Anexo A. DOCUMENTOS OBLIGATORIOS DE LA FASE PLAN DEL SGSI

A.1. Acta de inicio del proyecto del SGSI

El acta de inicio del SGSI representa la aprobación de la dirección al proyecto de SGSI para ser realizado en el procedimiento *Inscripciones y Admisiones* de DARCA de la Universidad del Cauca. Se explica al jefe DARCA los aspectos más relevantes de un SGSI, y se definen las responsabilidades pertinentes. Esta acta es un registro que permite dar cumplimiento al documento obligatorio "Registros de las decisiones de la dirección". Esta acta se realiza en el marco del proyecto titulado "Implantación de la fase Ejecución de un SGSI adaptando un marco de referencia con base en la norma ISO/IEC 27001:2013."

Fecha	17/04/2017	Hora inicio	7:00 AM	Hora de terminación	7:40 AM	N° de acta	001

1. Asistentes a la reunión

N°	Nombre	Cargo
1	Marisol Zuñiga **(MZ)**	Jefe de DARCA
2	Deisy Francely Imbachi **(DI)**	Estudiante
3	Fabio Cerón **(FC)**	Estudiante

2. Agenda de la reunión

N°	Tema	Tiempo
1	Presentación del proyecto para la implementación de un SGSI en DARCA	30 minutos
2	Definición de las responsabilidades que tendrá el Jefe de DARCA en el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI).	30 minutos

1. El proyecto se implementa en el marco de la NTC ISO/IEC 27001:2013 que define una serie de cláusulas necesarias para establecer el SGSI al interior del proceso *Inscripciones y Admisiones* de DARCA. La necesidad de implantar un SGSI en este proceso se hace evidente debido a que la información que se maneja es muy delicada y hay que implementar todas las medidas necesarias para protegerla.
2. Para realizar una implementación exitosa de un SGSI es necesario contar con el liderazgo y compromiso de la dirección de DARCA, de manera que facilite y disponga de los recursos y espacios necesarios para llevar a cabo todas y cada una de las actividades de implementación del SGSI.

   A continuación de definen las responsabilidades que tendrá que asumir el Jefe de DARCA:
   - Asegurar los recursos necesarios para la planeación, implementación y mantenimiento del SGSI.
   - Revisión periódica de documentos y controles del SGSI para asegurar que se alcancen los objetivos propuestos.

- Analizar los incidentes de seguridad y notificar inmediatamente a las autoridades correspondientes.
- Definir los protocolos necesarios que le permitan monitorear que los propietarios de los activos de información cumplan con lo estipulado en el SGSI.
- Hacer seguimiento a la implementación y seguimiento de los controles.

Firman los asistentes

N°	Nombre	Firma
1	Marisol Zuñiga **(MZ)**	
2	Deisy Francely Imbachi **(DI)**	
3	Fabio Cerón **(FC)**	

Fig. 1. Acta de inicio de proyecto de SGSI

A.2. Reporte General de Valoración de Riesgos

TABLA I. Comparación de la norma ISO/IEC 27005:2011 y OCTAVE-S para Valoración de Riesgos

ISO 27005:2011		OCTAVE-S		
Valoración del riesgo en la seguridad de la información (Numeral 8)	Identificación del riesgo (Numeral 8.2)	Fase 1	a. Establecimiento de criterios de evaluación de impacto	Construcción de perfiles de amenaza
			b. Identificación de activos de información	
			c. Evaluación de procedimientos de seguridad de DARCA	
			d. Selección de activos críticos	
			e. Identificación de los requisitos de seguridad para los activos críticos	
			f. Identificación de las amenazas a los activos críticos	
		Fase 2	a. Análisis de vías de acceso	Identificar las vulnerabilidades de la infraestructura
			b. Análisis de los procesos tecnológicos relacionados	
	Análisis de riesgo (Numeral 8.3)	Fase 2	a. Evaluación de los impactos de las amenazas	Desarrollo de estrategia y planes de seguridad
			b. Establecimiento de criterios de evaluación de probabilidad	
			c. Evaluación de probabilidades de amenazas	
	Evaluación del riesgo (Numeral 8.4)	Análisis de resultados de las fases 1 y 2.	d. Cálculo del valor del riesgo	
Tratamiento del riesgo en la seguridad de la información (Numeral 9)	Tratamiento del riesgo (Numerales 9.1; 9.2; 9.3 y 9.4)	Fase 3	e. Selección planteamiento de mitigación	
			f. Desarrollo de planes de mitigación de riesgo	

A continuación, se describe la valoración de riesgos con base en la adaptación de la metodología OCTAVE-S propuesta por J. P. Martinez Pulido y D. F. Espinosa Tafur (2015). Como se puede ver en la Tabla 1, la adaptación de OCTAVE-S para la valoración de riesgos está dividida en tres fases: Construcción de perfiles de amenaza; Identificar las vulnerabilidades de la infraestructura; Desarrollo de estrategia y planes de seguridad.

Fase 1. Construcción de perfiles de amenaza

Esta fase contiene 6 actividades:

a) Establecimiento de criterios de evaluación de impacto: Se definieron un conjunto de medidas cualitativas y cuantitativas para evaluar los efectos de los riesgos. (Paso 1 de OCTAVE-S)

b) Identificación de activos de información: Se identificaron 68 activos del proceso Inscripciones y Admisiones, los cuales se clasificaron según las categorías de la norma ISO/IEC 27002. (Paso 2 de OCTAVE-S)

c) Evaluación de procedimientos de seguridad de DARCA: Se evaluaron las áreas de seguridad de seguridad del proceso Inscripciones y Admisiones. (Paso 3 y 4 de OCTAVE-S)

d) Selección de activos críticos: Se identificaron 15 activos críticos (Paso 5, 6, 7. 8, 9 de OCTAVE-S

e) Identificación de los requisitos de seguridad para los activos críticos: Se obtuvieron los requisitos de seguridad (confidencialidad, integridad y disponibilidad) que debería tener cada activo crítico. (Pasos 10 y 11 de OCTAVE-S)

f) Identificación de las amenazas a los activos críticos: Se identificaron actores internos y externos que podrían amenazar los activos críticos. (Paso 12, 13, 14, 15, 16 de OCTAVE-S)

Fase 2. Identificación de las vulnerabilidades de la infraestructura

Esta fase se divide en dos actividades:

a) Análisis de vías de acceso: Se establecieron los sistemas más relevantes ligados a cada activo crítico. (Paso 17 y 18 de OCTAVE-S)

b) Análisis de los procesos tecnológicos relacionados: Se realizó un análisis de los activos desde el punto de vista de la infraestructura. (Paso 19, 20, 21 de OCTAVE-S)

Fase 3. Desarrollo de estrategia y planes de seguridad

Esta fase se divide en las siguientes actividades:

a) Evaluación de los impactos de las amenazas: Se identificaron los impactos potenciales y se les asigno una medida cualitativa y cuantitativa. (Paso 24 de OCTAVE-S)

b) Establecimiento de criterios de evaluación de probabilidad: Se definieron medidas de probabilidad basados en la frecuencia de ocurrencia de una amenaza. (Paso 23 de OCTAVE-C)

c) Evaluación de probabilidades de amenazas: A las amenazas se les asignó un valor de probabilidad cualitativa y cuantitativa con base en los resultados del punto anterior. (Paso 22 de OCTAVE-S)

d) Cálculo del valor del riesgo: Se encontró el valor de riesgo para cada uno de los 15 activos críticos teniendo en cuenta los criterios y valores encontrados anteriormente como por ejemplo el valor de impacto de amenaza. (Propio)

e) Selección planteamiento de mitigación: Se seleccionaron áreas de práctica de seguridad para la mitigación. (Paso 26, 27 de OCTAVE-S).

f) Desarrollo de planes de mitigación de riesgo. Se crearon planes de mitigación para cada área de práctica de seguridad (Paso 28 de OCTAVE-S)

A.3. Declaración de Aplicabilidad - SoA

La Tabla II, muestra la Declaración de Aplicabilidad donde se sintetizan los objetivos de control y controles del mapeo anterior.

TABLA II. Declaración de Aplicabilidad del procedimiento *Inscripciones y Admisiones*

	Control Seleccionado	**Control Implementado Si/No**	**Estado actual**
Dominio	**A.5** Políticas de seguridad de la información		
Objetivo de Control	**A.5.1** Orientación de la dirección para la gestión de la seguridad de la información. Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos de DARCA, con la legislación y reglamentación pertinentes.		
Control 1	**A.5.1.1 Políticas para la seguridad de la información** La dirección debería definir, aprobar y publicar un conjunto de políticas para la seguridad de la información; y comunicar las políticas a los empleados de DARCA y a las partes externas pertinentes.	Existencia de la política institucional	Inicial
Control 2	**A.5.1.2 Revisión de las políticas para la seguridad de la información** Las políticas para la seguridad de la información se deberían revisar a intervalos planificados (o en caso de que se produzcan cambios significativos) para garantizar su conveniencia, adecuación y eficacia continuas.	No	Inicial
Dominio	**A.7** Seguridad de los recursos humanos		
Objetivo de Control	**A.7.2** Durante la ejecución del empleo. Asegurarse de que los empleados y contratistas tomen conciencia de las responsabilidades de seguridad de la información		
Control 3	**A.7.2.1 Responsabilidades de la dirección** La dirección debería requerir a empleados y contratistas aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la Universidad del Cauca.	No	No Existente
Control 4	**A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información** Todos los empleados de DARCA y en donde sea relevante deberían recibir un entrenamiento adecuado y actualizaciones regulares sobre las políticas y procedimientos de la Universidad del Cauca que sean relevantes para las funciones de su cargo	No	No Existente
Dominio	**A.9** Control de acceso		
Objetivo de Control	**A.9.1** Requisitos de DARCA para control de acceso. Limitar el acceso a información y a instalaciones de procesamiento de información		
Control 5	**A.9.1.1 Política de control de acceso** Se debería establecer, documentar y revisar una política de control de acceso en base a las necesidades de seguridad de DARCA	Si	Administrado
Control 6	**A.9.1.2 Acceso a redes y a servicios de red** Se debería permitir el acceso a la red y a los servicios de red solamente a los usuarios que hayan sido autorizados específicamente	Si	Administrado por DivTIC
Dominio	**A.11** Seguridad física y del entorno		

Objetivo de Control	**A.11.1** Áreas seguras. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización		
Control 7	**A.11.1.2 Controles de Acceso Físico** Las áreas de seguridad deberían estar protegidos por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado	Si	Limitado
Control 8	**A.11.1.3 Seguridad de oficinas, recintos e instalaciones** Se debería asignar y aplicar la seguridad física a oficinas, recintos e instalaciones	Si	Limitado
Objetivo de Control	**A.11.2** Equipos. Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización		
Control 9	**A.11.2.9 Política de escritorio limpio y pantalla limpia** Se debería adoptar una política de escritorio limpio para los papeles y dispositivos de almacenamiento removibles, y una policía de pantalla limpia en los locales de procesamiento de información	No	No Existente
Dominio	**A.12** Seguridad de las operaciones		
Objetivo de Control	**A.12.1** Procedimientos operacionales y responsabilidades. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información		
Control 10	**A.12.1.1 Procedimientos de operación documentados** Se deberían documentar los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten	Si	Administrado
Objetivo de Control	**A.12.4** Registro y Seguimiento. Registrar eventos y generar evidencia		
Control 11	**A.12.4.1 Registro de eventos** Se deberían elaborar, conservar y revisar regularmente los registros acerca de las actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información.	No	No Existente
Objetivo de Control	**A.12.6** Gestión de vulnerabilidad Técnica		
Control 12	**A.12.6.1 Gestión de las vulnerabilidades técnicas** Se debería obtener información oportuna de las vulnerabilidades técnicas de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados	No	No Existente
Dominio	**A.13** Seguridad de las Comunicaciones		
Objetivo de Control	**A.13.2** Transferencia de Información		
Control 13	**A.13.2.1 Políticas y procedimientos de transferencia de información** Se deberían establecer políticas, procedimientos y controles de transferencia formales con objeto de proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones	Existencia de medidas informales	Inicial
Dominio	**A.15** Relaciones con los proveedores		
Objetivo de Control	**A.15.1** Seguridad de la información en las relaciones con los proveedores. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores		
Control 14	**A.15.1.1 Política de seguridad de la información para relación con proveedores**	No	No Existente

	Se deberían acordar con los proveedores los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, y esto debería documentarse		
Control 15	**A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores** Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pudiera tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Si	Limitado
Control 16	**A.15.1.3 Cadena de suministro de tecnología de información y comunicación** Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	No	No Existente
Objetivo de Control	**A.15.2.** Gestión de la prestación de servicios de proveedores. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores		
Control 17	**A.15.2.1 Seguimiento y revisión de los servicios de los proveedores** Se debería realizar seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores	No	No Existente
Dominio	**A.16** Gestión de incidentes de seguridad de la información		
Objetivo de Control	**A.16.1** Gestión de incidentes y mejoras en seguridad de la información. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades		
Control 18	**A.16.1.1 Responsabilidades y procedimientos** Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de la información	No	No Existente
Control 19	**A.16.1.3 Reporte de debilidades de seguridad de la información** Todos los empleados y contratistas que son usuarios de los servicios y sistemas de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de la información de los mismos	No	No Existente
Control 20	**A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos** Los eventos de seguridad de la información se deberían evaluar y decidir se clasificarían como incidentes de seguridad de la información	No	No Existente
Control 21	**A.16.1.5 Respuesta a incidentes de seguridad de la información** Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	No	No Existente
Dominio	**A.17** Aspectos de seguridad de la información de la gestión de continuidad del negocio		
Objetivo de Control	**A.17.1** Continuidad de seguridad de la información. La continuidad de la seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
Control 22	**A.17.1.1 Planificación de la continuidad de la seguridad de la información** Se deberían determinar los requisitos de la organización para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre	No	No Existente

Control 23	**A.17.1.2 Implementación de la continuidad de la seguridad de la información** Se deberían establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información ante una situación adversa	No	No Existente
Control 24	**A.17.1.3 Verificación, revisión y evaluación de la seguridad de la información** Se deberían verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados con objeto de garantizar su validez y eficacia durante situaciones adversas	No	No Existente
Dominio	**A.18** Cumplimiento		
Objetivo de Control	**A.18.1** Cumplimiento de requisitos legales y contractuales. Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad		
Control 25	**A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales** Todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la organización para cumplirlos, deberían ser explícitamente identificados, documentados y actualizados para cada uno de los sistemas de información y para la organización	No	No Existente
Control 26	**A.18.1.5 Reglamentación de controles criptográficos** Se deberían utilizar controles cifrados en conformidad con todos los acuerdos, legislación y de regulación relevantes	No	No Existente
Objetivo de Control	**A.18.2** Revisiones de seguridad de la información. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales		
Control 27	**A.18.2.1 Revisión independiente de la seguridad de la información** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar de manera independiente a intervalos planificados o cuando ocurran cambios significativos	No	No Existente
Control 28	**A.18.2.2 Cumplimiento con las políticas y normas de seguridad** Los directivos se deberían revisar con regularidad el procesamiento y procedimientos de información dentro de su área de responsabilidad con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad	No	No Existente

Como se puede ver en la Tabla 13 en el SoA se establece el estado actual en que se encuentran los controles. Este estado obedece la siguiente clasificación:

No existente: Carencia total de una política, procedimiento, control, etc.

Inicial: Se ha comenzado a implementar medidas, pero se requiere de un importante trabajo para cumplir con los requisitos de seguridad.

Limitado: Medidas de seguridad en desarrollo, pero no completas.

Definido: Es desarrollo de la medida es casi completo, pero aún no tiene el suficiente detalle

Administrado: El desarrollo de la medida de seguridad esta completado. Hace falta un procedimiento formal y/o documentar resultados y eficacia.

