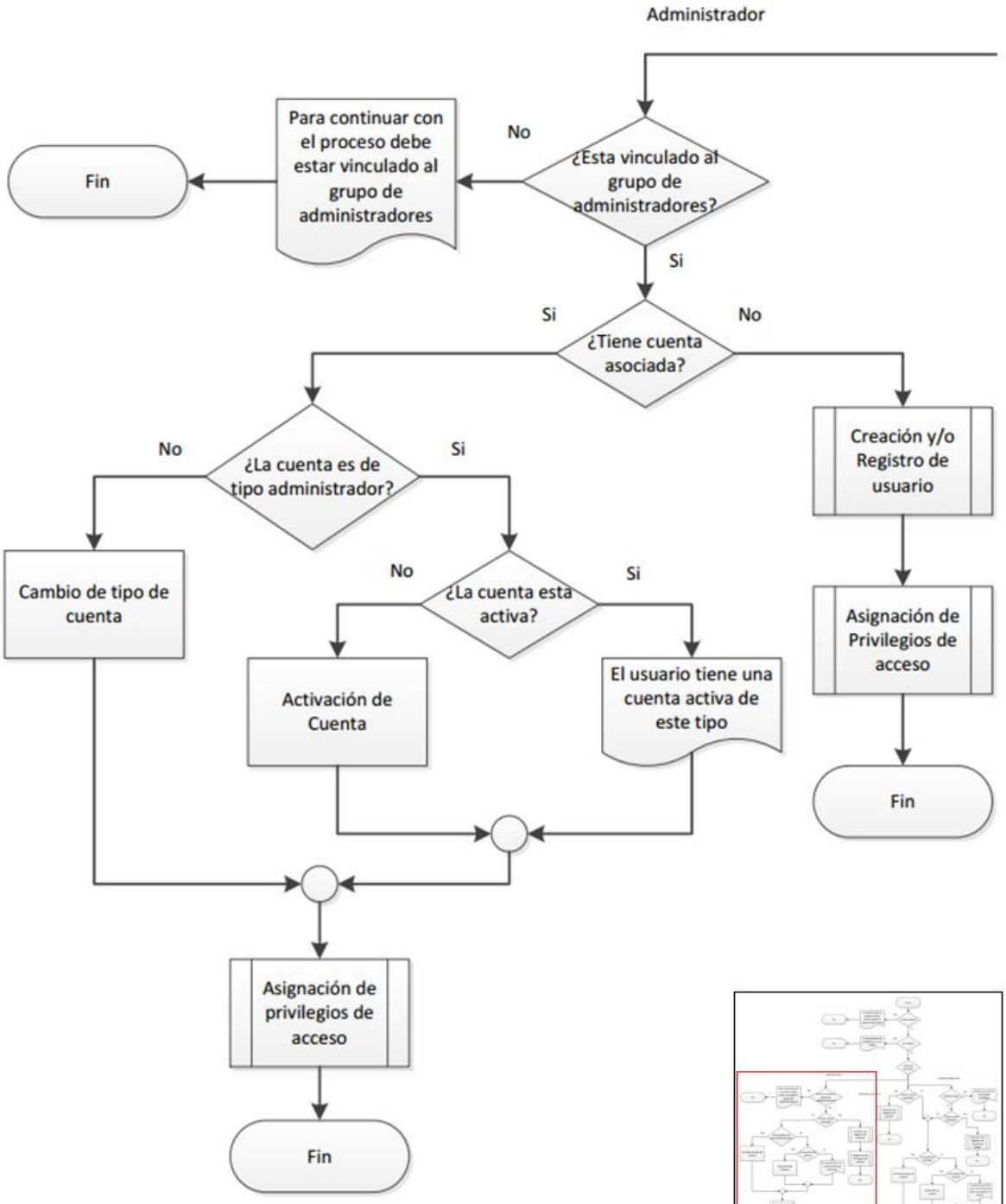
Usan una cuenta de administrador.

ANEXO C: Diagramas de Flujo.

Diagrama C.1: Diagrama de flujo para la creación del una cuenta de correo electrónico.






Administrador
¿Esta vinculado al grupo de administradores?
No
Para continuar con el proceso debe estar vinculado al grupo de administradores
Fin
Si
¿Tiene cuenta asociada?
Si
No
¿La cuenta es de tipo administrador?
No
Si
Cambio de tipo de cuenta
¿La cuenta esta activa?
No
Si
Activación de Cuenta
El usuario tiene una cuenta activa de este tipo
Creación y/o Registro de usuario
Asignación de Privilegios de acceso
Fin
Asignación de privilegios de acceso
Fin

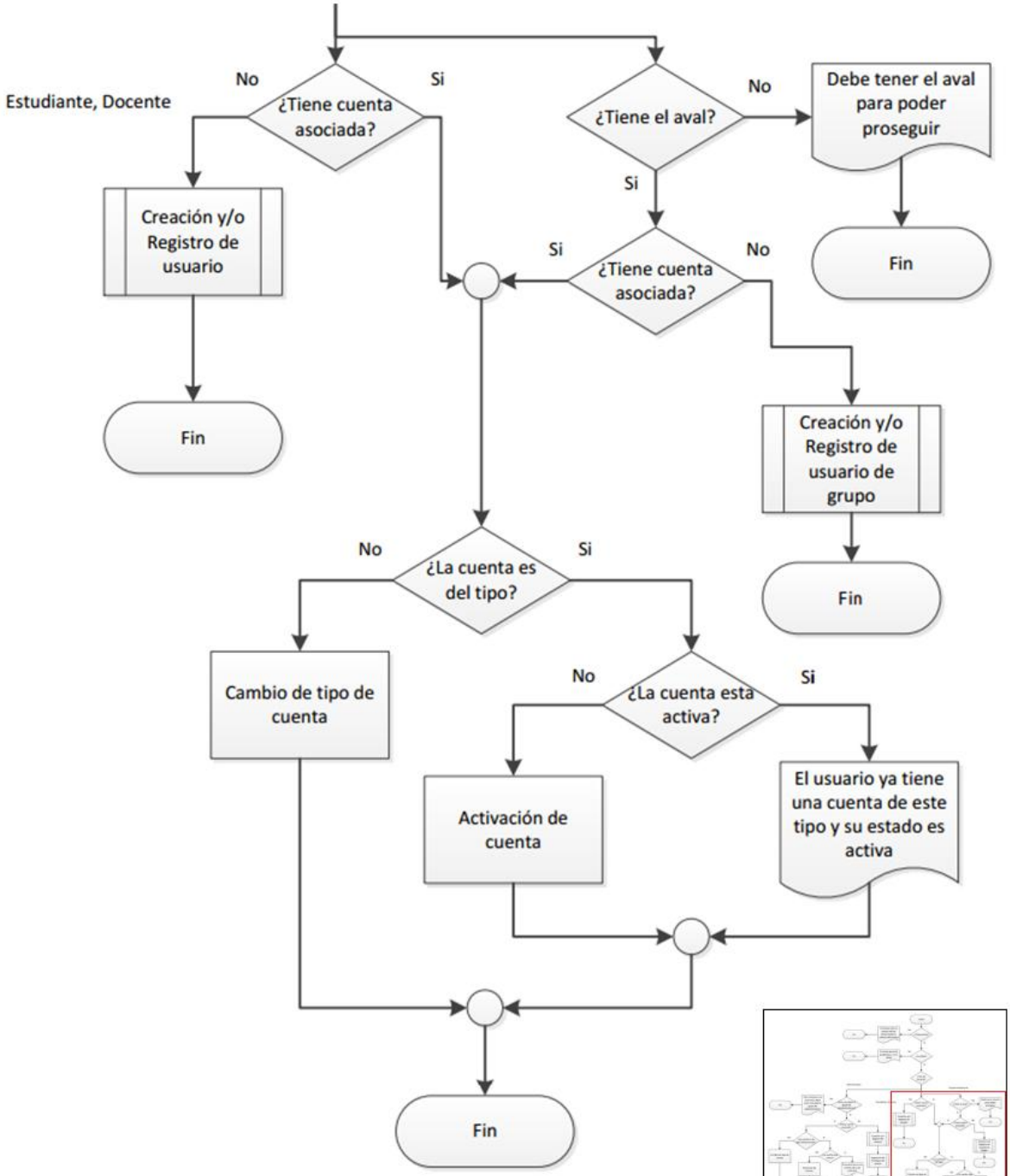

Estudiante, Docente
No
¿Tiene cuenta asociada?
Si
Creación y/o Registro de usuario
Fin
¿Tiene el aval?
No
Debe tener el aval para poder proseguir
Fin
Si
Si
¿Tiene cuenta asociada?
No
Creación y/o Registro de usuario de grupo
Fin
No
¿La cuenta es del tipo?
Si
Cambio de tipo de cuenta
No
¿La cuenta esta activa?
Si
Activación de cuenta
El usuario ya tiene una cuenta de este tipo y su estado es activa
Fin

Diagrama C.2: Diagrama de flujo subproceso de creación y/o registro de usuario.