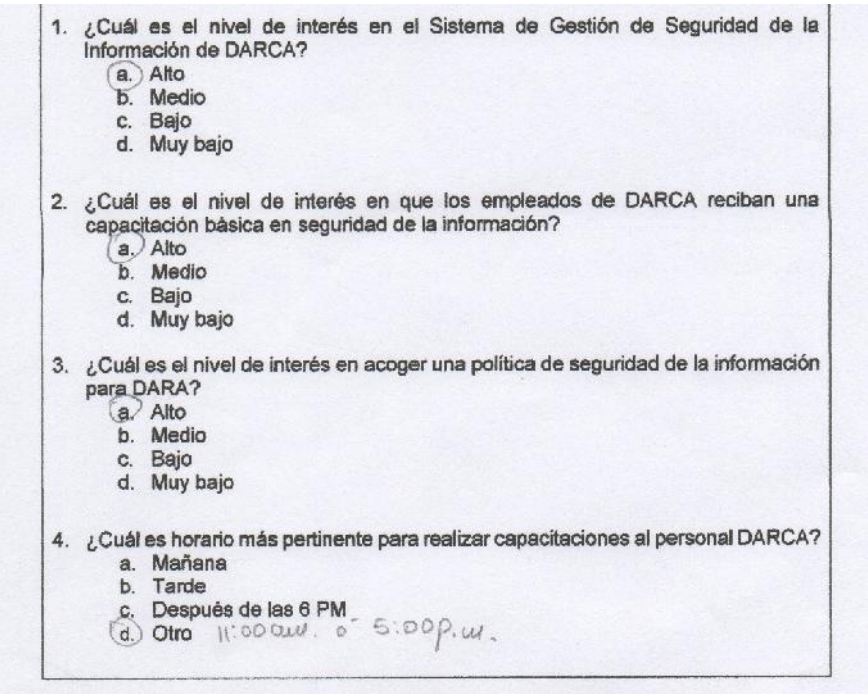
Anexo B. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Las técnicas e instrumentos de recolección de datos

fueron elaborados y aplicados en el alcance del procedimiento *Inscripciones y Admisiones,* perteneciente a DARCA de la Universidad del Cauca. El propósito fue determinar las características y necesidades en lo relacionado a la seguridad de la información (centrándose en la fase ejecución del SGSI). Adicionalmente sirvieron para contextualizar a los funcionarios de DARCA sobre el proyecto de implantación del SGSI.

B.1. Encuestas

- **Encuesta realizada al jefe DARCA.**



1. ¿Cuál es el nivel de interés en el Sistema de Gestión de Seguridad de la Información de DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo

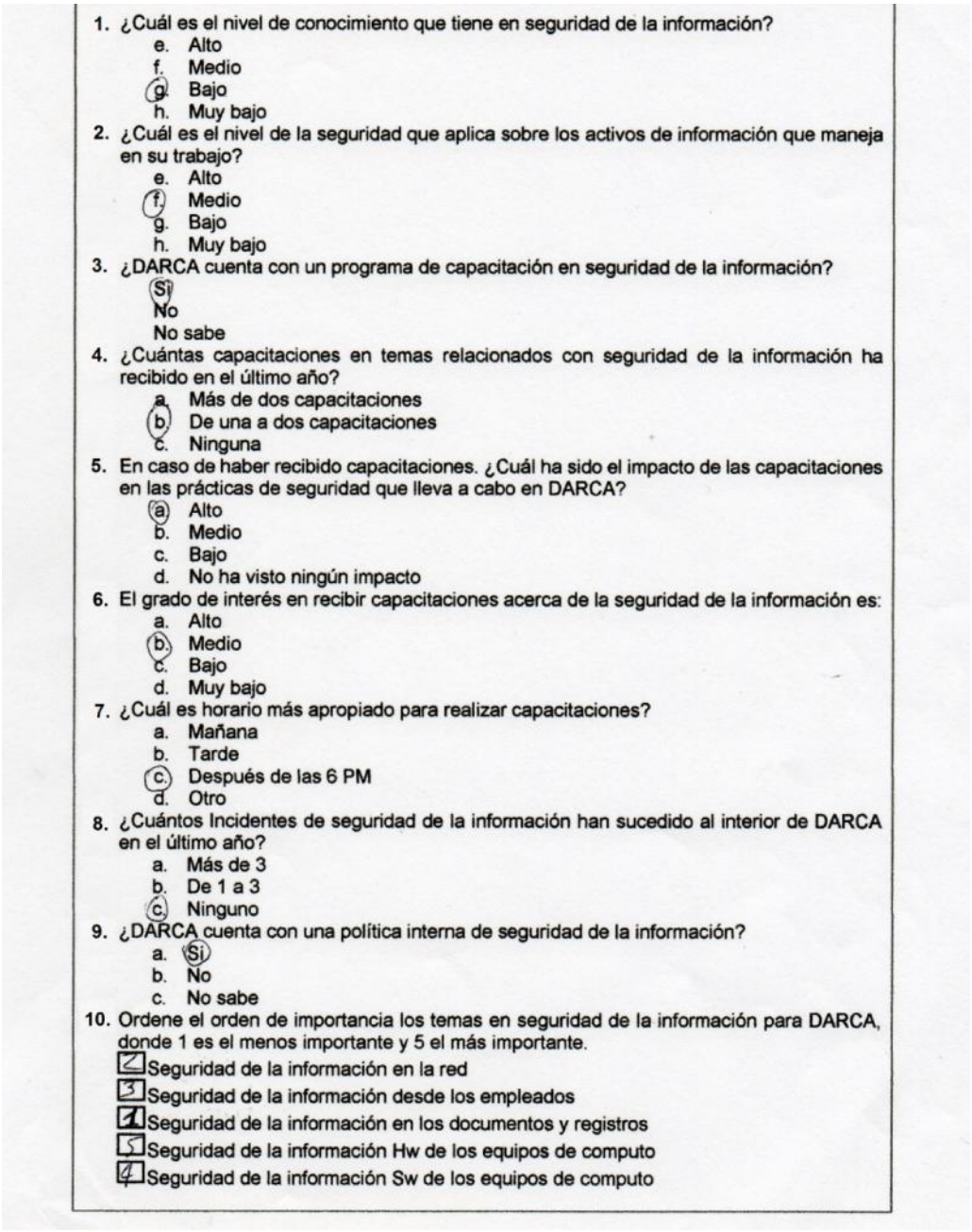
2. ¿Cuál es el nivel de interés en que los empleados de DARCA reciban una capacitación básica en seguridad de la información?
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo

3. ¿Cuál es el nivel de interés en acoger una política de seguridad de la información para DARA?
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo

4. ¿Cuál es horario más pertinente para realizar capacitaciones al personal DARCA?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro 11:00a.m. a 5:00p.m.

Fig. 2. Encuesta dirigida al jefe de DARCA

- **Encuesta realizada a funcionarios DARCA.**

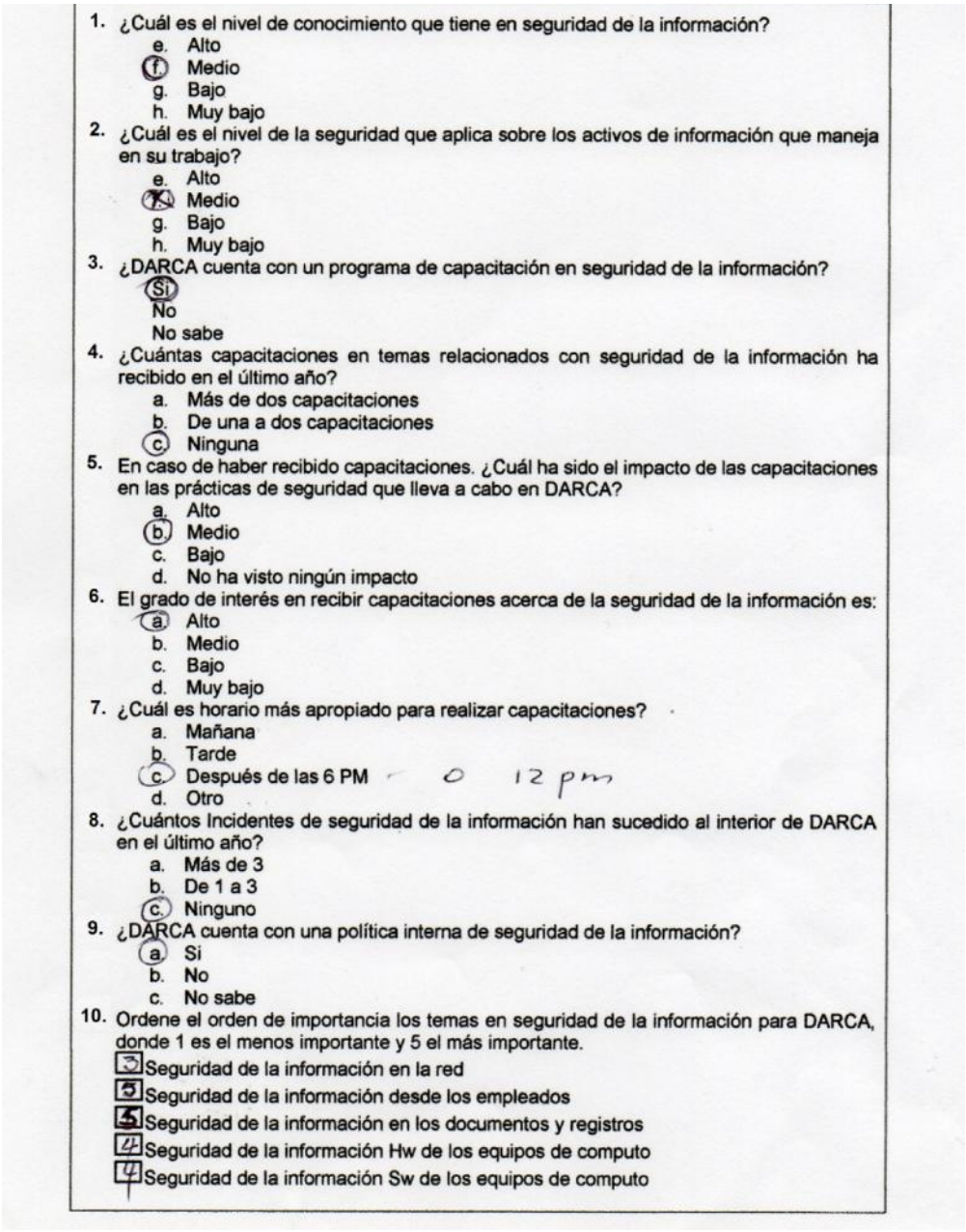


1. ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
2. ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
3. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe
4. ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna
5. En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto
6. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo
7. ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro
8. ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   c. Ninguno
9. ¿DARCA cuenta con una política interna de seguridad de la información?
   a. Si
   b. No
   c. No sabe
10. Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
    2 Seguridad de la información en la red
    3 Seguridad de la información desde los empleados
    1 Seguridad de la información en los documentos y registros
    5 Seguridad de la información Hw de los equipos de computo
    4 Seguridad de la información Sw de los equipos de computo

Fig. 3. Encuesta 1 dirigida al personal de DARCA

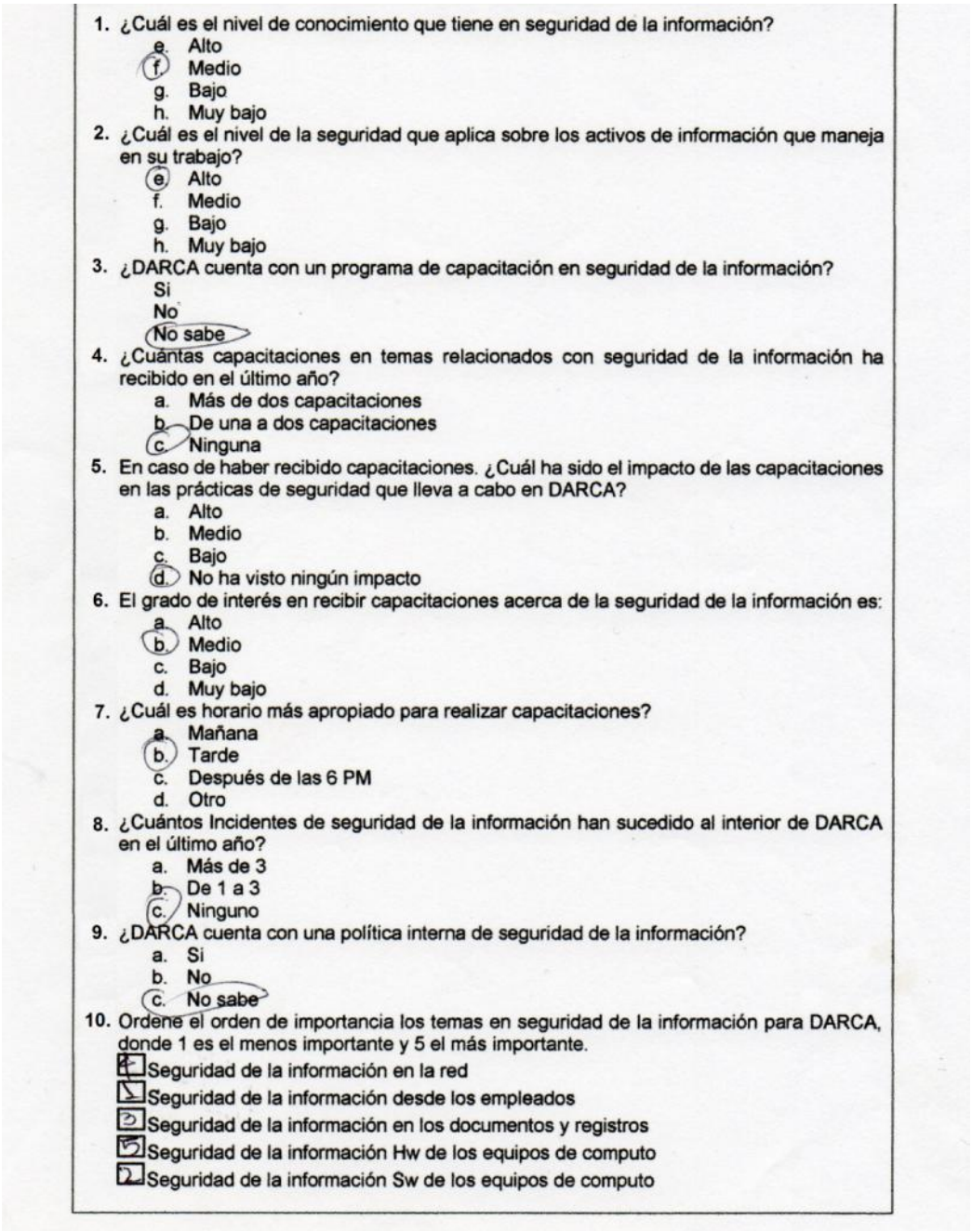
1. ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
2. ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
3. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe
4. ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna
5. En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto
6. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo
7. ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro
8. ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   c. Ninguno
9. ¿DARCA cuenta con una política interna de seguridad de la información?
   a. Si
   b. No
   c. No sabe
10. Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
    [5] Seguridad de la información en la red
    [4] Seguridad de la información desde los empleados
    [3] Seguridad de la información en los documentos y registros
    [2] Seguridad de la información Hw de los equipos de computo
    [1] Seguridad de la información Sw de los equipos de computo