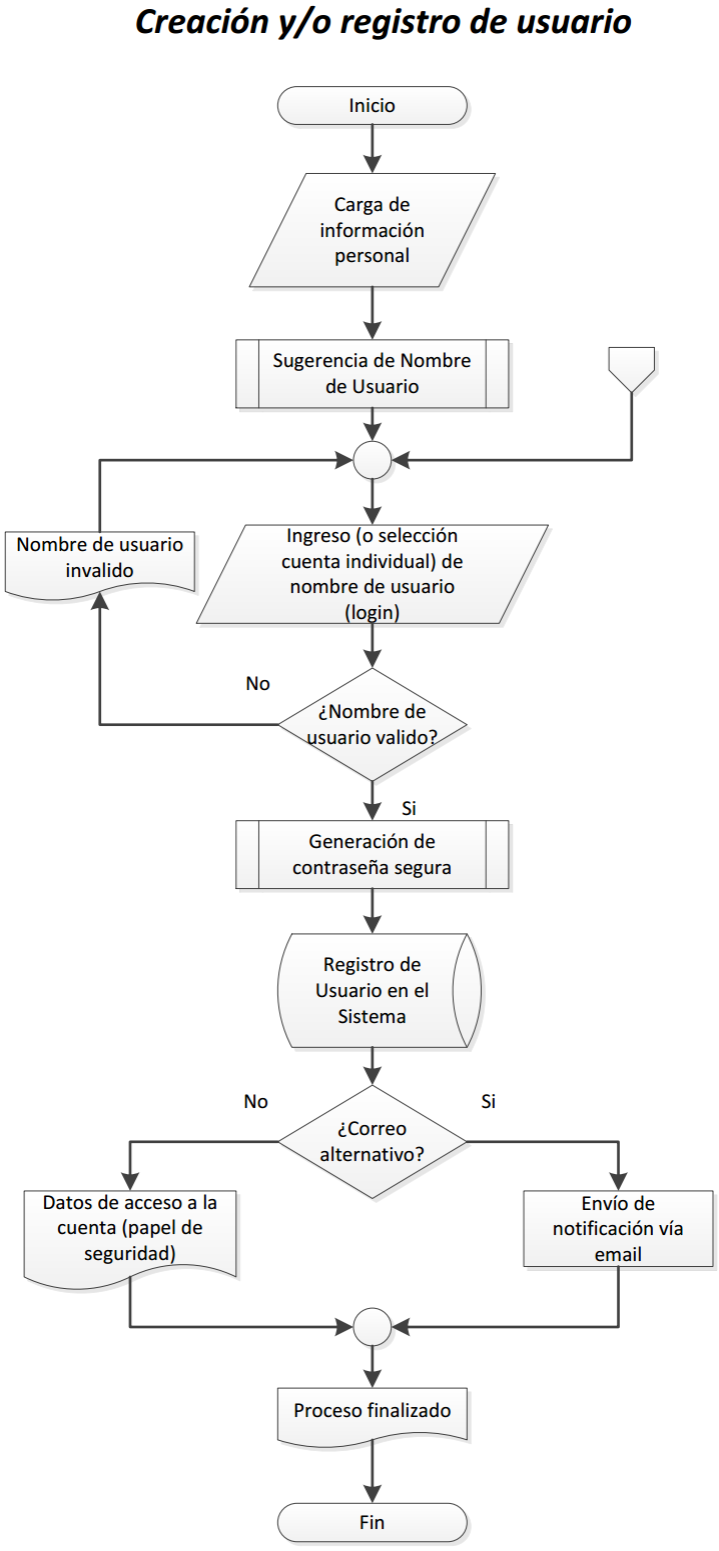


Diagrama C.3: Diagrama de flujo para el subproceso de creación y/o registro de grupo.

Diagrama C.4: Diagrama de flujo para el subproceso de asignación de privilegios de acceso.

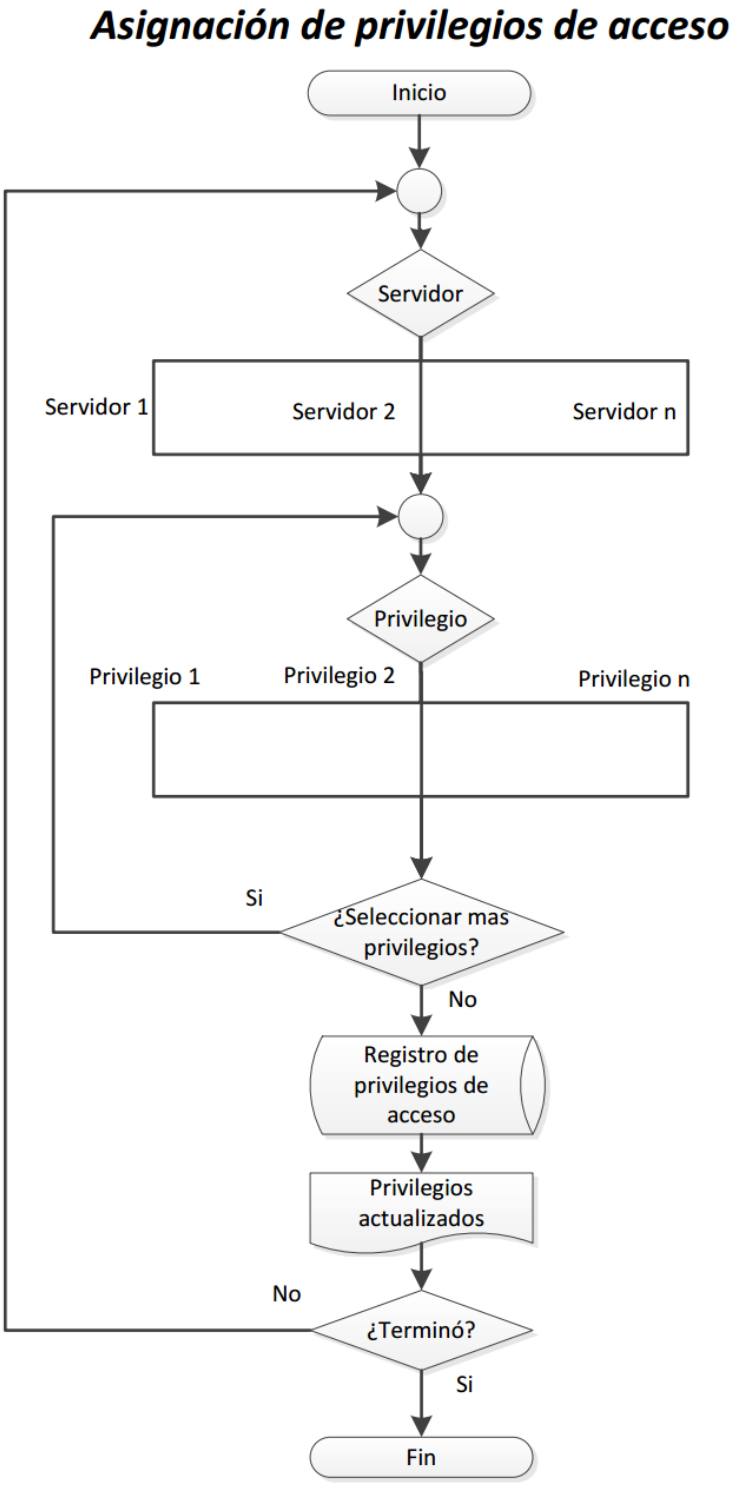


Diagrama C.5: Diagrama de flujo subproceso sugerencia de nombre de usuario.