Fig. 4. Encuesta 2 dirigida al personal de DARCA



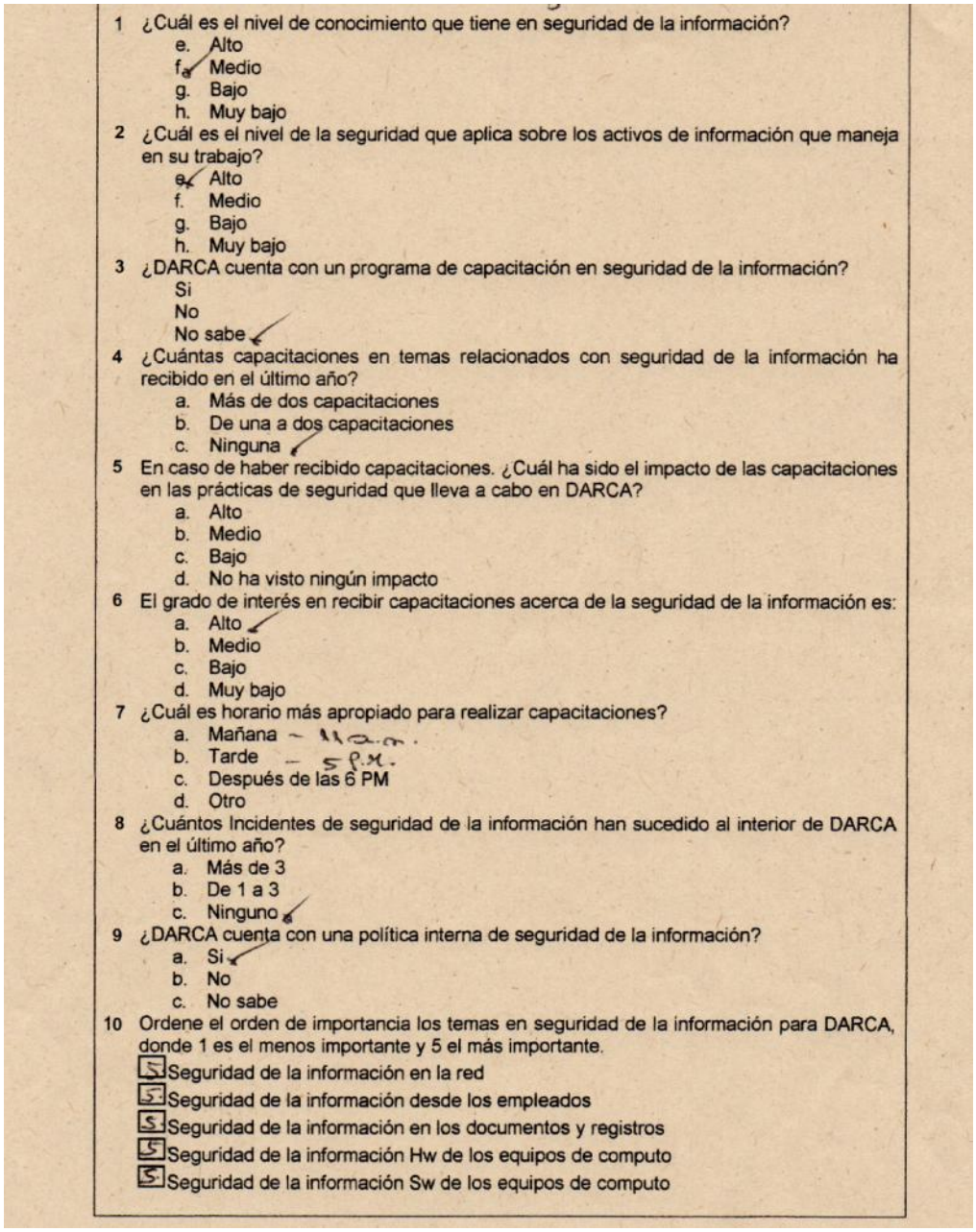
1. ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   (f) Medio
   g. Bajo
   h. Muy bajo
2. ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   (f) Medio
   g. Bajo
   h. Muy bajo
3. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   (Si)
   No
   No sabe
4. ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   (c) Ninguna
5. En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   (b) Medio
   c. Bajo
   d. No ha visto ningún impacto
6. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   (a) Alto
   b. Medio
   c. Bajo
   d. Muy bajo
7. ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   (c) Después de las 6 PM - o 12 pm
   d. Otro
8. ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   (c) Ninguno
9. ¿DARCA cuenta con una política interna de seguridad de la información?
   (a) Si
   b. No
   c. No sabe
10. Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
    [3] Seguridad de la información en la red
    [5] Seguridad de la información desde los empleados
    [5] Seguridad de la información en los documentos y registros
    [4] Seguridad de la información Hw de los equipos de computo
    [4] Seguridad de la información Sw de los equipos de computo

Fig. 5. Encuesta 3 dirigida al personal de DARCA



1. ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
2. ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
3. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe
4. ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna
5. En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto
6. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo
7. ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro
8. ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   c. Ninguno
9. ¿DARCA cuenta con una política interna de seguridad de la información?
   a. Si
   b. No
   c. No sabe
10. Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
    Seguridad de la información en la red
    Seguridad de la información desde los empleados
    Seguridad de la información en los documentos y registros
    Seguridad de la información Hw de los equipos de computo
    Seguridad de la información Sw de los equipos de computo

Fig. 6. Encuesta 4 dirigida al personal de DARCA



1 ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
- e. Alto
- f. Medio
- g. Bajo
- h. Muy bajo

2 ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
- e. Alto
- f. Medio
- g. Bajo
- h. Muy bajo

3 ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
- Si
- No
- No sabe

4 ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
- a. Más de dos capacitaciones
- b. De una a dos capacitaciones
- c. Ninguna

5 En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
- a. Alto
- b. Medio
- c. Bajo
- d. No ha visto ningún impacto

6 El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
- a. Alto
- b. Medio
- c. Bajo
- d. Muy bajo

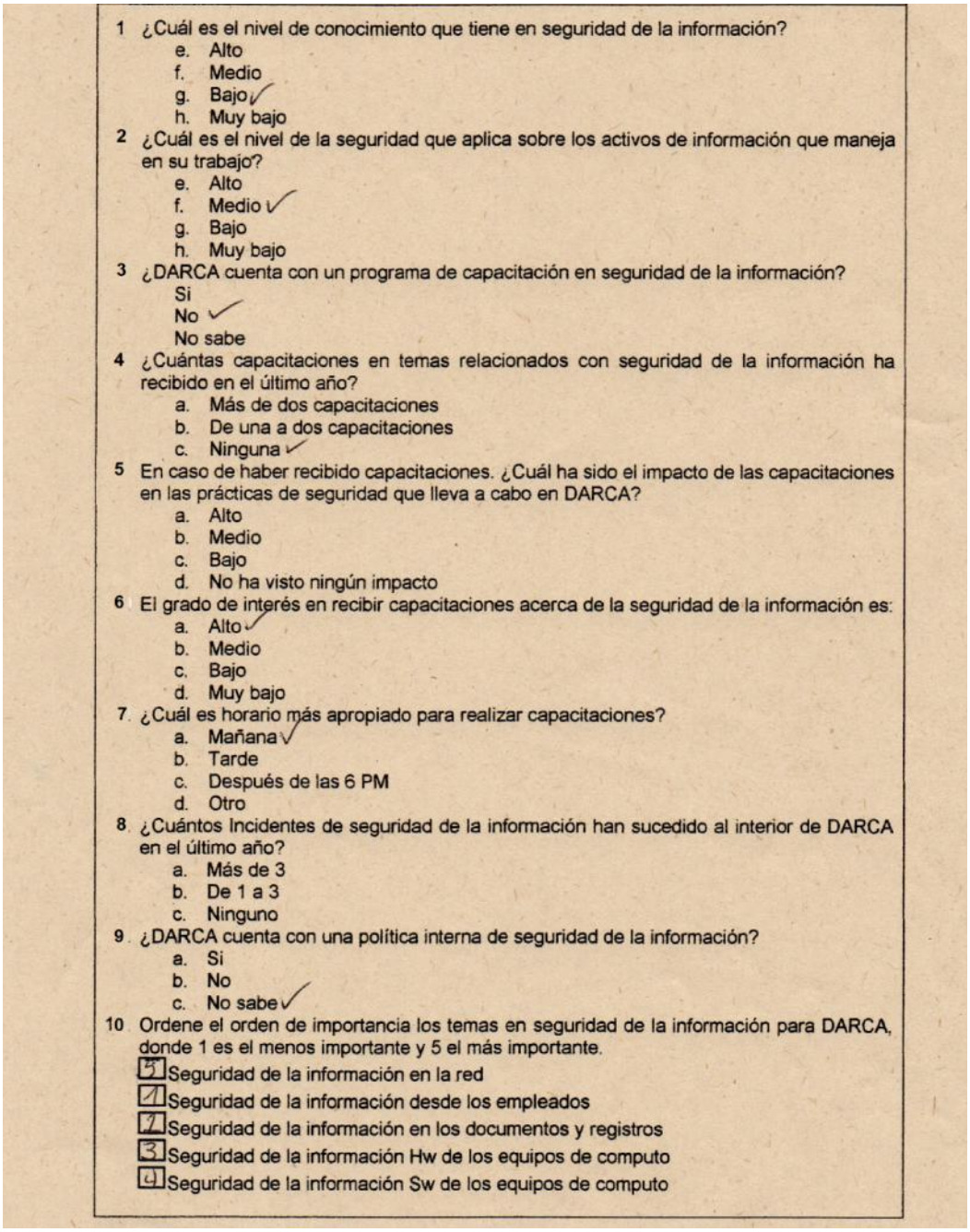
7 ¿Cuál es horario más apropiado para realizar capacitaciones?
- a. Mañana ~ 11 a.m.
- b. Tarde ~ 5 P.M.
- c. Después de las 6 PM
- d. Otro

8 ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
- a. Más de 3
- b. De 1 a 3
- c. Ninguno

9 ¿DARCA cuenta con una política interna de seguridad de la información?
- a. Si
- b. No
- c. No sabe

10 Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
- [5] Seguridad de la información en la red
- [5] Seguridad de la información desde los empleados
- [5] Seguridad de la información en los documentos y registros
- [5] Seguridad de la información Hw de los equipos de computo
- [5] Seguridad de la información Sw de los equipos de computo

Fig. 7. Encuesta 5 dirigida al personal de DARCA



1 ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
- e. Alto
- f. Medio
- g. Bajo ✓
- h. Muy bajo

2 ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
- e. Alto
- f. Medio ✓
- g. Bajo
- h. Muy bajo

3 ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
- Si
- No ✓
- No sabe

4 ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
- a. Más de dos capacitaciones
- b. De una a dos capacitaciones
- c. Ninguna ✓

5 En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
- a. Alto
- b. Medio
- c. Bajo
- d. No ha visto ningún impacto

6 El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
- a. Alto ✓
- b. Medio
- c. Bajo
- d. Muy bajo

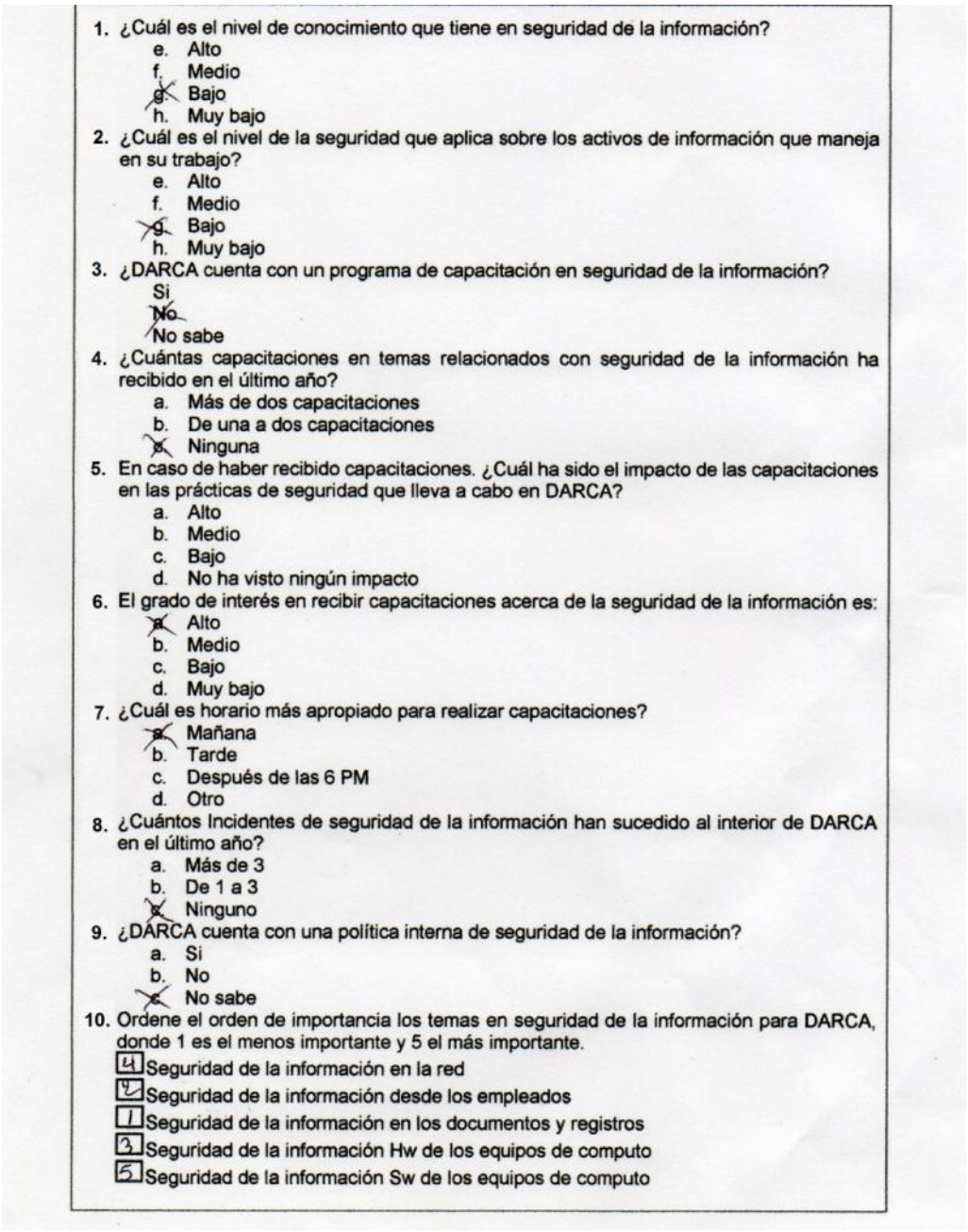
7 ¿Cuál es horario más apropiado para realizar capacitaciones?
- a. Mañana ✓
- b. Tarde
- c. Después de las 6 PM
- d. Otro

8 ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
- a. Más de 3
- b. De 1 a 3
- c. Ninguno

9 ¿DARCA cuenta con una política interna de seguridad de la información?
- a. Si
- b. No
- c. No sabe ✓

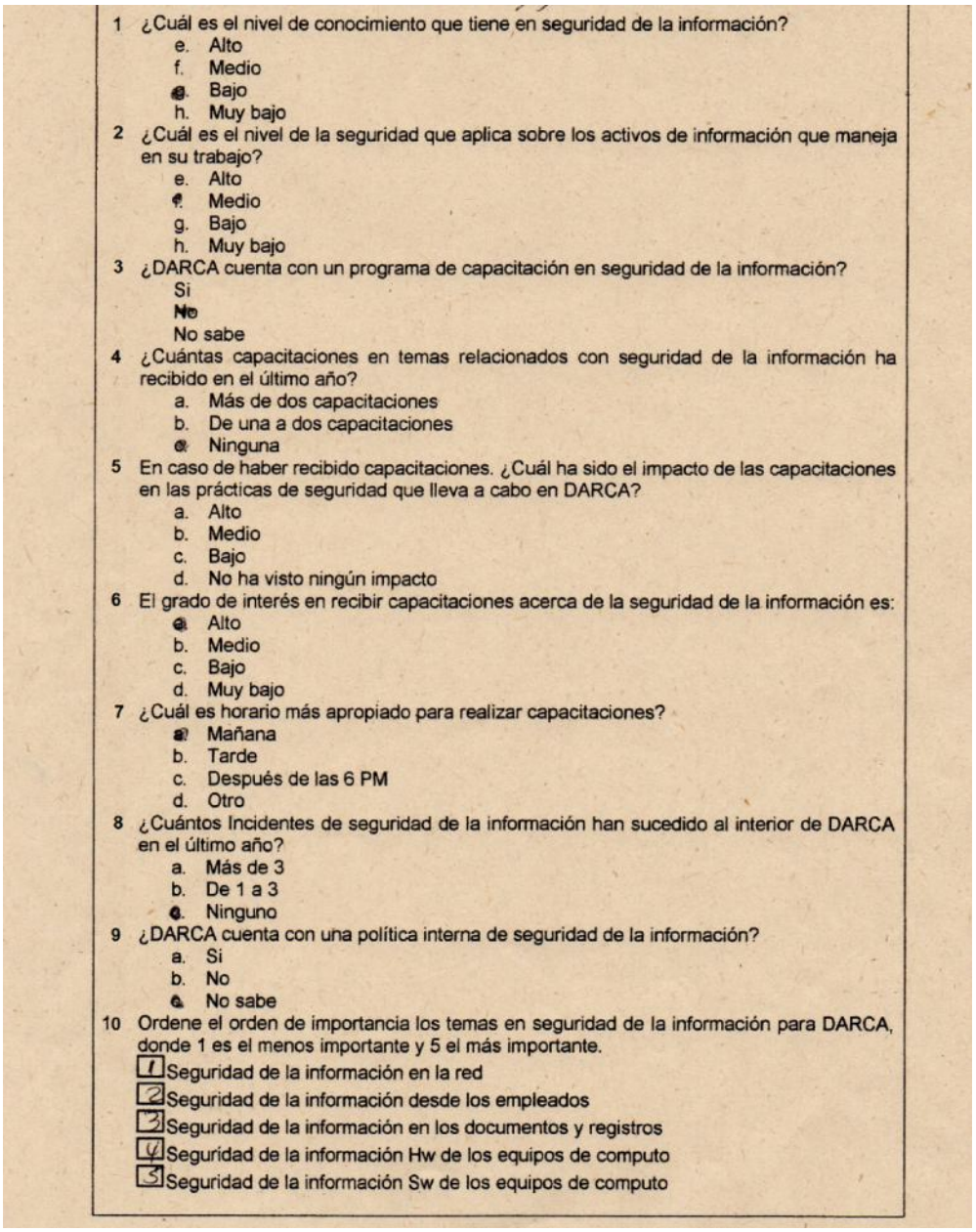
10 Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
- [5] Seguridad de la información en la red
- [1] Seguridad de la información desde los empleados
- [2] Seguridad de la información en los documentos y registros
- [3] Seguridad de la información Hw de los equipos de computo
- [4] Seguridad de la información Sw de los equipos de computo