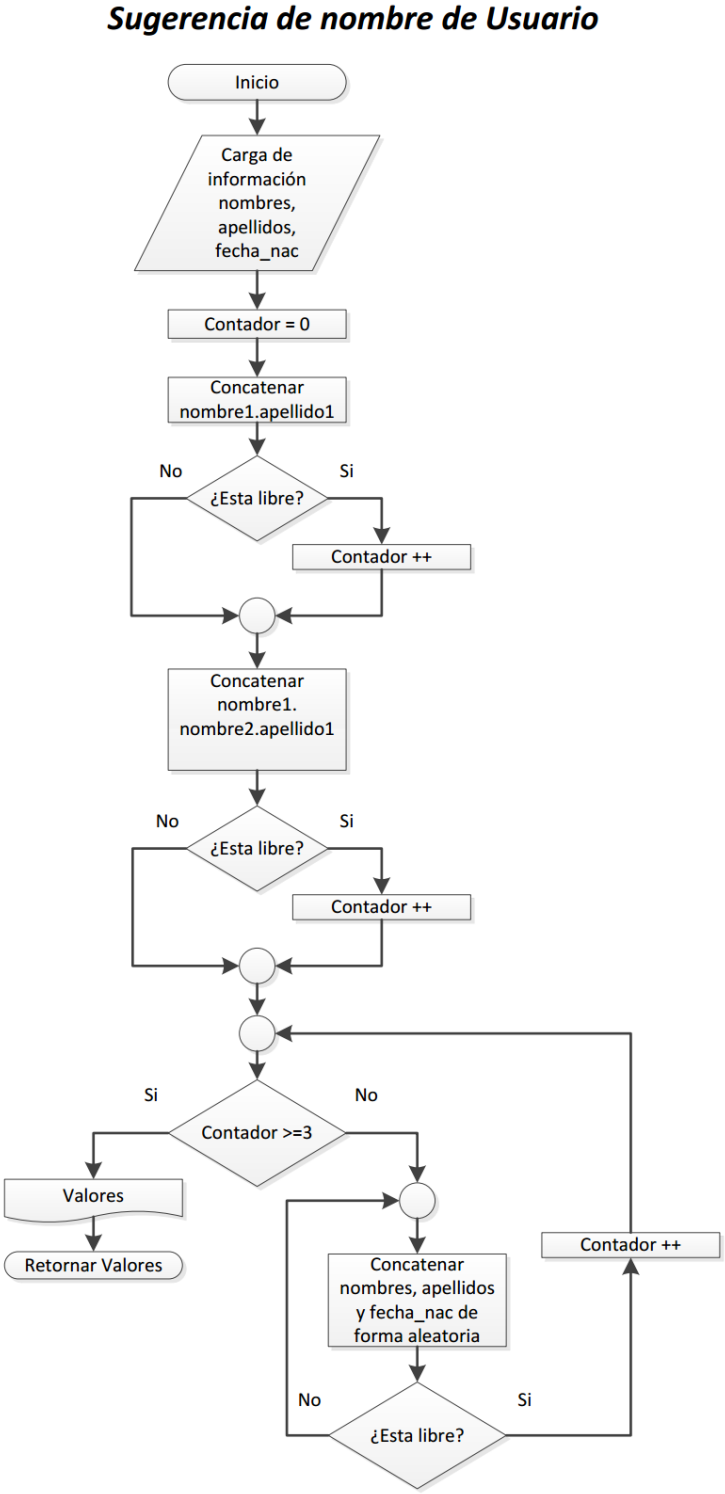
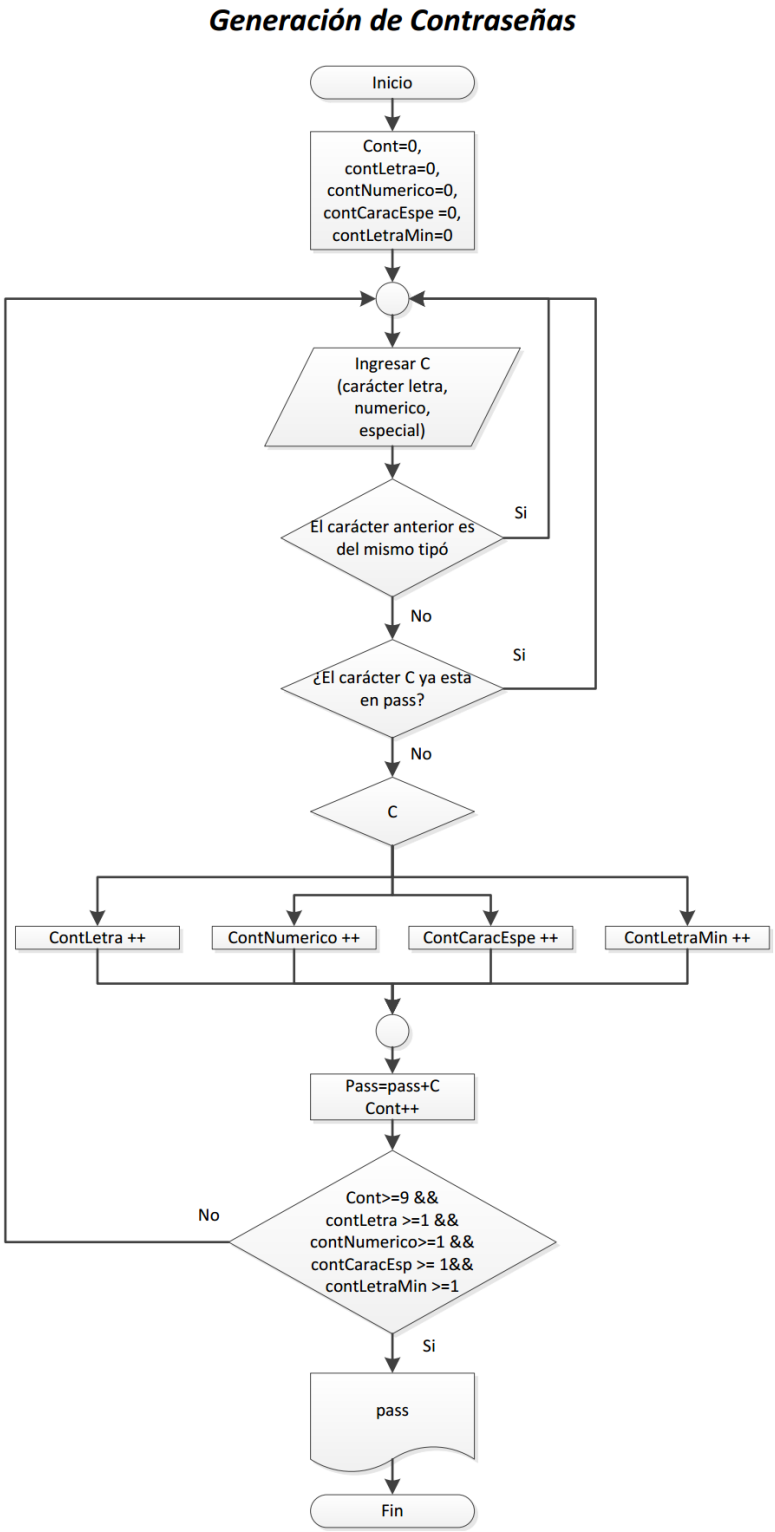
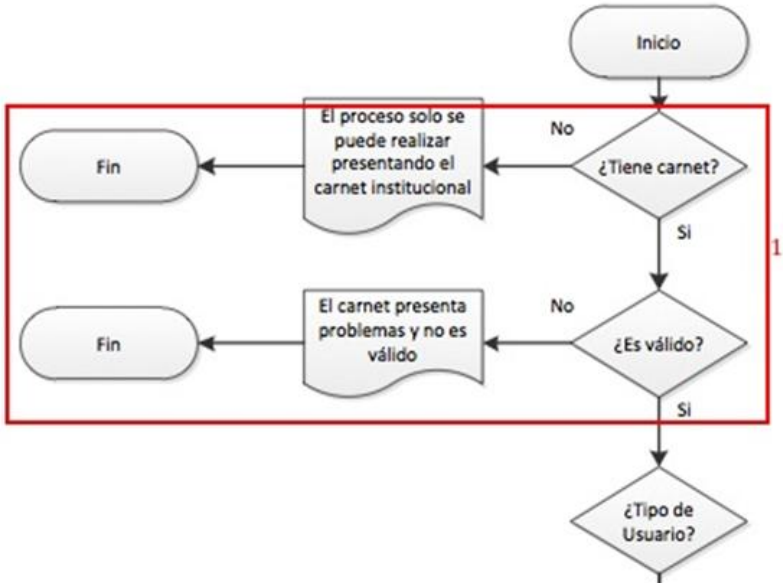


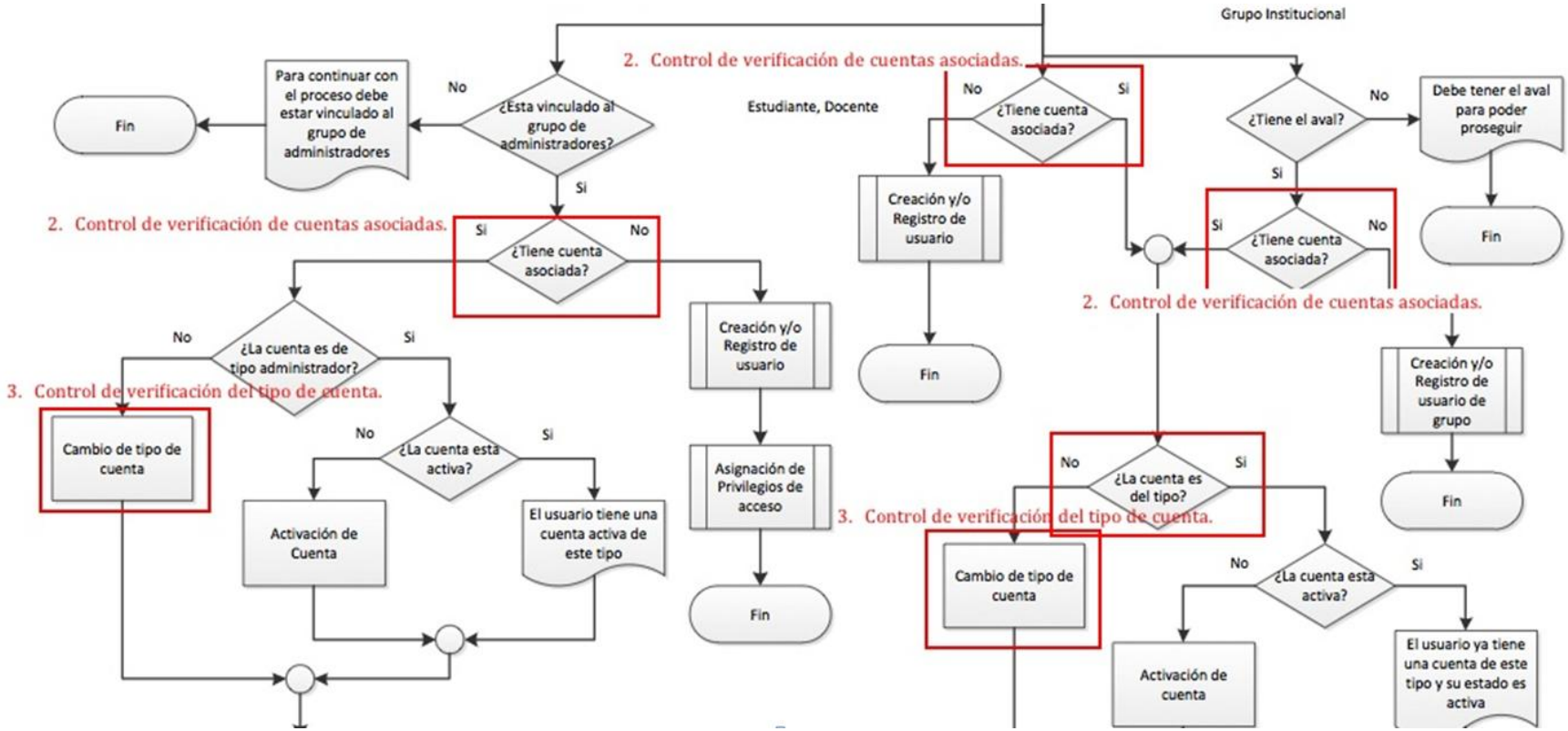
Diagrama C.6: Diagrama de flujo subproceso de generación de contraseñas.



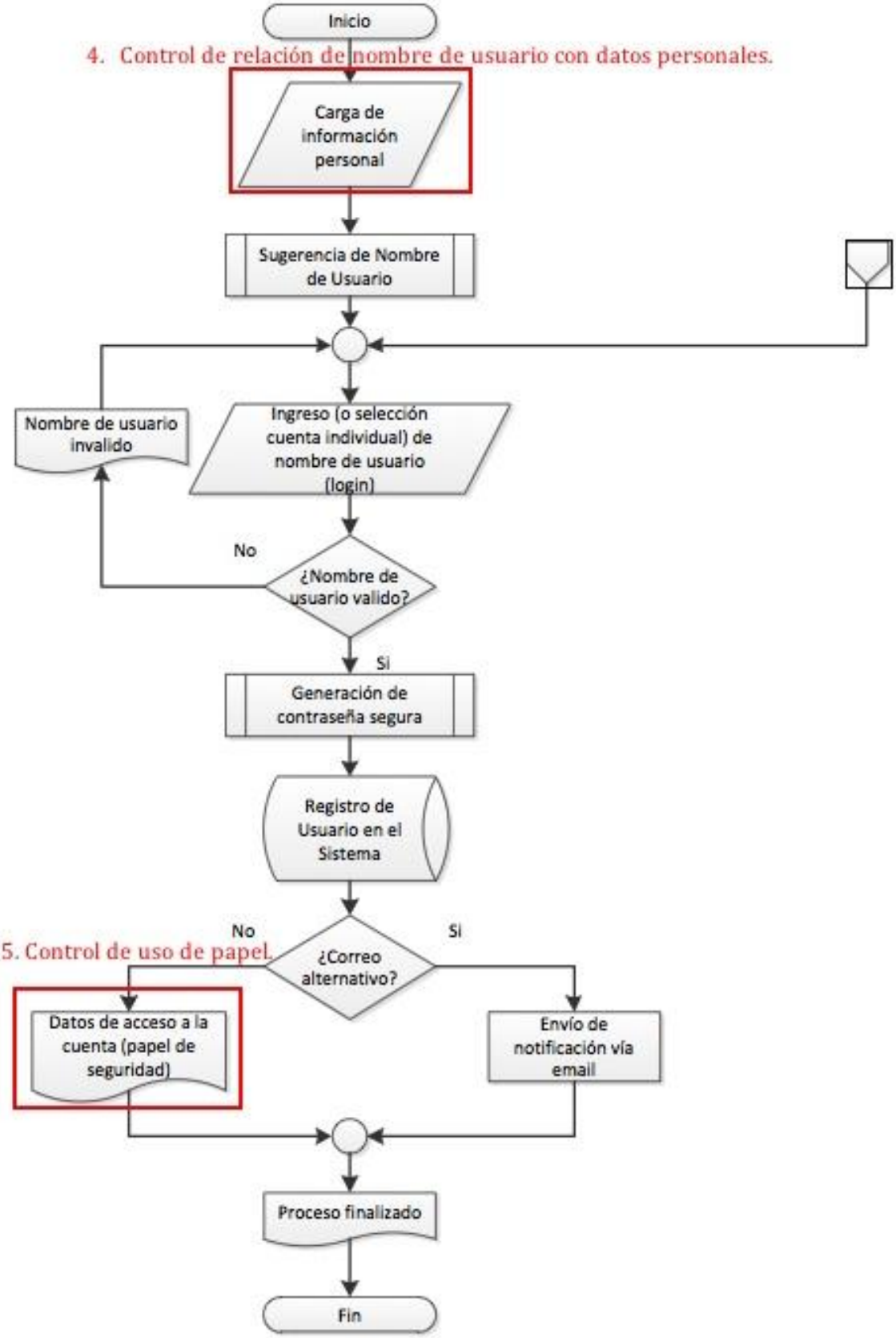
ANEXO D: Diagramas de Flujo con Controles.

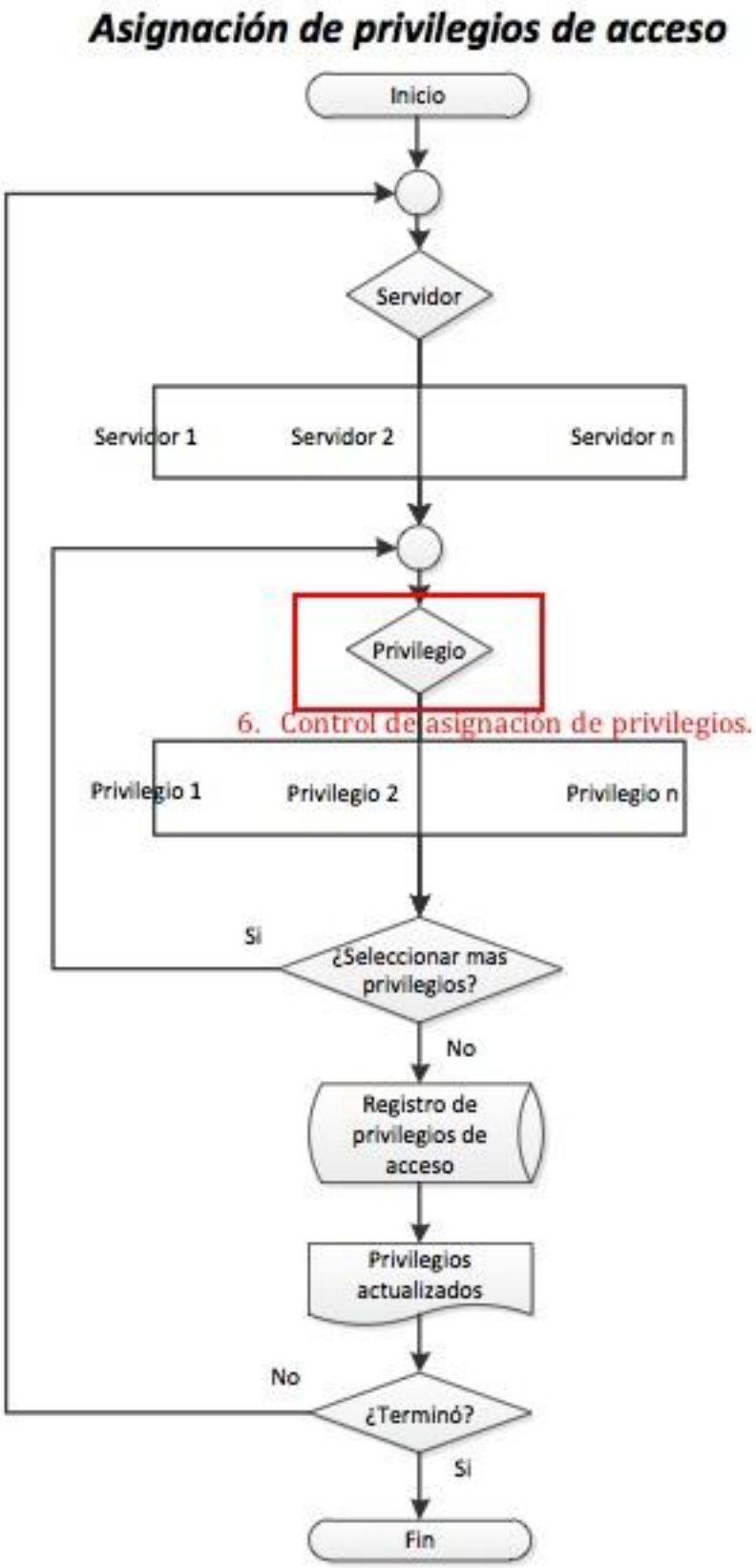


1. Control de verificación del carnet institucional.


Grupo Institucional
Estudiante, Docente
¿Esta vinculado al grupo de administradores?
No
Si
Para continuar con el proceso debe estar vinculado al grupo de administradores
Fin
2. Control de verificación de cuentas asociadas.
¿Tiene cuenta asociada?
Si
No
Creación y/o Registro de usuario
Fin
¿La cuenta es de tipo administrador?
3. Control de verificación del tipo de cuenta.
Cambio de tipo de cuenta
¿La cuenta esta activa?
Activación de Cuenta
El usuario tiene una cuenta activa de este tipo
Asignación de Privilegios de acceso
Fin
2. Control de verificación de cuentas asociadas.
¿Tiene cuenta asociada?
Creación y/o Registro de usuario
Fin
¿Tiene el aval?
Debe tener el aval para poder proseguir
Fin
2. Control de verificación de cuentas asociadas.
¿Tiene cuenta asociada?
Creación y/o Registro de usuario de grupo
Fin
3. Control de verificación del tipo de cuenta.
¿La cuenta es del tipo?
Cambio de tipo de cuenta
¿La cuenta esta activa?
Activación de cuenta
El usuario ya tiene una cuenta de este tipo y su estado es activa

Creación y/o registro de usuario




Asignación de privilegios de acceso
Inicio
Servidor
Servidor 1
Servidor 2
Servidor n
Privilegio
6. Control de asignación de privilegios.
Privilegio 1
Privilegio 2
Privilegio n
Si
¿Seleccionar mas privilegios?
No
Registro de privilegios de acceso
Privilegios actualizados
No
¿Terminó?
Si
Fin

ANEXO E: Entradas, proceso y salida para posibles controles.

Control de verificación del carnet institucional:

Datos de entrada: Carnet institucional, huella, se necesita la tabla o campos de la base de datos los cuales van a ser cargados en el sistema para realizar la simulación.