Fig. 8. Encuesta 6 dirigida al personal de DARCA



1. ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
2. ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
3. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe
4. ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna
5. En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto
6. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo
7. ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro
8. ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   c. Ninguno
9. ¿DARCA cuenta con una política interna de seguridad de la información?
   a. Si
   b. No
   c. No sabe
10. Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
    [4] Seguridad de la información en la red
    [2] Seguridad de la información desde los empleados
    [1] Seguridad de la información en los documentos y registros
    [3] Seguridad de la información Hw de los equipos de computo
    [5] Seguridad de la información Sw de los equipos de computo

Fig. 9. Encuesta 7 dirigida al personal de DARCA



1 ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo

2 ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo

3 ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe

4 ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna

5 En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto

6 El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo

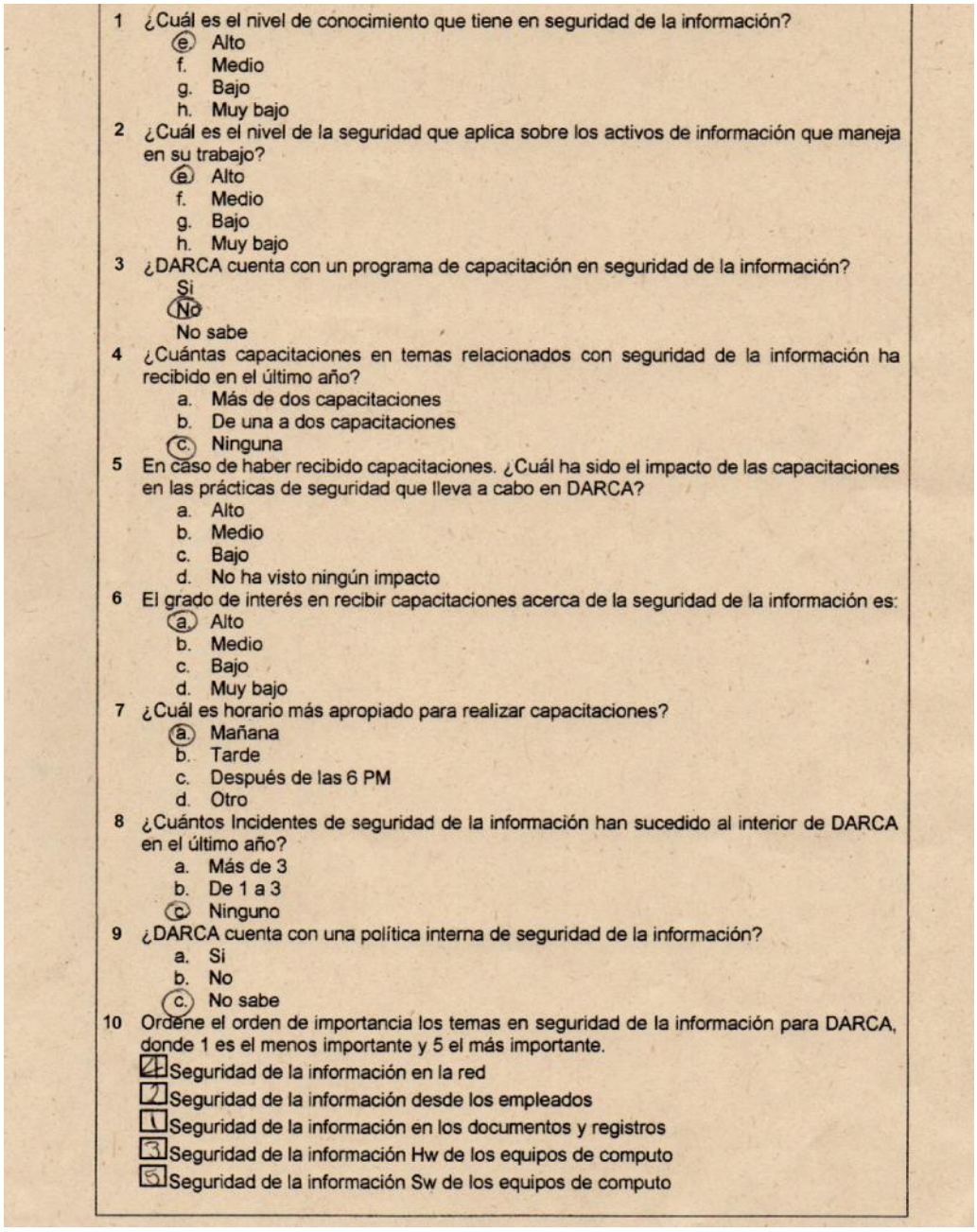
7 ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro

8 ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   c. Ninguno

9 ¿DARCA cuenta con una política interna de seguridad de la información?
   a. Si
   b. No
   c. No sabe

10 Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
   [1] Seguridad de la información en la red
   [2] Seguridad de la información desde los empleados
   [3] Seguridad de la información en los documentos y registros
   [4] Seguridad de la información Hw de los equipos de computo
   [5] Seguridad de la información Sw de los equipos de computo

Fig. 10. Encuesta 8 dirigida al personal de DARCA



1 ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
- e. Alto
- f. Medio
- g. Bajo
- h. Muy bajo

2 ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
- e. Alto
- f. Medio
- g. Bajo
- h. Muy bajo

3 ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
- Si
- No
- No sabe

4 ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
- a. Más de dos capacitaciones
- b. De una a dos capacitaciones
- c. Ninguna

5 En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
- a. Alto
- b. Medio
- c. Bajo
- d. No ha visto ningún impacto

6 El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
- a. Alto
- b. Medio
- c. Bajo
- d. Muy bajo

7 ¿Cuál es horario más apropiado para realizar capacitaciones?
- a. Mañana
- b. Tarde
- c. Después de las 6 PM
- d. Otro

8 ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
- a. Más de 3
- b. De 1 a 3
- c. Ninguno

9 ¿DARCA cuenta con una política interna de seguridad de la información?
- a. Si
- b. No
- c. No sabe

10 Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
- [4] Seguridad de la información en la red
- [2] Seguridad de la información desde los empleados
- [1] Seguridad de la información en los documentos y registros
- [3] Seguridad de la información Hw de los equipos de computo
- [5] Seguridad de la información Sw de los equipos de computo

Fig. 11. Encuesta 9 dirigida al personal de DARCA

1 ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
- e. Alto
- f. Medio
- g. Bajo
- h. Muy bajo

2 ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
- e. Alto
- f. Medio
- g. Bajo
- h. Muy bajo

3 ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
- Si
- No
- X No sabe

4 ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
- a. Más de dos capacitaciones
- b. De una a dos capacitaciones
- c. Ninguna

5 En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
- a. Alto
- b. Medio
- c. Bajo
- d. No ha visto ningún impacto

6 El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
- a. Alto
- b. Medio
- c. Bajo
- d. Muy bajo

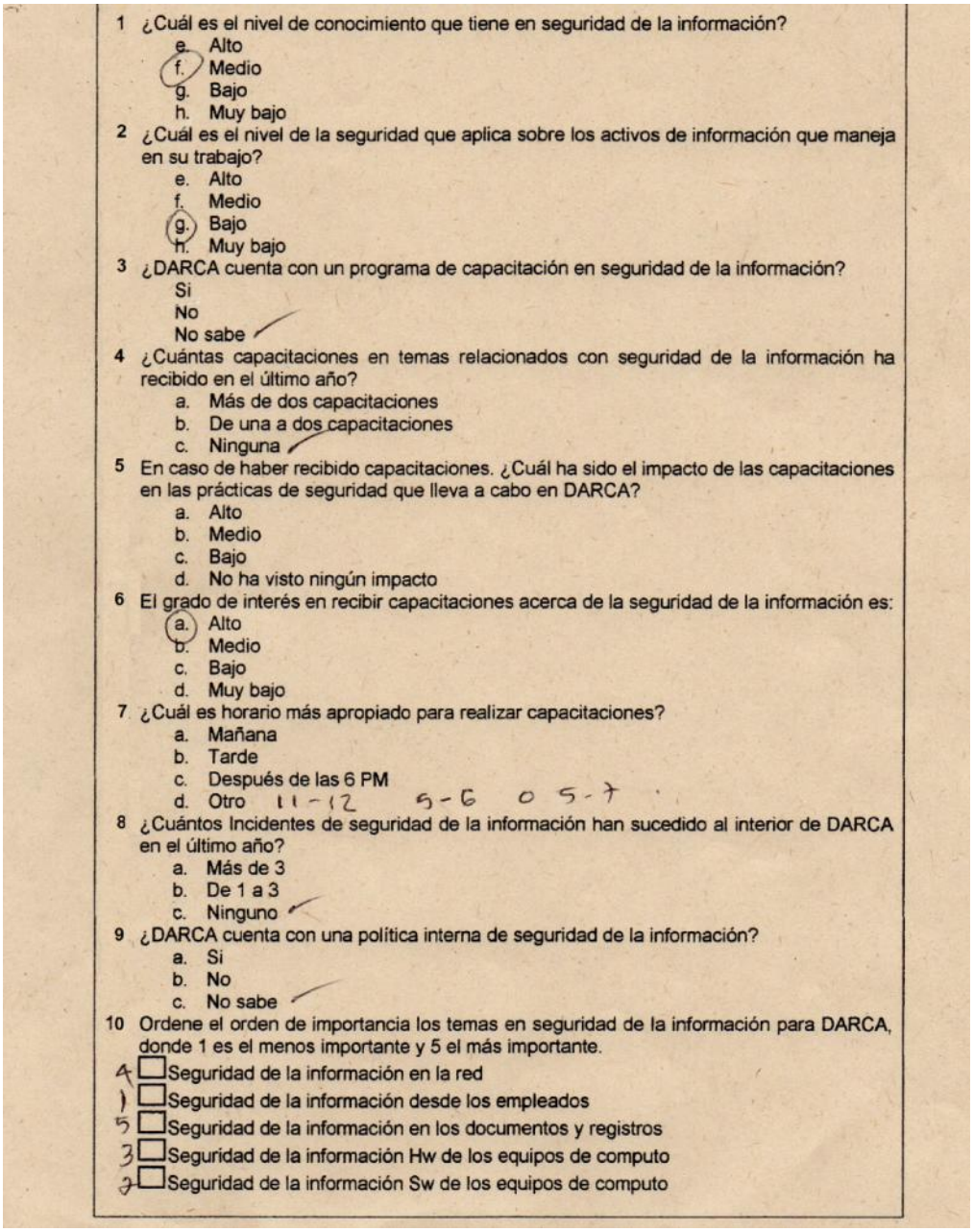
7 ¿Cuál es horario más apropiado para realizar capacitaciones?
- a. Mañana
- b. Tarde
- c. Después de las 6 PM
- d. Otro

8 ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
- a. Más de 3
- b. De 1 a 3
- c. Ninguno

9 ¿DARCA cuenta con una política interna de seguridad de la información?
- a. Si
- b. No
- c. No sabe

10 Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
- [3] Seguridad de la información en la red
- [5] Seguridad de la información desde los empleados
- [4] Seguridad de la información en los documentos y registros
- [1] Seguridad de la información Hw de los equipos de computo
- [2] Seguridad de la información Sw de los equipos de computo

Fig. 12. Encuesta 10 dirigida al personal de DARCA



1 ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo

2 ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo

3 ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe

4 ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna

5 En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto

6 El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo

7 ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro 11-12 5-6 o 5-7

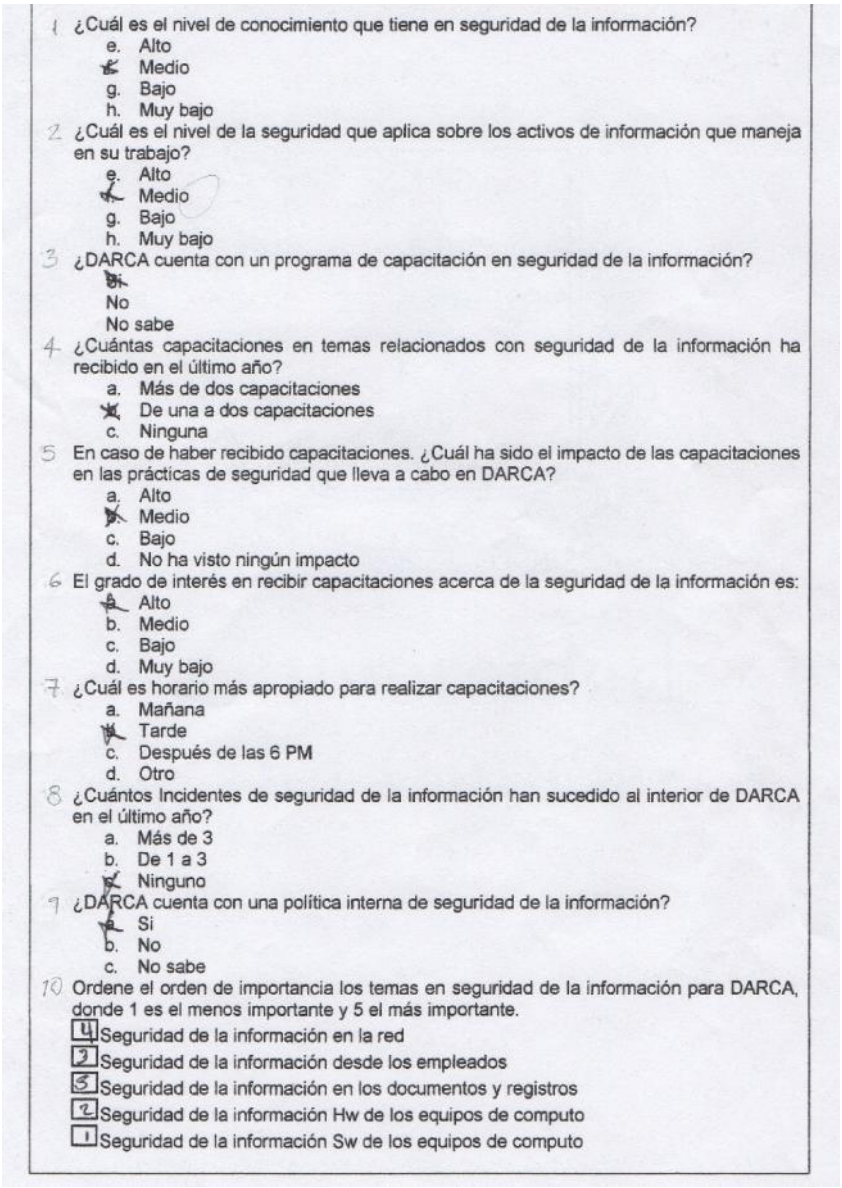
8 ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   c. Ninguno

9 ¿DARCA cuenta con una política interna de seguridad de la información?
   a. Si
   b. No
   c. No sabe

10 Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.