Proceso: Se debe realizar una búsqueda en las diferentes bases de datos DARCA o RH (Recursos humanos) para encontrar tipo de usuario relacionado con el carnet institucional, además del estado en el cual se encuentra el carnet institucional (Activo o Inactivo).

Dato de salida: Validez o invalidez del carnet institucional, además el tipo de usuario actual.

Control de verificación de cuentas asociadas:

Datos de entrada: Identificación del usuario al cual se le va a comprobar la disponibilidad de cuenta.

Proceso: Se debe de hacer una búsqueda en las diferentes bases de datos donde se encuentran almacenadas las cuentas de correo electrónico y verificar que ninguna cuenta de correo esté relacionada con la identificación del usuario.

Dato de salida: Asociación o no de la cuenta.

Control de verificación del tipo de cuenta:

Datos de entrada: Tipo de cuenta que se desea verificar.

Proceso: Con el tipo de cuenta que se desea crear comprobar que el usuario que va a crearla tenga los respectivos privilegios para crearla y además que no pueda crear una cuenta de privilegios superiores a los que este tenga.

Dato de salida: Tipo de cuenta valido o invalidez del tipo de cuenta.

Control de relación de nombre de usuario con datos personales:

Datos de entrada: Nombre de usuario.

Proceso: Consultar en la base de datos en donde se almacenen las cuentas de correo electrónico la información que está relacionada con el nombre de usuario y verificar que la cuenta de usuario este correctamente relacionada con los datos personales.
Dato de salida: Cuenta relacionada correctamente con los datos personales de la persona.

Control de uso de papel:
Datos de entrada: Número de consecutivo del papel.
Proceso: Se toma el número del consecutivo del papel a usar y se consulta en la base de datos si ya ha sido usado; en el caso que no se registra el uso del mismo en el sistema, si ya ha sido usado no se permitirá la impresión y será notificado el encargado.
Dato de salida: Notificación de que ese consecutivo ya ha sido usado al operador y al encargado.

Control de asignación de privilegios:
Datos de entrada: Privilegios a asignar, privilegios de quien ejecuta la asignación.
Proceso: Se verifica que los privilegios a asignar sean menores o iguales a los de la persona que los asigna.
Dato de salida: Mensaje de permiso o denegación al ejecutar la asignación.

Control de administración de servidor:
Datos de entrada: Nombre de usuario del que ejecuta la acción.
Proceso: Indiferente del equipo desde donde se ejecute la acción se debe verificar que el usuario que ejecuta sea administrador.
Dato de salida: Mensaje de permiso o denegación en la ejecución de la acción.

Control de robustez de contraseña:
Datos de entrada: Contraseña generada mediante el sistema.
Proceso: Realizar un análisis de la fortaleza de la contraseña generada.
Datos de salida: Contraseña robusta.

Control de realización de proceso:

Datos de entrada: Número de procesos fallidos y el número de intentos.

Proceso: Consulta el número de procesos fallidos y compararlos con el número de intentos realizados.

Datos de salida: Notificación de bloqueo de la cuenta en el caso de hallar sido realizado.

ANEXO F: Reglas de tipo P y Q entonces R.

Control de validez de contraseña segura:

Objetivo: Identificar si una contraseña es segura o no.

Tiempo de crackeo (Tc): Es el tiempo medido mediante un simulador, el cual se calcula mediante el simulacro en un equipo con unas características definidas obteniendo como resultado el tiempo que se demoraría craqueando una contraseña. Este tiempo se medirá en minutos y se puede clasificar como:

Bajo: Tiempo desde 0 hasta 14400 minutos.

Medio: Tiempo desde 14400 hasta 28800 minutos.

Alto: Tiempo desde 28800 hasta 43200 minutos.

Umbral de contraseña (Uc): Son las características que debe de tener una contraseña para considerarse mínimamente segura, esta medición se realizara según el número de características que cumpla. Se clasifican como:

Bajo: Cumple de 0 a 2 características.

Medio: Cumple de 2 a 5 características.

Alto: Cumple de 5 a 6 características.

Nivel de seguridad (Ns): Es la medida que indica si una contraseña se puede considerar como segura, aceptable o insegura.

Regla general: Tc ∧ Uc -> Ns

- Si tiempo de crackeo alta y contraseña supera el umbral entonces contraseña segura.

  Tc alto ∧ Uc Supera el umbral -> Ns Segura
- Si tiempo de crackeo medio y contraseña supera el umbral entonces contraseña aceptable.

  Tc medio ∧ Uc Supera el umbral -> Ns Aceptable

- Si tiempo de crackeo baja y contraseña supera el umbral entonces contraseña insegura.

  Tc bajo ∧ Uc Supera el Umbral -> Ns Insegura
- Si tiempo de crackeo alta y contraseña inferior al umbral entonces contraseña aceptable.

  Tc alto ∧ Uc Inferior al Umbral -> Ns Aceptable
- Si tiempo de crackeo medio y contraseña inferior al umbral entonces contraseña insegura.

  Tc medio ∧ Uc Inferior el Umbral -> Ns Insegura
- Si tiempo de crackeo baja y contraseña inferior al umbral entonces contraseña insegura.

  Tc bajo ∧ Uc Inferior al Umbral -> Ns Insegura

Tamaño de la contraseña (Tmc): Son la cantidad de caracteres que debe tener una contraseña para que se pueda considerar como un buen tamaño o malo.

Bueno: Se considera de buen tamaño si cuenta con 9 o más caracteres.

Malo: Se considera que el tamaño es malo si es inferior a 9 caracteres.

Combinación de caracteres (Ccar): Son características con respecto a la cantidad y forma con las cuales se puede decidir el rango en el cual se encuentra la combinación de una contraseña. Esta se puede clasificar como:

Baja: Cumple con 0 a 1 característica.

Media: Cumple con 2 a 3 características.

Alta: Cumple con 3 ó 4 características.

Regla General: Tmc ∧ Ccar -> Um

Si un buen tamaño de la contraseña y una combinación de caracteres alta entonces la contraseña supera el umbral.

Tmc Bueno ∧ Ccar Alta -> Um Superior.

- Si un buen tamaño de la contraseña y una combinación de caracteres media entonces la contraseña esta en un umbral medio.

  Tmc Bueno ∧ Ccar media -> Um Medio.

- Si un buen tamaño de la contraseña y una combinación de caracteres baja entonces la contraseña inferior al umbral.
  Tmc Bueno ∧ Ccar media -> Um Inferior.
- Si un mal tamaño de la contraseña y una combinación de caracteres alta entonces la contraseña esta en un umbral medio.
  Tmc Malo ∧ Ccar Alta -> Um Medio.
- Si un mal tamaño de la contraseña y una combinación de caracteres media entonces la contraseña inferior al umbral.
  Tmc Malo ∧ Ccar medio -> Um Inferior.
- Si un mal tamaño de la contraseña y una combinación de caracteres baja entonces la contraseña inferior al umbral.
  Tmc Malo ∧ Ccar baja -> Um Inferior.

Número de caracteres (Ncar): Es el número de caracteres que tiene una contraseña este se considera bueno si es mayor a 9 caracteres.

Bueno: Se considera de buen número de caracteres si cuenta con 9 o más caracteres.

Malo: Se considera que el número de caracteres es malo si este es inferior a 9 caracteres.

Regla General: Ncar -> Tmc

- Si el número de caracteres es bueno entonces buen tamaño de la contraseña.
  Ncar bueno -> Tmc bueno
- Si el número de caracteres es malo entonces tamaño de contraseña malo.
  Ncar malo -> Tmc malo

Letras mayúsculas (Lmay): Cantidad de letras mayúsculas que están contenidas en la contraseña.

Alto: Si el número de letras mayúsculas que tiene la contraseña es mayor a 3.

Bajo: Si el número de letras mayúsculas que tiene la contraseña es menor a 3.

Cantidad de Números (Cn): Cantidad de números que están contenidos en la contraseña.

Alto: Si la cantidad de números que tiene la contraseña es mayor a 3.

Bajo: Si la cantidad de números que tiene la contraseña es mayor a 3.

Letras Minúsculas (Lmin): Cantidad de letras minúsculas que están contenidas en la contraseña.

Alto: Si el número de letras minúsculas que tiene la contraseña es mayor a 3.

Bajo: Si el número de letras minúsculas que tiene la contraseña es menor a 3.

Símbolos (Csb): Cantidad de símbolos que están contenidos en la contraseña.

Alto: Si el número de símbolos que tiene la contraseña es mayor a 3.

Bajo: Si el número de símbolos que tiene la contraseña es menor a 3.

Regla General: Lmay ∧ Cn ∧ Lmin ∧ Csb -> Ccar

- Si número de letras mayúsculas alto, número de números alto, número de letras en minúsculas alto y número de símbolos alto entonces tiene una combinación de caracteres alta.

  Lmay alto ∧ Cn alto ∧ Lmin alto ∧ Csb alto -> Ccar alta
- Si número de letras mayúsculas alto, número de números alto, número de letras en minúsculas alto y número de símbolos bajo entonces tiene una combinación caracteres media.

  Lmay alto ∧ Cn alto ∧ Lmin alto ∧ Csb bajo -> Ccar medio
- Si número de letras mayúsculas alto, número de números alto, número de letras en minúsculas bajo y número de símbolos alto entonces tiene una combinación de caracteres media.

  Lmay alto ∧ Cn alto ∧ Lmin bajo ∧ Csb alto -> Ccar medio
- Si número de letras mayúsculas alto, número de números bajo, número de letras en minúsculas alto y número de símbolos alto entonces tiene una combinación de caracteres media.