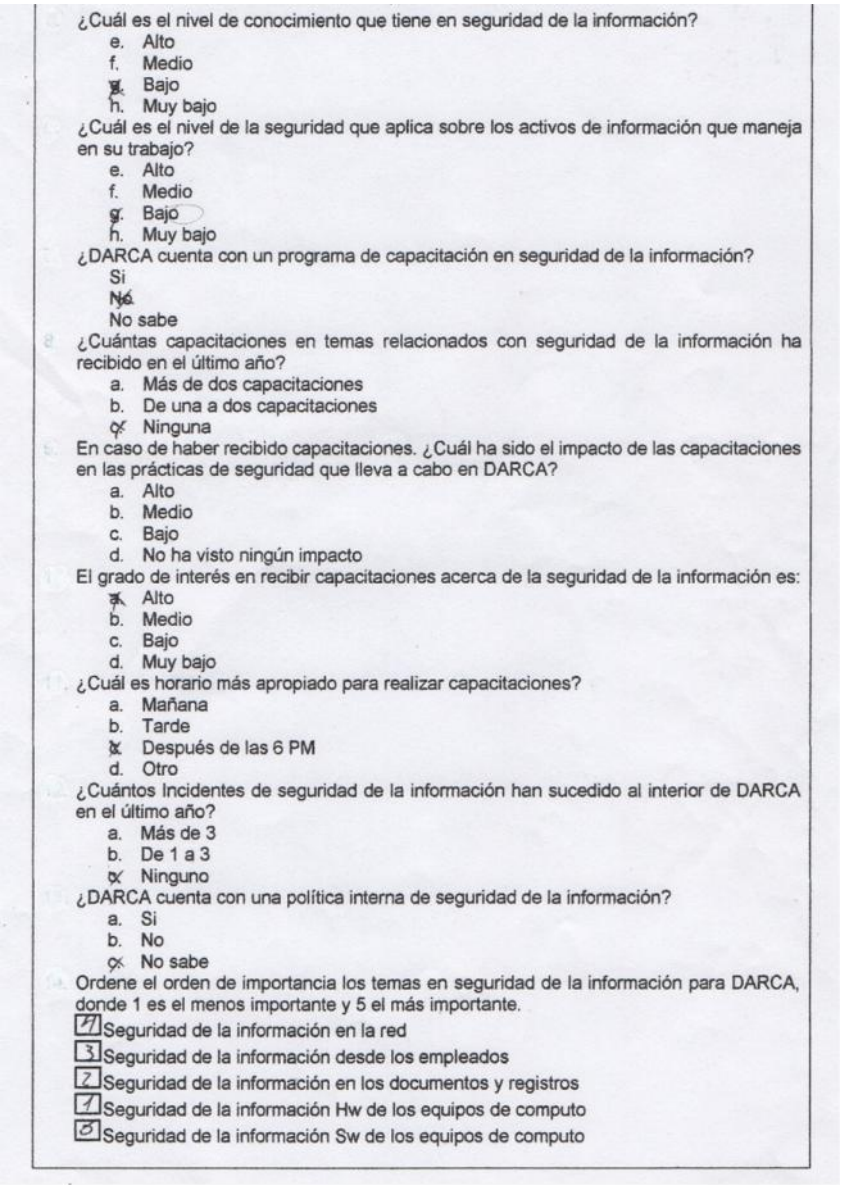
4 ☐ Seguridad de la información en la red
1 ☐ Seguridad de la información desde los empleados
5 ☐ Seguridad de la información en los documentos y registros
3 ☐ Seguridad de la información Hw de los equipos de computo
2 ☐ Seguridad de la información Sw de los equipos de computo

Fig. 13. Encuesta 11 dirigida al personal de DARCA



1. ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
2. ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
3. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe
4. ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna
5. En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto
6. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
   a. Alto
   b. Medio
   c. Bajo
   d. Muy bajo
7. ¿Cuál es horario más apropiado para realizar capacitaciones?
   a. Mañana
   b. Tarde
   c. Después de las 6 PM
   d. Otro
8. ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
   a. Más de 3
   b. De 1 a 3
   c. Ninguno
9. ¿DARCA cuenta con una política interna de seguridad de la información?
   a. Si
   b. No
   c. No sabe
10. Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
    [4] Seguridad de la información en la red
    [3] Seguridad de la información desde los empleados
    [5] Seguridad de la información en los documentos y registros
    [2] Seguridad de la información Hw de los equipos de computo
    [1] Seguridad de la información Sw de los equipos de computo

Fig. 14. Encuesta 12 dirigida al personal de DARCA



¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
e. Alto
f. Medio
g. Bajo
h. Muy bajo

¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
e. Alto
f. Medio
g. Bajo
h. Muy bajo

¿DARCA cuenta con un programa de capacitación en seguridad de la información?
Si
No
No sabe

¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
a. Más de dos capacitaciones
b. De una a dos capacitaciones
c. Ninguna

En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
a. Alto
b. Medio
c. Bajo
d. No ha visto ningún impacto

El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
a. Alto
b. Medio
c. Bajo
d. Muy bajo

¿Cuál es horario más apropiado para realizar capacitaciones?
a. Mañana
b. Tarde
c. Después de las 6 PM
d. Otro

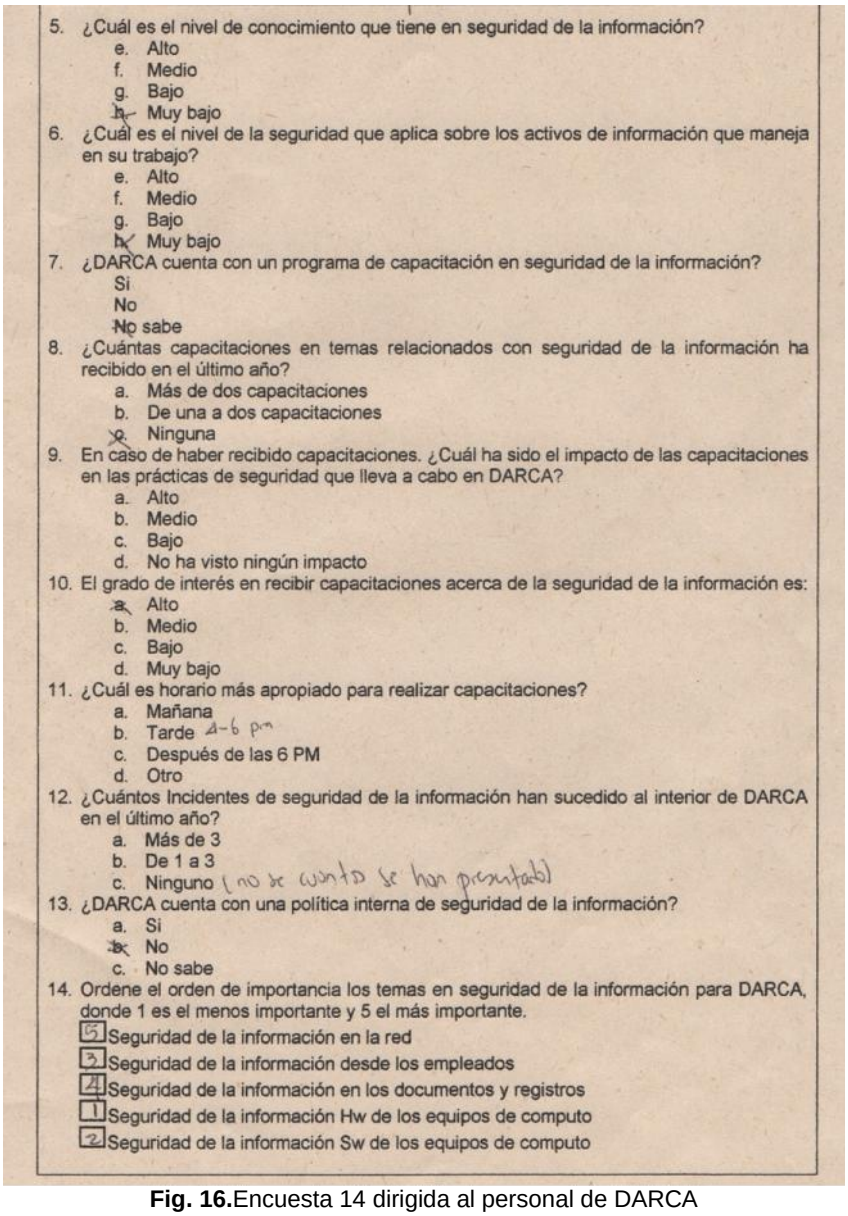
¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
a. Más de 3
b. De 1 a 3
c. Ninguno

¿DARCA cuenta con una política interna de seguridad de la información?
a. Si
b. No
c. No sabe

Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.

[4] Seguridad de la información en la red
[3] Seguridad de la información desde los empleados
[2] Seguridad de la información en los documentos y registros
[1] Seguridad de la información Hw de los equipos de computo
[5] Seguridad de la información Sw de los equipos de computo

Fig. 15. Encuesta 13 dirigida al personal de DARCA



5. ¿Cuál es el nivel de conocimiento que tiene en seguridad de la información?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
6. ¿Cuál es el nivel de la seguridad que aplica sobre los activos de información que maneja en su trabajo?
   e. Alto
   f. Medio
   g. Bajo
   h. Muy bajo
7. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?
   Si
   No
   No sabe
8. ¿Cuántas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?
   a. Más de dos capacitaciones
   b. De una a dos capacitaciones
   c. Ninguna
9. En caso de haber recibido capacitaciones. ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad que lleva a cabo en DARCA?
   a. Alto
   b. Medio
   c. Bajo
   d. No ha visto ningún impacto
10. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:
    a. Alto
    b. Medio
    c. Bajo
    d. Muy bajo
11. ¿Cuál es horario más apropiado para realizar capacitaciones?
    a. Mañana
    b. Tarde 4-6 pm
    c. Después de las 6 PM
    d. Otro
12. ¿Cuántos Incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?
    a. Más de 3
    b. De 1 a 3
    c. Ninguno (no se cuanto se han presentado)
13. ¿DARCA cuenta con una política interna de seguridad de la información?
    a. Si
    b. No
    c. No sabe
14. Ordene el orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 el más importante.
    [5] Seguridad de la información en la red
    [3] Seguridad de la información desde los empleados
    [4] Seguridad de la información en los documentos y registros
    [1] Seguridad de la información Hw de los equipos de computo
    [2] Seguridad de la información Sw de los equipos de computo

Fig. 16. Encuesta 14 dirigida al personal de DARCA

Pregunta 1. ¿Cuál considera que es su nivel de conocimiento en seguridad de la información?	
Códigos	**Respuestas**
a) Alto	2
b) Medio	6
c) Bajo	5
d) Muy Bajo	1
Total de entrevistas:	14

TABLA III. Tabulación Pregunta 1 – encuesta

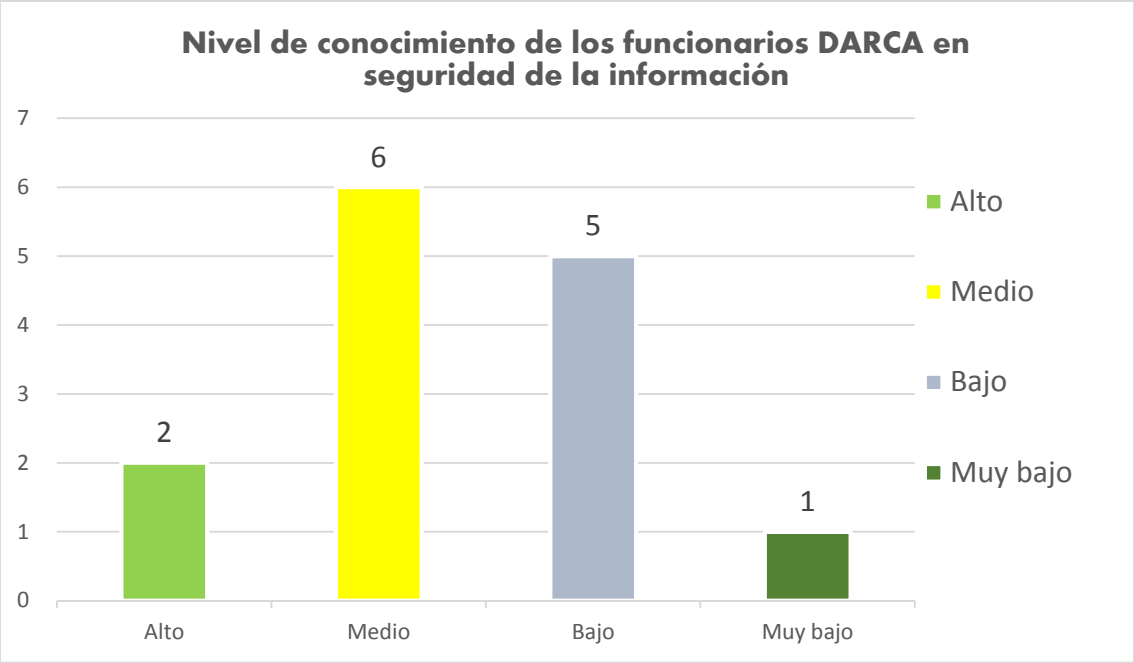


Fig. 17. Resultados Pregunta 1.

Pregunta 2. ¿Cuál es el nivel de seguridad que aplica sobre los activos de información que maneja en su trabajo?	
Códigos	**Respuestas**
a) Alto	5
b) Medio	4
c) Bajo	3
d) Muy Bajo	2
Total de entrevistas:	14

TABLA IV. Tabulación Pregunta 2 – encuesta.

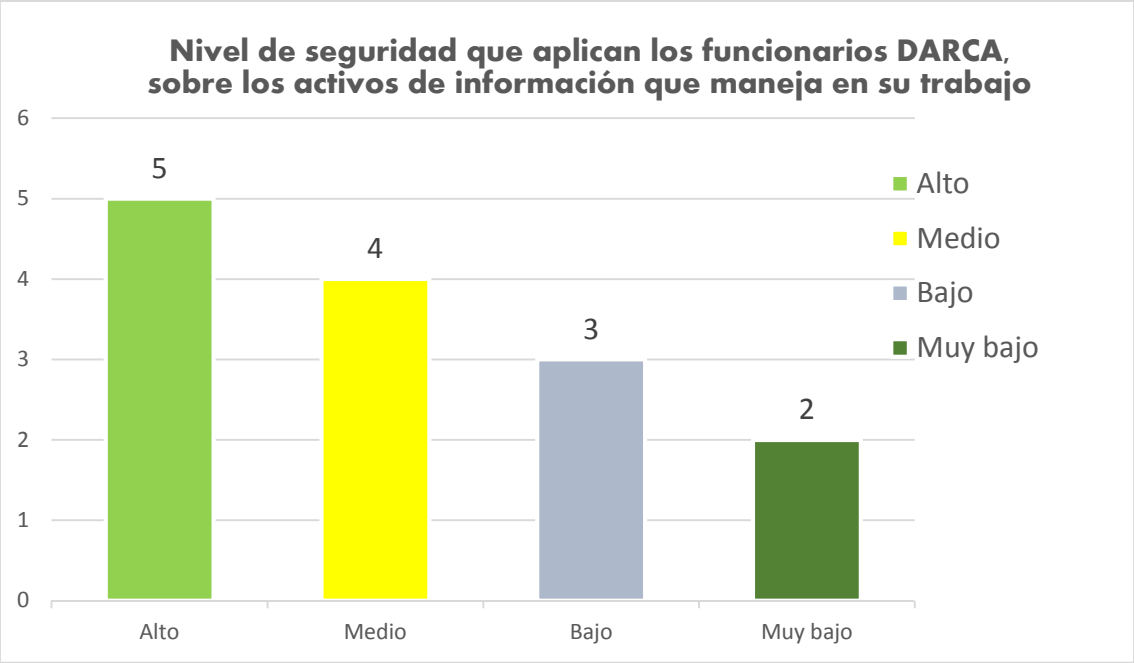


Fig. 18. Resultados Pregunta 2.