  Lmay alto ∧ Cn bajo ∧ Lmin alto ∧ Csb alto -> Ccar medio

- Si número de letras mayúsculas bajo, número de números alto, número de letras en minúsculas alto y número de símbolos alto entonces tiene una combinación de caracteres media.

  Lmay bajo ∧ Cn alto ∧ Lmin alto ∧ Csb alto -> Ccar medio
- Si número de letras mayúsculas alto, número de números alto, número de letras en minúsculas bajo y número de símbolos bajo entonces tiene una combinación de caracteres media.

  Lmay alto ∧ Cn alto ∧ Lmin bajo ∧ Csb bajo -> Ccar medio
- Si número de letras mayúsculas alto, número de números bajo, número de letras en minúsculas alto y número de símbolos bajo entonces tiene una combinación de caracteres media.

  Lmay alto ∧ Cn bajo ∧ Lmin alto ∧ Csb bajo -> Ccar medio
- Si número de letras mayúsculas bajo, número de números alto, número de letras en minúsculas alto y número de símbolos bajo entonces tiene una combinación de caracteres media.

  Lmay bajo ∧ Cn alto ∧ Lmin alto ∧ Csb bajo -> Ccar medio
- Si número de letras mayúsculas alto, número de números bajo, número de letras en minúsculas bajo y número de símbolos alto entonces tiene una combinación de caracteres media.

  Lmay alto ∧ Cn bajo ∧ Lmin bajo ∧ Csb alto -> Ccar medio
- Si número de letras mayúsculas bajo, número de números bajo, número de letras en minúsculas alto y número de símbolos alto entonces tiene una combinación de caracteres media.

  Lmay bajo ∧ Cn bajo ∧ Lmin alto ∧ Csb alto -> Ccar medio
- Si número de letras mayúsculas alto, número de números bajo, número de letras en minúsculas bajo y número de símbolos bajo entonces tiene una combinación de caracteres baja.

  Lmay alto ∧ Cn bajo ∧ Lmin bajo ∧ Csb bajo -> Ccar bajo
- Si número de letras mayúsculas bajo, número de números alto, número de letras en minúsculas bajo y número de símbolos bajo entonces tiene una combinación de caracteres baja.

Lmay bajo ∧ Cn alto ∧ Lmin bajo ∧ Csb bajo -> Ccar bajo

- Si número de letras mayúsculas bajo, número de números bajo, número de letras en minúsculas alto y número de símbolos bajo entonces tiene una combinación de caracteres baja.
  Lmay bajo ∧ Cn bajo ∧ Lmin alto ∧ Csb bajo -> Ccar bajo
- Si número de letras mayúsculas bajo, número de números bajo, número de letras en minúsculas bajo y número de símbolos alto entonces tiene una combinación de caracteres baja.
  Lmay bajo ∧ Cn bajo ∧ Lmin bajo ∧ Csb alto -> Ccar bajo
- Si número de letras mayúsculas bajo, número de números bajo, número de letras en minúsculas bajo y número de símbolos bajo entonces tiene una combinación de caracteres baja.
  Lmay bajo ∧ Cn bajo ∧ Lmin bajo ∧ Csb bajo -> Ccar bajo

Velocidad de generación de la contraseña (Vc): Es el tiempo que se demora en generar una contraseña este tiempo está dado en segundos. Este se puede clasificar como:

Bajo: De 0 a 3 segundos.
Medio: De 4 a 7 segundos.
Alto: De 8 a 10 segundos.

Complejidad de la contraseña (Cc): Son el conjunto de características que tiene una contraseña para que sea considerada como compleja. Se puede clasificar como:

Baja: Cumple con 0 a 2 características.
Media: Cumple con 3 a 5 características.
Alta: Cumple con 5 a 6 características.

Regla General: Vc ∧ Cc -> Tc

- Si la velocidad de generación de contraseña alto y la complejidad de la contraseña alto entonces tiempo de crackeo alto.
  Vc alto ∧ Cc alto -> Tc alto

- Si la velocidad de generación de contraseña alto y la complejidad de la contraseña medio entonces tiempo de crackeo medio.
  Vc alto ∧ Cc medio -> Tc medio
- Si la velocidad de generación de contraseña alto y la complejidad de la contraseña bajo entonces tiempo de crackeo bajo.
  Vc alto ∧ Cc bajo -> Tc bajo
- Si la velocidad de generación de contraseña medio y la complejidad de la contraseña alto entonces tiempo de crackeo medio.
  Vc medio ∧ Cc alto -> Tc medio
- Si la velocidad de generación de contraseña medio y la complejidad de la contraseña medio entonces tiempo de crackeo medio.
  Vc medio ∧ Cc medio -> Tc medio
- Si la velocidad de generación de contraseña medio y la complejidad de la contraseña bajo entonces tiempo de crackeo bajo.
  Vc medio ∧ Cc bajo -> Tc bajo
- Si la velocidad de generación de contraseña bajo y la complejidad de la contraseña alto entonces tiempo de crackeo bajo.
  Vc bajo ∧ Cc alto -> Tc bajo
- Si la velocidad de generación de contraseña bajo y la complejidad de la contraseña medio entonces tiempo de crackeo bajo.
  Vc bajo ∧ Cc medio -> Tc bajo
- Si la velocidad de generación de contraseña bajo y la complejidad de la contraseña bajo entonces tiempo de crackeo bajo.
  Vc bajo ∧ Cc bajo -> Tc bajo

Cantidad de letras (Cl): Es el número de letras que están contenidos en una contraseña.

Alto: Contiene más de 3 letras.

Bajo: Contiene de 0 a 2 letras.

Palabra del Lenguaje (Pl): Determina si la contraseña es una palabra convencional que se encuentra en un lenguaje.

Si: Es una palabra del lenguaje.

No: No es una palabra del lenguaje.

Fecha (Fc): Determina si la contraseña es una fecha.

Si: Si es una fecha.

No: No es una fecha.

Cantidad de caracteres especiales (Cce): Determina el número de caracteres especiales que contiene una contraseña.

Alto: Contiene más de 3 caracteres especiales.

Bajo: Contiene de 0 a 2 caracteres especiales.

Cantidad de caracteres repetidos (Ccrep): Determina el número de caracteres repetidos dentro de una contraseña.

Alto: Contiene más de 3 caracteres repetidos.

Bajo: Contiene de 0 a 2 caracteres repetidos.

Regla General: Cl ∧ Cn ∧ Fc ∧ Pl ∧ Tmc ∧ Cce ∧ Ccrep -> Cc

- Si cantidad de números alto, cantidad de letras alta, palabra del lenguaje no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña alta.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc alto
- Si cantidad de números alta, cantidad de letras alta, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc medio
- Si cantidad de números alta, cantidad de letras alta, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.

Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc medio

- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña alto, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña media.

  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha no, el tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc medio

- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña alto, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña media.
  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc medio
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc medio

- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña buena, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras alta, palabra del diccionario no, fecha no, tamaño de la contraseña buena, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha Si, tamaño de la contraseña mala, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc mala ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alta, cantidad de letras alta, palabra del diccionario si, fecha no, tamaño de la contraseña mala, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

Cl alto ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc mala ∧ Cce alto ∧ Ccrep bajo -> Cc medio

- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc mala ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc mala ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc buena ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña alto, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc buena ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc buena ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, hay caracteres repetidos entonces complejidad contraseña media.

  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc buena ∧ Cce alto ∧ Ccrep bajo -> Cc medio

- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña buena, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc buena ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc buena ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña media.
  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc medio

- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña media.
  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.
  Cl alto ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, hay caracteres repetidos bajo entonces complejidad contraseña media.

Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc medio

- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña media.

  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc medio
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.

  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña baja.

  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc baja

- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña baja.

Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc baja

- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc malo ∧ Cce alto ∧ Ccrep alto -> Cc baja

- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja

- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc baja

- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña malo, número de caracteres especiales alto, caracteres repetidos bajo entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc malo ∧ Cce alto ∧ Ccrep bajo -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha si, tamaño de la contraseña bueno, número de caracteres especiales alto, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc si ∧ Tmc bueno ∧ Cce alto ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras bajo, palabra del diccionario no, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.

Cl bajo ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja

- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras bajo, palabra del diccionario si, fecha no, tamaño de la contraseña bueno, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl bajo ∧ Cn alto ∧ Pl si ∧ Fc no ∧ Tmc bueno ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números bajo, cantidad de letras alto, palabra del diccionario no, fecha no, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn bajo ∧ Pl no ∧ Fc no ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja
- Si cantidad de números alto, cantidad de letras alto, palabra del diccionario no, fecha si, tamaño de la contraseña malo, número de caracteres especiales bajo, caracteres repetidos alto entonces complejidad contraseña baja.
  Cl alto ∧ Cn alto ∧ Pl no ∧ Fc si ∧ Tmc malo ∧ Cce bajo ∧ Ccrep alto -> Cc baja

Velocidad de la maquina (Vmaq): Es la velocidad de procesamiento que tiene el equipo.

Bajo: De 0 a 300

Medio: De 400 a 700

Alto: De 800 a 1000

Tipo de entrada (Te): Es la forma como se va a realizar el crackeo que puede ser incremental o diccionario.

Incremental: 0 El crackeo se hace de manera incremental.

Diccionario: 1 El crackeo se hace usando diccionarios.

Regla General: Vmaq ∧ Te -> Vc

- Si la velocidad de la maquina alto y el tipo de entrada incremental entonces velocidad de generación de contraseña media.