Pregunta 3. ¿DARCA cuenta con un programa de capacitación en seguridad de la información?	
Códigos	**Respuestas**
a) Si	3
b) No	5
c) No sabe	6
Total de entrevistas:	14

TABLA V. Tabulación Pregunta 3 – encuesta.

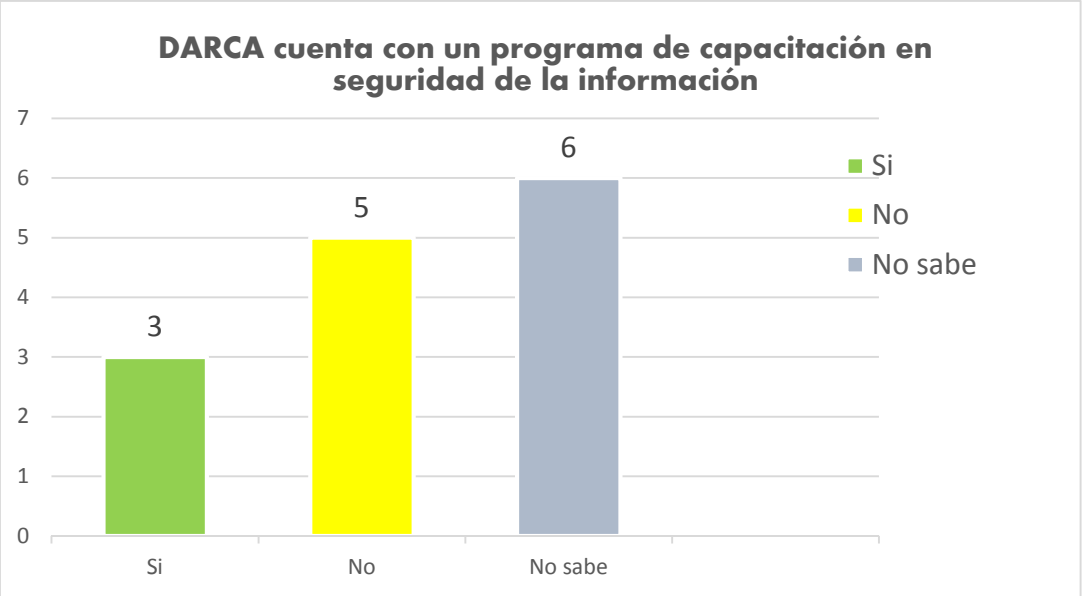


Fig. 19. Resultados Pregunta 3.

Pregunta 4. ¿Cuantas capacitaciones en temas relacionados con seguridad de la información ha recibido en el último año?		
Códigos		**Respuestas**
a)	Más de dos capacitaciones	0
b)	Entre una y dos capacitaciones	3
c)	Ninguna	11
	Total de entrevistas:	14

TABLA VI. Tabulación Pregunta 4 – encuesta.

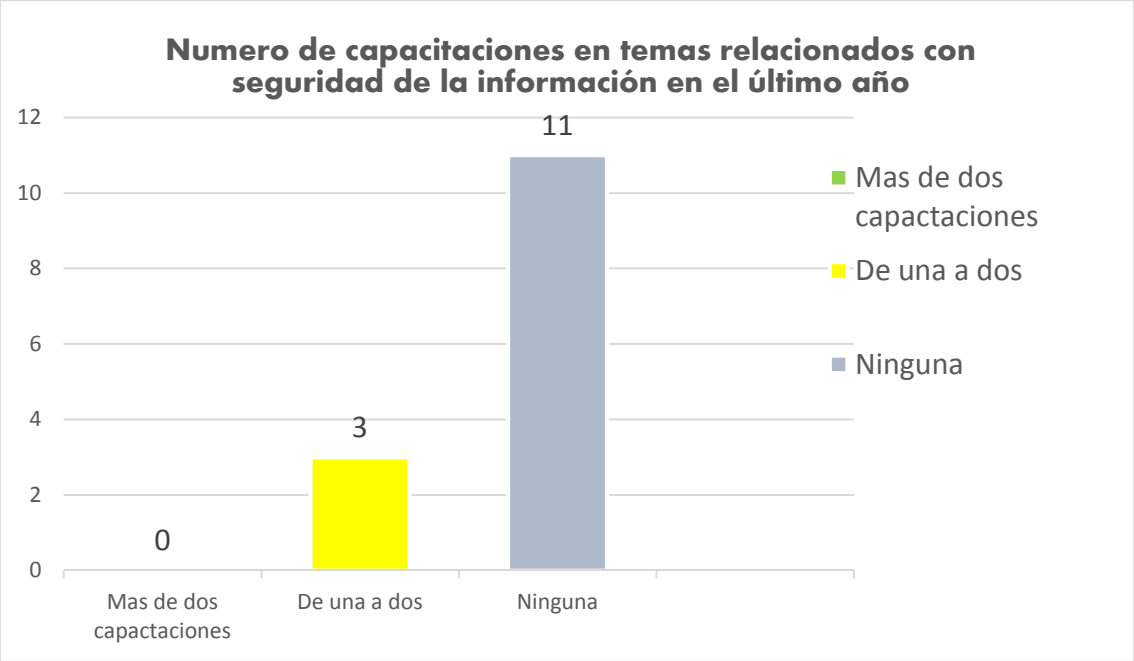


Fig. 20. Resultados Pregunta 4.

Pregunta 5. En caso de haber recibido capacitaciones, ¿Cuál ha sido el impacto de las capacitaciones en las prácticas de seguridad de la información que se llevan a cabo en DARCA?		
Códigos		**Respuestas**
a)	Alto	1
b)	Medio	2
c)	Bajo	0
d)	No ha visto ningún impacto	0
	Total de entrevistas:	14

TABLA VII. Tabulación Pregunta 5 – encuesta.

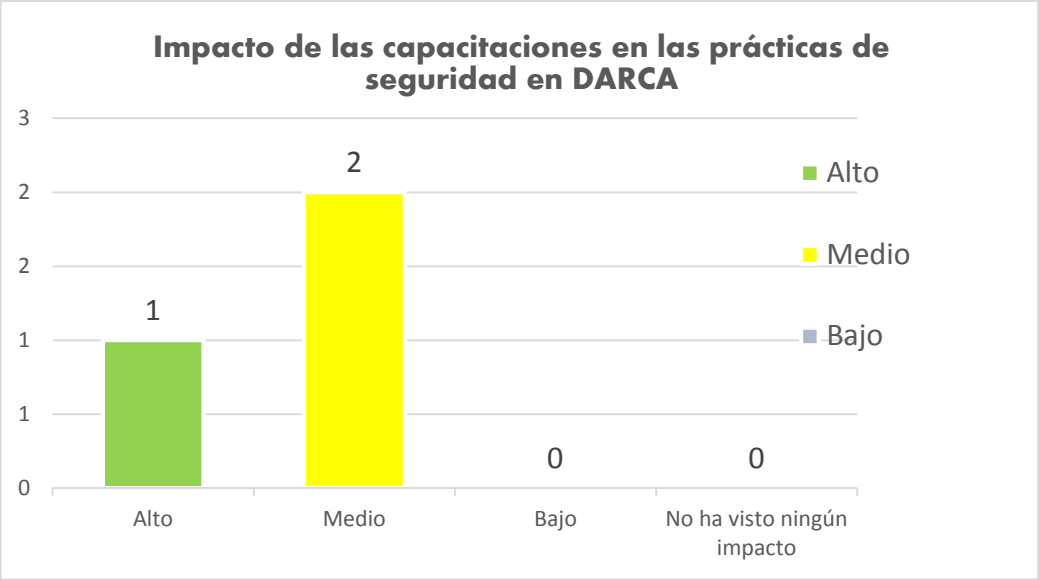


Fig. 21. Resultados Pregunta 5.

Pregunta 6. El grado de interés en recibir capacitaciones acerca de la seguridad de la información es:	
Códigos	**Respuestas**
a) Alto	12
b) Medio	2
c) Bajo	0
d) Muy Bajo	0
Total de entrevistas:	14

TABLA VIII. Tabulación Pregunta 6 - encuesta.

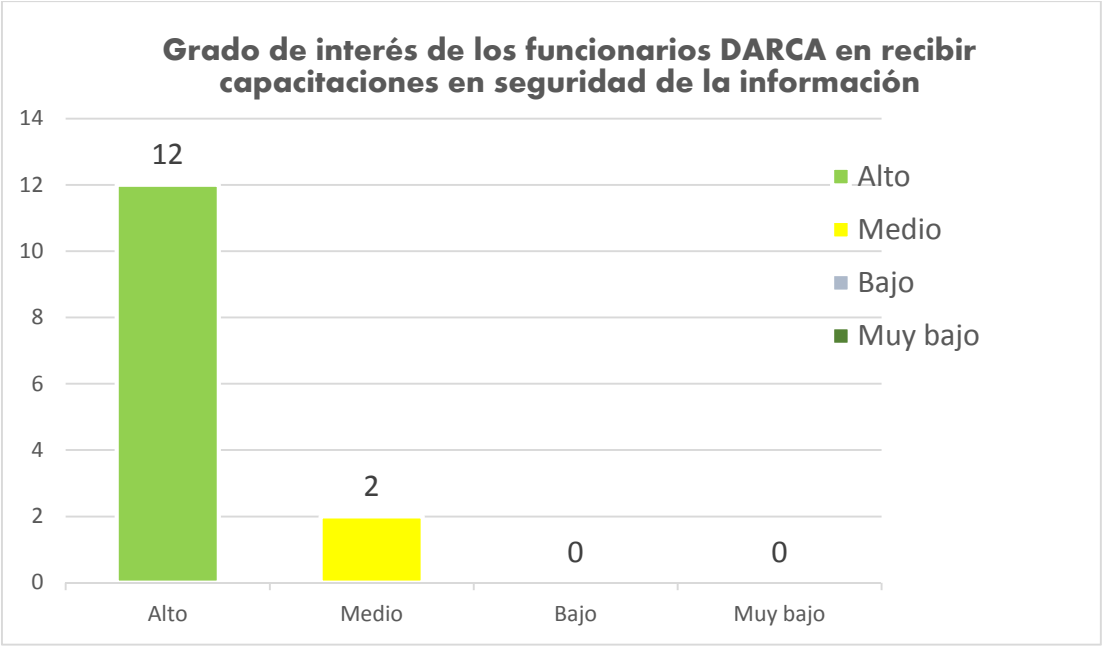


Fig. 22. Resultados Pregunta 6.

Pregunta 7. ¿Cuál es el horario más apropiado para realizar capacitaciones?		
Códigos	**Respuestas**	
a) Mañana		5
b) Tarde		5
c) Después de las 6 PM		3
d) Otro		1
	Total de entrevistas:	14

TABLA IX. Tabulación Pregunta 7 – encuesta.

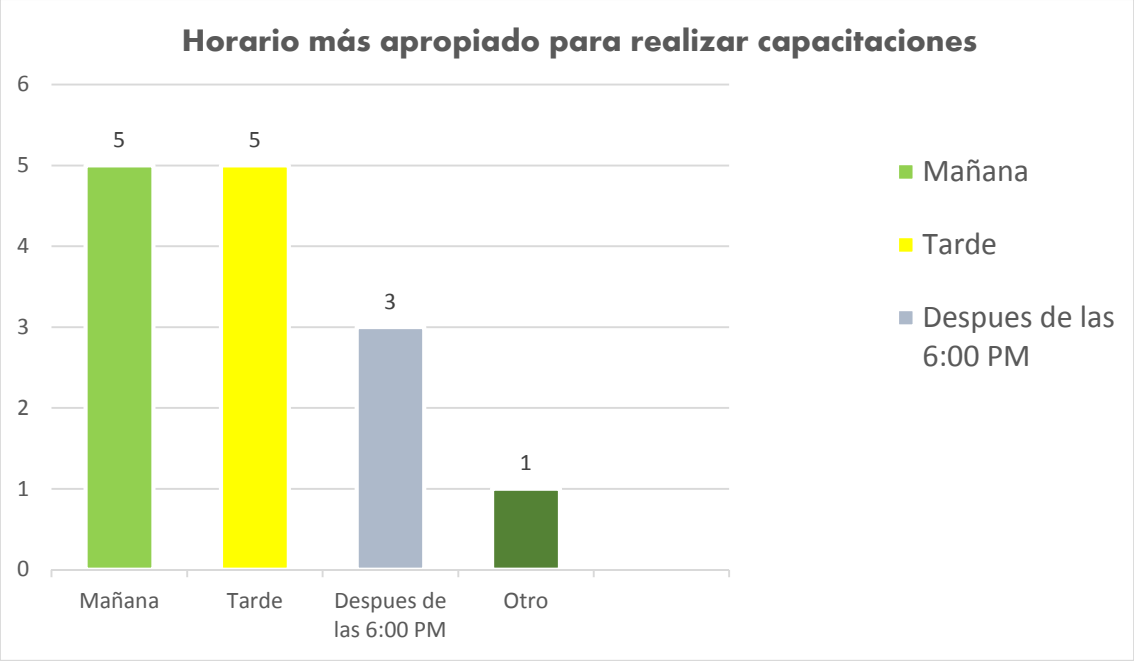


Fig. 23. Resultados Pregunta 7.

Pregunta 8. ¿Cuántos incidentes de seguridad de la información han sucedido al interior de DARCA en el último año?		
Códigos	**Respuestas**	
a) Más de 3		0
b) De 1 a 3		0
c) Ninguno		14
	Total de entrevistas:	14

TABLA X. Tabulación Pregunta 8 – encuesta.

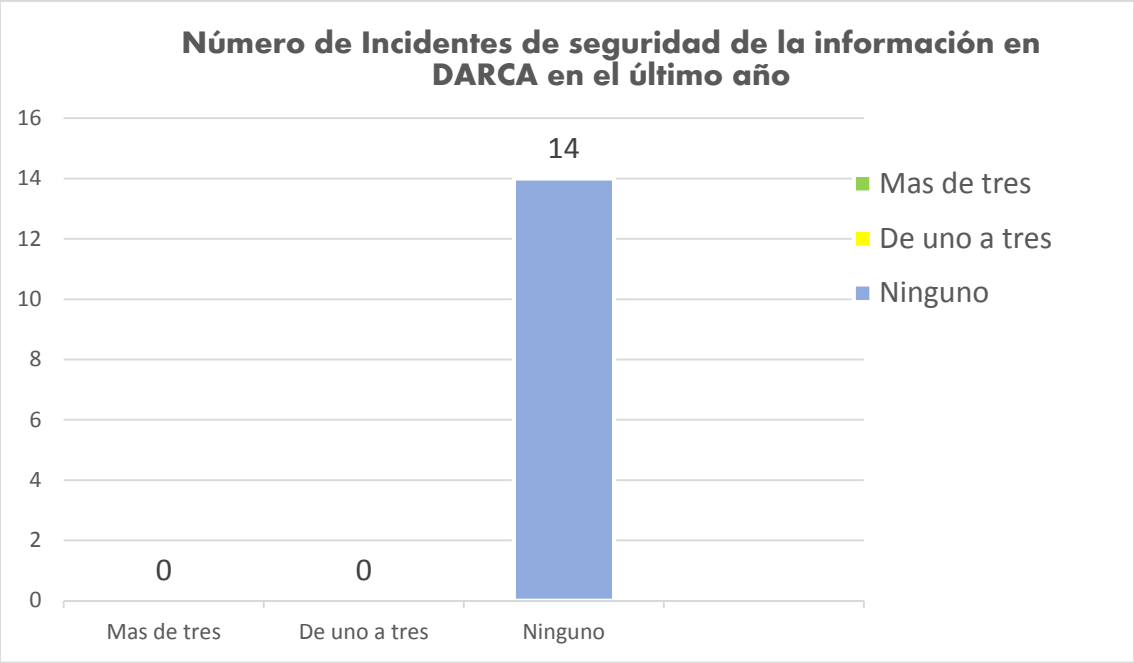


Fig. 24. Resultados Pregunta 8.