Vmaq alto ∧ Te incremental -> Vc media

- Si la velocidad de la maquina alto y el tipo de entrada diccionario entonces velocidad de generación de contraseña alta.
  Vmaq alto ∧ Te diccionario -> Vc alta
- Si la velocidad de la maquina medio y el tipo de entrada incremental entonces velocidad de generación de contraseña alta.
  Vmaq medio ∧ Te incremental -> Vc bajo
- Si la velocidad de la maquina medio y el tipo de entrada diccionario entonces velocidad de generación de contraseña media.
  Vmaq medio ∧ Te diccionario -> Vc media
- Si la velocidad de la maquina bajo y el tipo de entrada incremental entonces velocidad de generación de contraseña bajo.
  Vmaq bajo ∧ Te incremental -> Vc bajo
- Si la velocidad de la maquina bajo y el tipo de entrada diccionario entonces velocidad de generación de contraseña bajo.
  Vmaq bajo ∧ Te diccionario -> Vc bajo

Control validez de carnet:

Objetivo: Identificar si un carnet institucional es o no valido.

Nivel de permisividad (Nper): Es el que determina revisar que tan estricta es la solicitud de la información que se puede obtener con el carnet institucional. Este se clasifica como:

Bajo: Se obtiene 1 a 2 datos almacenados en el carnet institucional.

Alto: Se obtiene 3 a 4 datos almacenados en el carnet institucional.

Porcentaje de validez de información (Pvi): Es un valor numérico el cual da información de que tan válida es la información almacenada en el carnet según la información que se puede obtener con el carnet institucional. Este se clasifica como:

Bajo: Tiene de 0 a 2 elementos almacenados en el carnet y el sistema.

Medio: Tiene de 3 a 4 elementos almacenados en el carnet y el sistema.

Alto: Tiene de 4 a 6 elementos almacenados en el carnet y el sistema.

Nivel de validez (Nv): Es la medida que indica si un carnet es válido o inválido.

Regla General: Nper ∧ Pvi -> Nv

- Si el nivel de permisividad alto y el porcentaje validez información alto entonces carnet valido.
  Nper alto ∧ Pvi alto -> Nv valido
- Si el nivel de permisividad alto y el porcentaje validez información medio entonces carnet valido.
  Nper alto ∧ Pvi medio -> Nv valido
- Si el nivel de permisividad alto y el porcentaje validez información bajo entonces carnet inválido.
  Nper alto ∧ Pvi bajo -> Nv valido
- Si el nivel de permisividad bajo y el porcentaje validez información alto entonces carnet inválido.
  Nper bajo ∧ Pvi alto -> Nv valido
- Si el nivel de permisividad bajo y el porcentaje validez información medio entonces carnet inválido.
  Nper bajo ∧ Pvi medio -> Nv inválido
- Si el nivel de permisividad bajo y el porcentaje validez información bajo entonces carnet inválido.
  Nper bajo ∧ Pvi bajo -> Nv inválido

Criticidad del proceso (Cp): Indica que tan crítico es un proceso que se está realizando en un momento dado. Este se clasifica como:

Bajo: Proceso no critico.

Alto: Proceso critico.

Rango de permisividad (Rper): Es la medida que indica que tan estricto es el sistema al verificar los datos. Este se clasifica como:

Bajo: De 0 a 3. El sistema no es estricto con la información.

Medio: De 4 a 7. El sistema tiene una rigurosidad media.

Alto: De 8 a 10. El sistema tiene una alta rigurosidad.

Regla General: Cp ∧ Rper -> Nper

- Si criticidad de proceso alta y rango de permisividad alto entonces el nivel de permisividad alto.
  Cp alta ∧ Rper alto -> Nper alto
- Si criticidad de proceso alta y rango de permisividad medio entonces el nivel de permisividad bajo.
  Cp alta ∧ Rper medio -> Nper bajo
- Si criticidad de proceso alta y rango de permisividad bajo entonces el nivel de permisividad bajo.
  Cp alto ∧ Rper bajo -> Nper bajo
- Si criticidad de proceso bajo y rango de permisividad alto entonces el nivel de permisividad alto.
  Cp bajo ∧ Rper alto -> Nper alto
- Si criticidad de proceso bajo y rango de permisividad medio entonces el nivel de permisividad bajo.
  Cp bajo ∧ Rper medio -> Nper bajo
- Si criticidad de proceso bajo y rango de permisividad bajo entonces el nivel de permisividad bajo.
  Cp bajo ∧ Rper bajo -> Nper bajo

Criticidad de la Dependencia (Cdp): Es la criticidad de la dependencia en la cual se está realizando un determinado proceso que se va a verificar con el respectivo control. Este puede ser:

Bajo: De 0 a 3. Dependencia poco critica.

Medio: De 4 a 7. Dependencia medianamente critica.

Alto: De 8 a 10. Dependencia altamente critica.

Manejo de información crítica (Mcri): Indica que tan crítica es la información que se está manejando en el proceso.

Bajo: De 0 a 3. Información poco critica.

Media: De 4 a 7. Información medianamente critica.

Alto: De 8 a 10. Información altamente critica.

Regla General: Cdp ∧ Mcri -> Cp

- Si la criticidad de la dependencia alta y el manejo información crítica alto entonces la criticidad proceso alta.
  Cdp alta ∧ Mcri alta -> Cp alta
- Si la criticidad de la dependencia alta y el manejo información crítica medio entonces la criticidad proceso medio.
  Cdp alta ∧ Mcri medio -> Cp bajo
- Si la criticidad de la dependencia alta y el manejo información crítica bajo entonces la criticidad proceso bajo.
  Cdp alta ∧ Mcri bajo -> Cp bajo
- Si la criticidad de la dependencia media y el manejo información crítica alto entonces la criticidad proceso media.
  Cdp media ∧ Mcri alta -> Cp bajo
- Si la criticidad de la dependencia media y el manejo información crítica media entonces la criticidad proceso media.
  Cdp media ∧ Mcri media -> Cp bajo
- Si la criticidad de la dependencia media y el manejo información crítica bajo entonces la criticidad proceso bajo.
  Cdp media ∧ Mcri bajo -> Cp bajo
- Si la criticidad de la dependencia bajo y el manejo información crítica alto entonces la criticidad proceso bajo.
  Cdp bajo ∧ Mcri alto -> Cp bajo
- Si la criticidad de la dependencia bajo y el manejo información crítica medio entonces la criticidad proceso bajo.
  Cdp bajo ∧ Mcri medio -> Cp bajo
- Si la criticidad de la dependencia bajo y el manejo información crítica bajo entonces la criticidad proceso bajo.
  Cdp bajo ∧ Mcri bajo -> Cp bajo

Rango de permisividad anterior (RperAnt): Es la medida que indica que tan estricto es el sistema al verificar los datos en un punto anterior. Este se clasifica como:

Bajo: De 0 a 3. El sistema no es estricto con la información.

Medio: De 4 a 7. El sistema tiene una rigurosidad media.

Alto: De 8 a 10. El sistema tiene una alta rigurosidad.

Nivel de riesgo actual (Nrac): Probabilidad actual que ocurra un evento que afecte el proceso. Este se clasifica:

Bajo: De 0 a 3. Poco probable.

Medio: De 4 a 7. Medianamente probable.

Alto: De 8 a 10. Muy probable.

Regla General: RperAnt ∧ Nrac -> Rper

- Si el rango permisividad anterior alto y el nivel de riesgo actual alto entonces rango de permisividad alto.
  RperAnt alto ∧ Nrac alto -> Rper alto
- Si el rango permisividad anterior alto y el nivel de riesgo actual medio entonces rango de permisividad medio.
  RperAnt alto ∧ Nrac medio -> Rper medio
- Si el rango permisividad anterior alto y el nivel de riesgo actual bajo entonces rango de permisividad bajo.
  RperAnt alto ∧ Nrac bajo -> Rper bajo
- Si el rango permisividad anterior medio y el nivel de riesgo actual alto entonces rango de permisividad medio.
  RperAnt medio ∧ Nrac alto -> Rper medio
- Si el rango permisividad anterior medio y el nivel de riesgo actual medio entonces rango de permisividad medio.
  RperAnt medio ∧ Nrac medio -> Rper medio
- Si el rango permisividad anterior medio y el nivel de riesgo actual bajo entonces rango de permisividad bajo.
  RperAnt medio ∧ Nrac bajo -> Rper bajo

- Si el rango permisividad anterior bajo y el nivel de riesgo actual alto entonces rango de permisividad medio.
  RperAnt bajo ∧ Nrac alto -> Rper medio
- Si el rango permisividad anterior bajo y el nivel de riesgo actual medio entonces rango de permisividad bajo.
  RperAnt bajo ∧ Nrac medio -> Rper bajo
- Si el rango permisividad anterior bajo y el nivel de riesgo actual bajo entonces rango de permisividad bajo.
  RperAnt bajo ∧ Nrac bajo -> Rper bajo

Información del carnet (InfoCar): Información que se encuentra almacenada en el chip inteligente incrustada en el carnet institucional. Este se clasifica como.

Alto: 1 Información almacenada en el carnet.

Bajo: 0 Información no almacenada en el carnet.

Información del sistema (InfoSis): Información que se encuentra almacenada en el sistema

Alto: 1 Información almacenada en el carnet.

Bajo: 0 Información no almacenada en el carnet.