Pregunta 9. ¿DARCA cuenta con una política interna de seguridad de la información?	
Códigos	**Respuestas**
a) Si	4
b) No	1
c) No sabe	9
Total de entrevistas:	14

TABLA XI. Tabulación Pregunta 9 – encuesta.

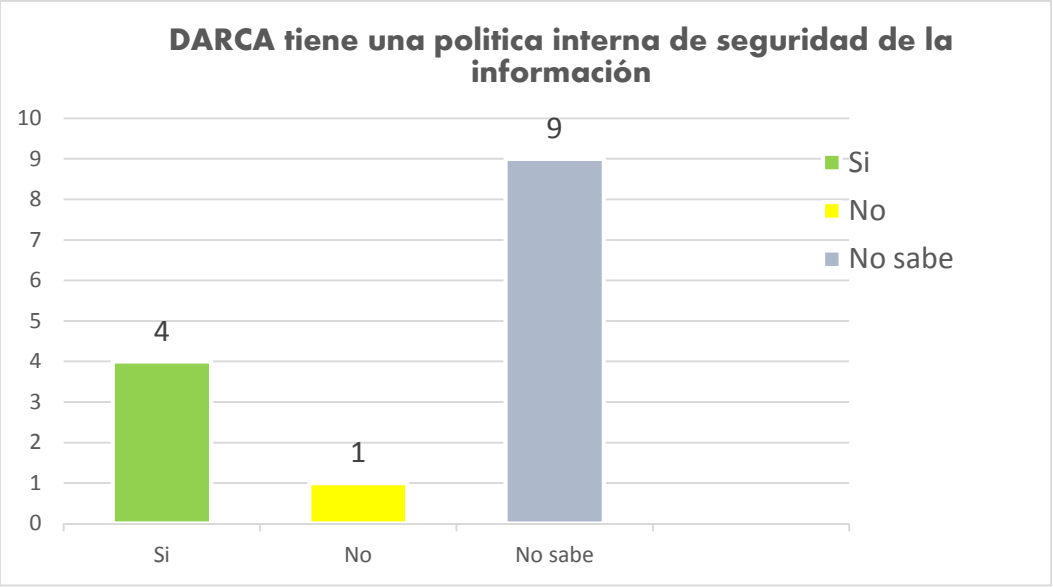


Fig. 25. Resultados Pregunta 9

Pregunta 10. Ordene en orden de importancia los temas en seguridad de la información para DARCA, donde 1 es el menos importante y 5 es el más importante.																
Códigos	**Respuestas**															**Total**
a) Seguridad de la información en la red	2	5	3	4	5	5	4	1	4	3	4	5	4	4		53
b) Seguridad de la información desde los empleados	3	4	5	1	5	1	2	2	2	5	1	3	3	3		40
c) Seguridad de la información en los documentos y registros	1	3	5	3	5	1	1	3	1	4	5	4	5	2		43
d) Seguridad de la información Hardware de los equipos de computo	5	2	4	5	5	3	3	4	3	1	3	1	2	1		42
e) Seguridad de la información Software de los equipos de computo	4	1	4	2	5	4	5	5	5	2	2	2	1	5		47
															Total general:	14
															Total de entrevistas:	14

TABLA XII. Tabulación Pregunta 10 – encuesta.

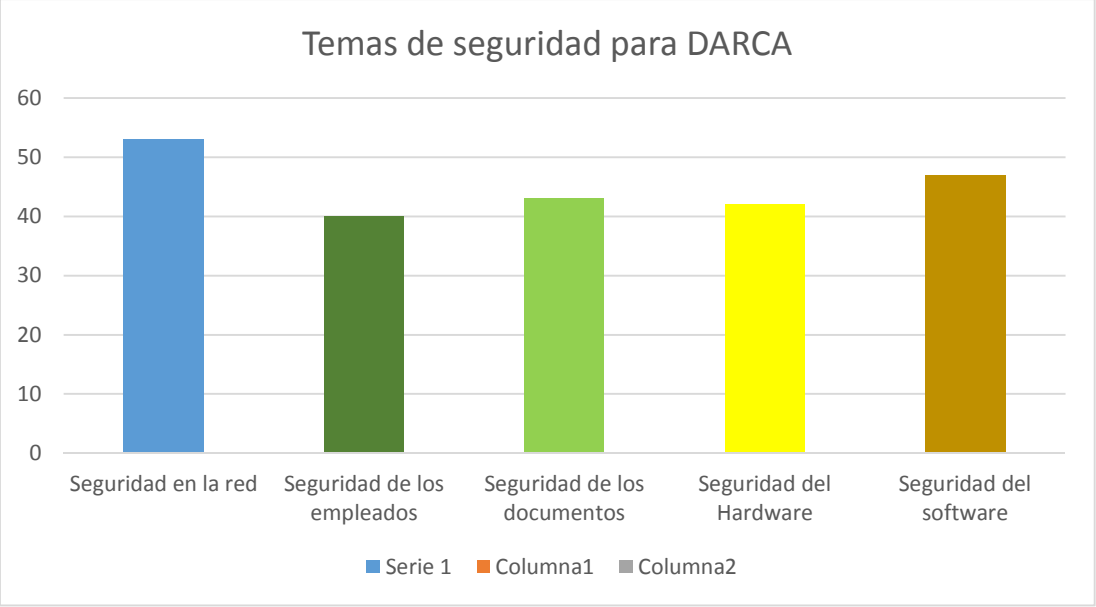


Fig. 26. Resultados Pregunta 10.

B.2. Entrevistas

- **Entrevista dirigida al jefe de DARCA**

Políticas

Pregunta	Respuesta
a. ¿Cuál es su posición como jefe de DARCA respecto al apoyo en la implementación de un modelo de gestión de seguridad de la información para el procedimiento *Evaluación de la Prueba*?	Apoyo el SGSI porque el procedimiento *Inscripciones y Admisiones* está a mi cargo y soy muy responsable de este procedimiento y necesita de la seguridad de la información.
b. ¿Conoce la política del sistema de gestión de seguridad de la información de la Universidad del Cauca?	No
c. ¿Existe una política formalmente establecida de seguridad de la información al interior de DARCA?	No
d. ¿Quiénes aprueban las políticas y cuál es el proceso para su aprobación?	Tienen que hablar con el centro de gestión de la calidad porque ellos con ellos se hace todo el trámite de la elaboración de la política y luego pasa para la aprobación de la alta dirección.
e. ¿Existen procedimientos formales para hacer cumplir las políticas?	No sé, Habría que preguntarle al jefe de gestión de la Calidad.
f. ¿Cómo es el proceso utilizado para la divulgación de políticas a los empleados de DARCA?	Las políticas se realizan por medio del portal Ivmen o reuniones que realizan en donde convocan al personal, o cada que hay algo nuevo la institución se comunica la política permanentemente.
g. ¿Qué acciones se toman en DARCA cuando existe un incidente de seguridad de la información?	Mientras he estado aquí no ha pasado nada. A veces llegan correos diciendo que ha sucedido algo en SIMCA y lo que se hace es pedir una auditoria y un rastreo.
h. ¿Qué medidas se toman en DARCA para garantizar la seguridad de la información?	Indicarles a los funcionarios lo aprendido en las reuniones realizadas, de lo aprendido y escuchado acerca de la seguridad de la información. Decirles que tengan cuidado con los equipos, con la información y con el ingreso de las personas.
i. ¿DARCA cuenta con restricciones de control de acceso ante el personal ajeno al departamento?	En este momento el biométrico que controla la entrada a los funcionarios de DARCA no funciona, y esto debe arreglarse. En este momento la puesta no funciona. Los colaboradores no tienen cultura de seguridad de la información
j. ¿Existe una política de seguridad de la información exclusiva para el procedimiento *Evaluación de la Prueba*?	No
k. ¿Al realizar el procedimiento *Evaluación de la Prueba* existen restricciones de control de acceso ante el personal ajeno al proceso?	Si, tanto en DARCA como en Medellín.
l. ¿Los equipos de trabajo utilizados en las instalaciones de DARCA y en el Procedimiento *Evaluación de la Prueba* son protegidos contra virus informáticos?	Sí, todos los equipos tienen antivirus actualizados por el área de mantenimiento

m.	¿Se guardan copias de seguridad de los equipos de trabajo utilizados en el procedimiento *Evaluación de la Prueba* de manera constante?	Se han estado sacando las copias, el ingeniero Rodrigo realiza una copia de seguridad dos veces al día, para el procedimiento Evaluación de la Prueba.
n.	¿Los funcionarios de DARCA que intervienen en el procedimiento *Evaluación de la Prueba* establecen prácticas de seguridad para la selección y uso de contraseñas?	Si
o.	¿Cada cuánto se cambian las contraseñas que utilizan los empleados de DARCA que intervienen en el procedimiento *Evaluación de la Prueba* para ingresar a los equipos de cómputo?	Permanentemente, cada mes o dos meses
p.	¿Los empleados de DARCA que intervienen en el procedimiento *Evaluación de la Prueba* tienen definidas sus responsabilidades frente a los activos de información que manejan y la información contenida en ellos?	Si
q.	¿Los derechos de acceso a los funcionarios de DARCA que intervienen en el procedimiento *Evaluación de la Prueba* se revisan frecuentemente?	Sí, porque existen permisos diarios.
r.	¿Las personas que intervienen en el procedimiento *Evaluación de la Prueba* y que tienen a cargo equipos de cómputo saben cómo deben utilizarlos para la seguridad Software y Hardware?	Si
s.	¿Existe un horario en el cual la sesión del sistema se encuentra activa, y después de este horario se suspenden?	Si
t.	¿Se realizan pruebas de la calidad de las contraseñas de manera frecuente?	No lo sé. Esta parte es responsabilidad de la división de TIC.
u.	¿Existe un tiempo de inactividad definido para que los equipos de cómputo suspendan la sesión en el sistema?	Si, y además el equipo acostumbro a bloquearlo de manera manual, cuando salgo.
v.	El antivirus que tienen instalado (si es el caso), ¿está actualizado?	Si, y no solo los antivirus, sino los programas tienen licencia y esto se monitorea desde mantenimiento.

TABLA XIII. Entrevista de Política de seguridad de la información – Jefe DARCA

Capacitación

Pregunta		Respuesta
a.	¿Existe un programa de capacitación en políticas de seguridad de la información en DARCA?	No
b.	¿Existe una estrategia de capacitación que incluya la seguridad de las tecnologías compatibles en el procedimiento *Evaluación de la Prueba*?	No
c.	¿Existe un programa de capacitación que aborde temáticas relacionadas con la seguridad de la información?	No
d.	¿La universidad del Cauca o DARCA cuenta con un procedimiento de capacitación documentada?	No

e.	¿Los empleados de DARCA conocen la normatividad relacionada con la seguridad de la información?	No
f.	¿Los empleados de DARCA y contratistas reciben formación acerca de la seguridad de la información en lo que respecta a sus funciones de trabajo?	Los empleados reciben directrices de la seguridad de la información en su puesto de trabajo, pero no se ha hecho capacitación.
g.	¿Los temas de seguridad de la información se orientan con respecto a las características y necesidades del procedimiento *Evaluación de la Prueba*?	No, pero debería ser así.
h.	¿La capacitación se orienta con unos lineamientos especializados o con lineamientos básicos?	No
i.	¿DARCA mantiene contacto con grupos de interés, foros de seguridad especializados, o asociaciones profesionales en relación a la seguridad de la información?	No
j.	¿DARCA cuenta con un mecanismo formal para proporcionar actualizaciones periódicas / boletines sobre los problemas de seguridad a los miembros del personal que intervienen en el procedimiento *Evaluación de la Prueba*.	No
k.	¿Qué temas considera pertinentes para realizar la capacitación en seguridad de la información?	Todos, porque estamos en ceros.

TABLA XIV. Entrevista de Capacitaciones de seguridad de la información – Jefe DARCA

Procedimientos y Registros

Pregunta		Respuesta
a.	¿Anteriormente ha habido incidentes que vulneran la seguridad de la información? ¿Cómo se han manejado estos incidentes?	No se sabe
b.	¿Existe un procedimiento que defina la forma en que los incidentes de seguridad de la información deben ser reportados?	Los incidentes se reportan a la división de TIC, o se les pide que ayuden a investigar lo que ha sucedido. No existe un procedimiento formalmente establecido.
c.	¿Existen actividades de seguridad de la información que sean coordinadas por áreas como RRHH, mantenimiento, División de las TIC y otros?	Por el momento no, pero puede ser que estas actividades no se realicen por las demás actividades que se deja a un lado lo importante de la seguridad de la información.
d.	¿Considera importante que las actividades de seguridad de la información sean compartidas con otras áreas como la DivTIC, RRHH, Calidad, mantenimiento, según sus roles y responsabilidades pertinentes?	Si, estas divisiones son las que deben estar apoyando a DARCA y la vicerrectoría académica porque DARCA depende mucho de ellos.
e.	¿Cada cuánto se realiza mantenimiento preventivo sobre los ordenadores de DARCA?	No hay una periodicidad, y esto es manejado por el área de mantenimiento donde manejan un cronograma
f.	¿Existe una revisión de políticas, objetivos, controles, procesos y procedimientos para la seguridad de la información y su implementación?	No
g.	¿DARCA o la Universidad del Cauca cuentan con procedimientos de operación	No

	documentados y están disponibles a todos los usuarios cuando sea requerido?	
h.	¿Son auditados regularmente los servicios prestados por terceros?	No sabe
i.	¿Se mantienen registros de las actividades de auditoria, excepciones y eventos de seguridad de la información? ¿Estos registros son mantenidos por un periodo de tiempo acordado para ayudar en investigaciones futuras y monitoreo del control de acceso?	No
j.	¿A detectado amenazas y/o vulnerabilidades que puedan afectar la seguridad de su información de DARCA?	Errores humanos del personal DARCA.

TABLA XV. Entrevista Procedimientos – Jefe DARCA

- **Entrevista dirigida al personal de DARCA**

a. ¿Conoce la política del sistema de gestión de seguridad de la información de la Universidad del Cauca?	
Código	**Respuesta**
B01	Un poquito
B02	No
B03	No la conoce, pero si realiza las prácticas de seguridad.
B04	No
B05	No
B06	No
B07	Si
B08	No
B09	No
B10	No
B11	Si
B12	No
B13	No
B14	No

TABLA XVI. Pregunta literal a - entrevista

b. ¿Sabe usted de algún incidente de seguridad de la información que haya sucedido al interior de DARCA?	
Código	**Respuesta**
B01	No
B02	No
B03	No
B04	No
B05	No
B06	No
B07	No
B08	No
B09	No
B10	No

B11	No
B12	No
B13	No
B14	No

TABLA XVII. Pregunta literal b - entrevista

c. ¿Qué acciones ha tomado ante un incidente de seguridad de la información?	
Código	**Respuesta**
B01	No ha sucedido
B02	No ha sucedido
B03	No ha sucedido
B04	No ha sucedido
B05	No ha sucedido
B06	No ha sucedido
B07	No ha sucedido
B08	No ha sucedido
B09	No ha sucedido
B10	No ha sucedido
B11	No ha sucedido
B12	No ha sucedido
B13	No ha sucedido
B14	No ha sucedido

TABLA XVIII. Pregunta literal c - entrevista.

d. ¿Sabe cuál es el procedimiento para reportar los incidentes de seguridad de la información en caso de que lleguen a suceder?	
Código	**Respuesta**
B01	Si. Primero se informa a la jefe inmediata y luego oficializar el incidente.
B02	Reportar a la División de las TIC
B03	Informarle al jefe inmediato, poner un denuncio y luego ir a recursos humanos o control interno a dar un reporte.
B04	No
B05	Denunciar
B06	No
B07	No
B08	No
B09	No
B10	No
B11	Si
B12	No
B13	No
B14	No

TABLA XIX. Pregunta literal d - entrevista.

e. ¿Su equipo de trabajo está protegido contra virus informático?	
Código	**Respuesta**
B01	Creo que si
B02	Si
B03	Si

B04	Si
B05	Si
B06	Si
B07	Si
B08	Si
B09	Si
B10	Si
B11	Si
B12	Si
B13	Si
B14	Si

TABLA XX. Pregunta literal e - entrevista**.**

f. ¿La computadora empleada para realizar su trabajo tiene información relevante para DARCA almacenados dentro de su disco duro?	
Código	**Respuesta**
B01	Si. El computador tiene el sistema delta
B02	No
B03	No
B04	Si
B05	Si
B06	Si
B07	Si
B08	Si
B09	Si
B10	Si
B11	No
B12	Si
B13	No
B14	Si

TABLA XXI. Pregunta literal f - entrevista.

g. ¿Acostumbra a guardar copias de seguridad del disco duro de su equipo de trabajo? ¿Cada cuánto lo hace?	
Código	**Respuesta**
B01	No
B02	No acostumbra guardar copias de seguridad
B03	No
B04	Si
B05	Cada fin de periodo académico
B06	Si
B07	No
B08	Si (Cada 2 o 3 Meses)
B09	SI, cada 8 días
B10	SI, cada 6 meses
B11	Si
B12	No
B13	Una vez al mes
B14	No, envían copias a correos alternativos.