Regla General: InfoCar ∧ InfoSis -> Pvi

- Si la información del carnet alta y la información en el sistema alta entonces porcentaje de validez de información alto.
  InfoCar alta ∧ InfoSis alta -> Pvi alto
- Si la información del carnet alta y la información en el sistema bajo entonces porcentaje de validez de información bajo.
  InfoCar alta ∧ InfoSis bajo -> Pvi bajo
- Si la información del carnet bajo y la información en el sistema alta entonces porcentaje de validez de información bajo.
  InfoCar bajo ∧ InfoSis alta -> Pvi bajo

- Si la información del carnet bajo y la información en el sistema bajo entonces porcentaje de validez de información bajo.
  InfoCar bajo ∧ InfoSis bajo -> Pvi bajo

Identificación en el carnet (Idcar): Indica si la identificación se encuentra almacenada en el carnet. Está clasificado como:

Bajo: 0. La identificación se encuentra almacenada.

Alto: 1. La identificación no se almacenada.

Nombres en el carnet (Ncar): Indica si los nombres se pueden obtener mediante la información almacenada en el carnet. Está clasificado como:

Bajo: 0. Los nombres no se pueden obtener.

Alto: 1. Los nombres no se pueden obtener.

Huella en el carnet (Hcar): Indica si la huella se encuentra almacenada en el carnet. Está clasificado como:

Bajo: 0. La huella se encuentra almacenada.

Alto: 1. La huella no se almacenada.

Fotografía en el carnet (Fcar): Indica si la fotografía se pueden obtener mediante la información almacenada en el carnet. Está clasificado como:

Bajo: 0. La fotografía no se puede obtener.

Alto: 1. La fotografía no se puede obtener.

Regla General: Idcar ∧ Ncar ∧ Hcar ∧ Fcar -> InfoCar

- Si carnet tiene identificación alto, nombres alto, huella alto y fotografía alto entonces información almacenada en el carnet alta.
  Idcar alto ∧ Ncar alto ∧ Hcar alto ∧ Fcar alto -> InfoCar alta
- Si carnet tiene identificación alto, nombres alto, huella alto y fotografía bajo entonces información almacenada en el carnet alto.
  Idcar alto ∧ Ncar alto ∧ Hcar alto ∧ Fcar bajo -> InfoCar alto

- Si carnet tiene identificación alto, nombres alto, huella bajo y fotografía alto entonces información almacenada en el carnet bajo.
  Idcar alto ∧ Ncar alto ∧ Hcar bajo ∧ Fcar alto -> InfoCar bajo
- Si carnet tiene identificación alto, nombres bajo, huella alto y fotografía alto entonces información almacenada en el carnet alto.
  Idcar alto ∧ Ncar bajo ∧ Hcar alto ∧ Fcar alto -> InfoCar alto
- Si carnet tiene identificación bajo, nombres alto, huella alto y fotografía alto entonces información almacenada en el carnet bajo.
  Idcar bajo ∧ Ncar alto ∧ Hcar alto ∧ Fcar alto -> InfoCar bajo
- Si carnet tiene identificación alto, nombres bajo, huella alto y fotografía bajo entonces información almacenada en el carnet alto.
  Idcar alto ∧ Ncar bajo ∧ Hcar alto ∧ Fcar bajo -> InfoCar alto
- Si carnet tiene identificación bajo, nombres alto, huella alto y fotografía alto entonces información almacenada en el carnet bajo.
  Idcar bajo ∧ Ncar alto ∧ Hcar alto ∧ Fcar alto -> InfoCar bajo
- Si carnet tiene identificación alto, nombres alto, huella bajo y fotografía bajo entonces información almacenada en el carnet bajo.
  Idcar alto ∧ Ncar alto ∧ Hcar bajo ∧ Fcar bajo -> InfoCar bajo
- Si carnet tiene identificación alto, nombres bajo, huella bajo y fotografía alto entonces información almacenada en el carnet bajo.
  Idcar alto ∧ Ncar bajo ∧ Hcar bajo ∧ Fcar alto -> InfoCar bajo
- Si carnet tiene identificación bajo, nombres bajo, huella alto y fotografía alto entonces información almacenada en el carnet bajo.
  Idcar bajo ∧ Ncar bajo ∧ Hcar alto ∧ Fcar alto -> InfoCar bajo
- Si carnet tiene identificación alto, nombres bajo, huella bajo y fotografía bajo entonces información almacenada en el carnet bajo.
  Idcar alto ∧ Ncar bajo ∧ Hcar bajo ∧ Fcar bajo -> InfoCar bajo
- Si carnet tiene identificación bajo, nombres alto, huella bajo y fotografía bajo entonces información almacenada en el carnet bajo.
  Idcar bajo ∧ Ncar alto ∧ Hcar bajo ∧ Fcar bajo -> InfoCar bajo

- Si carnet tiene identificación bajo, nombres bajo, huella alto y fotografía bajo entonces información almacenada en el carnet bajo.
  Idcar bajo ∧ Ncar bajo ∧ Hcar alto ∧ Fcar bajo -> InfoCar bajo
- Si carnet tiene identificación bajo, nombres bajo, huella bajo y fotografía alto entonces información almacenada en el carnet bajo.
  Idcar bajo ∧ Ncar bajo ∧ Hcar bajo ∧ Fcar alto -> InfoCar bajo
- Si carnet tiene identificación bajo, nombres bajo, huella bajo y fotografía bajo entonces información almacenada en el carnet bajo.
  Idcar bajo ∧ Ncar bajo ∧ Hcar bajo ∧ Fcar bajo -> InfoCar bajo

Identificación en el sistema (Idsis): Indica si la identificación se encuentra almacenada en el sistema. Está clasificado como:

Bajo: 0. La identificación se encuentra almacenada.

Alto: 1. La identificación no se almacenada.

Nombres en el sistema (Nsis): Indica si los nombres se encuentran almacenados en el sistema. Está clasificado como:

Bajo: 0. Los nombres no se pueden obtener.

Alto: 1. Los nombres no se pueden obtener.

Código en el sistema (Codsis): Indica si el código se encuentra almacenada en el sistema. Está clasificado como:

Bajo: 0. El código se encuentra almacenado.

Alto: 1. El código no se encuentra almacenado.

Fotografía en el sistema (Fotsis): Indica si la fotografía se encuentra almacenada en el sistema. Está clasificado como:

Bajo: 0. La fotografía se encuentra almacenada.

Alto: 1. La fotografía no se almacenada.

Regla General: Idsis ∧ Nsis ∧ Codsis ∧ Fotsis -> InfoSis

- Si se encuentra registrado en el sistema documento de identidad alto, nombres alto, código alto y fotografía alto entonces se encuentra la información en el sistema alto.

  Idsis alto ∧ Nsis alto ∧ Codsis alto ∧ Fotsis alto -> InfoSis alto
- Si se encuentra registrado en el sistema documento de identidad alto, nombres alto, código alto y fotografía bajo entonces se encuentra la información en el sistema alto.

  Idsis alto ∧ Nsis alto ∧ Codsis alto ∧ Fotsis bajo -> InfoSis alto
- Si se encuentra registrado en el sistema documento de identidad alto, nombres alto, código bajo y fotografía alto entonces se encuentra la información en el sistema bajo.

  Idsis alto ∧ Nsis alto ∧ Codsis bajo ∧ Fotsis alto -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad alto, nombres bajo, código alto y fotografía alto entonces se encuentra la información en el sistema bajo.

  Idsis alto ∧ Nsis bajo ∧ Codsis alto ∧ Fotsis alto -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad bajo, nombres alto, código alto y fotografía alto entonces se encuentra la información en el sistema bajo.

  Idsis bajo ∧ Nsis alto ∧ Codsis alto ∧ Fotsis alto -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad alto, nombres alto, código bajo y fotografía bajo entonces se encuentra la información en el sistema bajo.

  Idsis alto ∧ Nsis alto ∧ Codsis bajo ∧ Fotsis bajo -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad alto, nombres bajo, código alto y fotografía bajo entonces se encuentra la información en el sistema bajo.

  Idsis alto ∧ Nsis bajo ∧ Codsis alto ∧ Fotsis bajo -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad bajo, nombres alto, código alto y fotografía bajo entonces se encuentra la información en el sistema bajo.

Idsis bajo ∧ Nsis alto ∧ Codsis alto ∧ Fotsis bajo -> InfoSis bajo

- Si se encuentra registrado en el sistema documento de identidad alto, nombres alto, código alto y fotografía alto entonces se encuentra la información en el sistema bajo.

  Idsis alto ∧ Nsis bajo ∧ Codsis bajo ∧ Fotsis alto -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad bajo, nombres alto, código bajo y fotografía alto entonces se encuentra la información en el sistema bajo.

  Idsis bajo ∧ Nsis alto ∧ Codsis bajo ∧ Fotsis alto -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad bajo, nombres alto, código bajo y fotografía alto entonces se encuentra la información en el sistema bajo.

  Idsis bajo ∧ Nsis bajo ∧ Codsis alto ∧ Fotsis alto -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad alto, nombres alto, código bajo y fotografía bajo entonces se encuentra la información en el sistema bajo.

  Idsis alto ∧ Nsis bajo ∧ Codsis bajo ∧ Fotsis bajo -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad bajo, nombres bajo, código bajo y fotografía alto entonces se encuentra la información en el sistema bajo.

  Idsis bajo ∧ Nsis bajo ∧ Codsis bajo ∧ Fotsis alto -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad bajo, nombres alto, código alto y fotografía bajo entonces se encuentra la información en el sistema bajo.

  Idsis bajo ∧ Nsis alto ∧ Codsis alto ∧ Fotsis bajo -> InfoSis bajo
- Si se encuentra registrado en el sistema documento de identidad bajo, nombres bajo, código bajo y fotografía bajo entonces se encuentra la información en el sistema bajo.

  Idsis bajo ∧ Nsis bajo ∧ Codsis bajo ∧ Fotsis bajo -> InfoSis bajo