TABLA XXII. Pregunta literal g - entrevista.

h. ¿Establece prácticas de seguridad para la selección y uso de contraseña?	
Código	**Respuesta**
B01	Si
B02	No
B03	Utiliza letras y números para la contraseña.
B04	No
B05	Si
B06	Si
B07	Si
B08	No
B09	Si
B10	Si
B11	Si
B12	Si
B13	Si
B14	Si

TABLA XXIII. Pregunta literal h - entrevista.

i. ¿Cada cuánto cambia la contraseña de ingreso al equipo de trabajo?	
Código	**Respuesta**
B01	Cambia su contraseña cada tres meses o dos meses.
B02	Cada 5 meses
B03	No ha cambiado nunca la contraseña de ingreso al computador. Para ingresar a SIMCA se ha visto obligada a cambiar la contraseña porque la plataforma se lo exige. (Ha cambiado la contraseña 5 veces en 7 años)
B04	No la cambia a menos que se bloquee SIMCA y le pida un cambio de contraseña.
B05	Cada seis meses
B06	Cada dos o tres meses
B07	Cada dos o tres meses
B08	Cada año
B09	Cada mes
B10	Cada seis meses
B11	Cada ocho o quince días
B12	Cada seis meses
B13	Cada 15 días
B14	Cada dos meses

TABLA XXIV. Pregunta literal i - entrevista.

j. ¿Sabe cómo debe utilizar su equipo de trabajo para la seguridad del Software y del Hardware?	
Código	**Respuesta**
B01	Si
B02	No
B03	Si
B04	No
B05	No
B06	No
B07	No
B08	Si
B09	Si

B10	No
B11	Si
B12	No
B13	No
B14	No

Tabla XXV. Pregunta literal j - entrevista.

k. ¿Se realizan capacitaciones en cuanto a seguridad de la información? En caso Afirmativo, ¿Cada cuánto se realizan estas capacitaciones?, ¿Quién dicta estas capacitaciones?	
Código	**Respuesta**
B01	No sabe
B02	No
B03	No
B04	No ha escuchado acerca de ninguna capacitación.
B05	No
B06	No
B07	No
B08	No
B09	No
B10	No
B11	No
B12	No
B13	No
B14	No

TABLA XXVI. Pregunta literal k - entrevista.

l. ¿Qué temas considera pertinentes para ser capacitado con respecto a la seguridad de la información?	
Código	**Respuesta**
B01	Considera que es más importante la seguridad de los programas.
B02	Proteger la información contra intrusos
B03	Control de acceso
B04	Todo lo que tiene que ver con seguridad de la información
B05	Todo lo concerniente a la seguridad de la información
B06	Seguridad de programas
B07	Todo lo de seguridad informática
B08	Resguardo de archivos, evitar accesos remotos
B09	Copias de seguridad y seguridad informática
B10	Reporte de incidentes
B11	Que hacer en caso de un ataque informático
B12	Todo lo de seguridad informática
B13	seguridad en desarrollo de aplicaciones, bases de datos, redes
B14	No sabe

TABLA XXVII. Pregunta literal l - entrevista.

m. ¿Conoce sobre normatividad relacionada con la seguridad de la información? En caso afirmativo ¿Qué ley, norma, estatuto, reglamentación conoce?	
Código	**Respuesta**
B01	No las conoce
B02	No

B03	No
B04	No
B05	No
B06	No
B07	No
B08	No
B09	Si
B10	No
B11	No
B12	No
B13	No
B14	No

TABLA XXVIII. Pregunta literal m - entrevista.

B.3. Lista de Chequeo

Requisitos de la norma NTC-ISO/IEC 27001		¿El procedimiento *Inscripciones y Admisiones* cuenta con este requisito?		
Clausula		**Si**	**No**	**Observaciones**
4. Contexto de la organización	**4.1** Conocimiento de la organización y de su contexto	X		No cumple para DARCA, si para el procedimiento *Inscripciones y Admisiones*
	4.2 Comprensión de necesidades y expectativas	X		
	4.3 Determinación del alcance	X		
5. Liderazgo	**5.1** Liderazgo y compromiso	X		La política de la Universidad del Cauca aplica para DARCA
	5.2 Política	X		
	5.3 Roles y responsabilidades		X	
6. Planificación	**6.1** Acciones para tratar riesgos y oportunidades	X		No existen planes para DARCA
	6.2 Objetivos de seguridad de la información y planes		X	
7. Soporte	**7.1** Recursos		X	
	7.2 Competencia		X	
	7.3 Toma de Conciencia		X	
	7.4 Comunicación		X	
	7.5 Información Documentada		X	
8. Operación	**8.1** Planificación y control operacional		X	
	8.2 Valoración de riesgos de la seguridad de la información realizado constantemente		X	
	8.3 Tratamiento de riesgos de seguridad de la información realizado constantemente		X	
9. Evaluación de desempeño	**9.1** Seguimiento, medición, análisis		X	
	9.2 Auditoría Interna		X	
	9.3 Revisión por la dirección		X	
10. Mejora	**10.1** No conformidades y acciones Correctivas		X	
	10.2 Mejora Continua		X	

TABLA XXIX. Tabulación Lista de chequeo

Anexo C. MAPEO ENTRE SUBCRITERIOS DEL MODELO EFQM Y REQUISITOS DE ISO/IEC 27001

Criterio *Liderazgo*	***Liderazgo***
Subcriterios (Modelo EFQM)	**ISO/IEC 27001.**
1a. Los líderes desarrollan la Misión, Visión, valores y principios éticos y actúan como modelo de referencia.	No especificado
1b. Los líderes definen, supervisan, revisan e impulsan tanto la mejora del sistema de gestión de la organización como su rendimiento.	**5.1.** Liderazgo y compromiso **5.2.** Política de la seguridad de la información
1c. Los líderes se implican con los grupos de interés externos.	Los grupos de interés externo (proveedores, sociedad, trabajadores, otros…) no tienen consideración en la norma ISO/IEC 27001. No obstante, en la norma ISO 27002 se encuentra el dominio A.15: seguridad con los proveedores
1d. Los líderes refuerzan una cultura de excelencia entre las personas de la organización	**5.3.** Roles y responsabilidades
1e. Los líderes se aseguran de que la organización sea flexible y gestionan el cambio de manera eficaz.	**9.3.** Revisión por la dirección.
Criterio *Estrategia*	***Programa de implementación***
Subcriterios (Modelo EFQM)	**ISO/IEC 27001.**
2a. La estrategia se basa en comprender las necesidades y expectativas de los grupos de interés y del entorno externo.	**6.1.** Acciones para tratar riesgos y oportunidades **4.1.** Conocimiento de la organización y de su contexto. **4.2.** Comprensión de las necesidades y expectativas de las partes **4.3.** Determinación del alcance del Sistema de Gestión de la seguridad de la información
2b. La estrategia se basa en comprender el rendimiento de la organización y sus capacidades.	
2c. La estrategia y sus políticas de apoyo se desarrollan, revisan y actualizan.	**6.2.** Objetivos de seguridad de la información y planes para lograrlos. (Elaborar los planes) **8.1.** Planificación y control operacional (implantar los planes)
2d. La estrategia y sus políticas de apoyo se comunican, implantan y supervisan.	**10.2.** Mejora continua **8.2.** Valoración de riesgos de seguridad de la información **8.3** Tratamiento de riesgos de la seguridad de la información
Criterio *Personas*	***Competencia y toma de conciencia***
Subcriterios (Modelo EFQM)	**ISO/IEC 27001.**
3a. Los planes de gestión de las personas apoyan la estrategia de la organización.	**7.3.** Toma de conciencia
3b. Se desarrolla el conocimiento y las capacidades de las personas.	**7.2.** Competencia
3c. Las personas están alineadas con las necesidades de la organización, implicadas y asumen su responsabilidad.	No especificado
3d. Las personas se comunican eficazmente en toda la organización.	No especificado

3e. Recompensa, reconocimiento y atención a las personas de la organización.	No especificado
Criterio *Alianzas y Recursos*	***Recursos***
Subcriterios (Modelo EFQM)	**ISO/IEC 27001.**
4a. Gestión de aliados y proveedores para obtener un beneficio sostenible.	7.4. Comunicación
4b. Gestión de los recursos económico-financieros para asegurar un éxito sostenido.	**7.1.** Recursos
4c. Gestión sostenible de edificios, equipos, materiales y recursos naturales.	
4d. Gestión de la tecnología para hacer realidad la estrategia.	
4e. Gestión de la información y el conocimiento para apoyar una eficaz toma de decisiones y construir las capacidades de la organización.	Este es el enfoque de la norma ISO/IEC 27001.
Criterio *Procesos, Productos y Servicios*	***Procesos y procedimientos***
Subcriterios (Modelo EFQM)	**ISO/IEC 27001.**
5a. Los procesos se diseñan y gestionan a fin de optimizar el valor para los grupos de interés.	7.5. Información Documentada 8.1. Planificación y control operacional
5b. Los Productos y Servicios se desarrollan para dar un valor óptimo a los clientes	No especificado
5c. Los Productos y Servicios se promocionan y ponen en el mercado eficazmente	No especificado
5d. Los Productos y Servicios se producen, distribuyen y gestionan.	No especificado
5e. Las relaciones con los clientes se gestionan y mejoran.	No especificado
Criterio *Resultados*	***Resultados***
Subcriterios (Modelo EFQM)	**ISO/IEC 27001.**
9a. Resultados Clave de la Actividad	9.1. Seguimiento, medición, análisis y evaluación 9.2. Auditoría interna 9.3. Revisión por la dirección 10.1 No conformidades y acciones correctivas
9b. Indicadores Clave de Rendimiento de la Actividad	

.

Anexo D. REGISTROS - ACTAS DE REUNIÓN CON LA ALTA DIRECCIÓN

Universidad del Cauca

Gestión de la Calidad
Gestión de la Calidad Administrativa
Acta General para Actividades Universitarias

Código: PE-GS-2.2.1-FOR-22	Versión: 0	Fecha de Actualización: 17-01-2017

Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad		Estudiantes Deisy Imbachi y Fabio Cerón	
Fecha	20	02	2017	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	6 pm	8 pm	División de Admisiones, Registro y Control	01

ORDEN DEL DIA

1. Verificación de Asistencia
2. Lectura de acta anterior SI ☐ NO ☐
3. Temas a tratar

No	TEMAS A TRATAR
1	Presentación del proyecto Implantación de la fase de Ejecución de un SGSI adaptando un marco de referencia con base en la norma ISO/IEC 27001:2013.
2	Aportes de la seguridad de la información al procedimiento Inscripciones y Admisiones.

DESARROLLO DE LA REUNIÓN

Esta primera fase inicio con una reunión realizada en la división de admisiones registro y control académico – DARCA, en donde participaron los estudiantes Fabio Cerón y Deisy Imbachi, con la presencia del jefe de DARCA. En esta primera reunión se le dio a conocer al jefe de DARCA el contexto en el que se encuentra ubicado este trabajo de grado y sus aportes en cuanto a la seguridad de la información en el procedimiento Inscripciones y Admisiones.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Manuel Zuñiga	Prof. Especializado	Darca	
2	Deisy Imbachi	Estudiante	Fiet	Deisy F. Imbachi
3	Fabio Cerón	Estudiante	Fiet	

OBSERVACIONES

NOMBRE QUIEN PRESIDE — Deisy Imbachi

FIRMA DE QUIEN PRESIDE

NOMBRE SECRETARIO — Fabio Cerón

FIRMA SECRETARIO

Fig. 27. Acta **-** Primera reunión

Universidad del Cauca

Gestión de la Calidad
Gestión de la Calidad Administrativa
Acta General para Actividades Universitarias

Código: PE-GS-2.2.1-FOR-22	Versión: 0	Fecha de Actualización: 17-01-2017

Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad		Estudiantes Deisy Imbachi y Fabio Cerón	
				Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
Fecha	27	02	2017	6 pm	8 pm	División de Admisiones, Registro y Control – DARCA	02
	Día	Mes	Año				

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI** ☐ **NO** ☐
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Aspectos más relevantes del SGSI y la importancia de su implantación
2	Introducción a la Norma ISO/IEC 27001 y sus requisitos.

DESARROLLO DE LA REUNIÓN

En esta reunión se dieron a conocer los aspectos más relevantes de un SGSI y la importancia de su implantación para la preservación de la confidencialidad, integridad y disponibilidad. Además, se realizo una introduccion a la norma ISO/IEC 27001 y sus requisitos con base en las fases del ciclo Deming.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Deisy Imbachi	Estudiante	FIET	
2	Fabio Perdomo	Estudiante	FIET	
3	Marisol Zuñiga	Prof. Especializado	DARCA.	

OBSERVACIONES

NOMBRE QUIEN PRESIDE

Fabio Cerón

FIRMA DE QUIEN PRESIDE

NOMBRE SECRETARIO

Deisy Imbachi

FIRMA SECRETARIO

Fig. 28. Acta – Segunda Reunión

Universidad del Cauca

Gestión de la Calidad
Gestión de la Calidad Administrativa
Acta General para Actividades Universitarias

Código: PE-GS-2.2.1-FOR-22	Versión: 0	Fecha de Actualización: 17-01-2017

Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad		Estudiantes Deisy Imbachi y Fabio Cerón.	
Fecha	06	03	2017	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	6:00 pm	8:00 pm	División de Admisiones, Registro y Control	03

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI ☐ NO ☐**
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Descripción de la pare plan del SGSI y de los documento obligatorios.
2	

DESARROLLO DE LA REUNIÓN

En esta reunión se realizo una descripción de la pare plan del SGSI y de los documentos obligatorios que están contenidos en esta pare, desarrollada y finalizada para el procedimiento Inscripciones y Admisiones

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Marisol Zuñiga	Prof. Especializado	DARCA	
2	Fabio Cerón	Estudiante	Fiet	
3	Deisy Imbachi	Estudiante	Fiet	Deisy F. Imbachi

OBSERVACIONES

NOMBRE QUIEN PRESIDE

Deisy Imbachi

FIRMA DE QUIEN PRESIDE

NOMBRE SECRETARIO

Fabio Cerón

FIRMA SECRETARIO

Fig. 29. Acta – Tercera Reunión

Universidad del Cauca

Gestión de la Calidad
Gestión de la Calidad Administrativa
Acta General para Actividades Universitarias

Código: PE-GS-2.2.1-FOR-22	Versión: 0	Fecha de Actualización: 17-01-2017

Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad		Estudiantes Deisy Imbachi y Fabio Cerón.	
Fecha	13	03	2017	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	7:pm	9 PM	Division de Admisiones, Registro y Control.	04

ORDEN DEL DIA

1. Verificación de Asistencia
2. Lectura de acta anterior SI ☐ NO ☐
3. Temas a tratar

No	TEMAS A TRATAR
1	Descripcion de la fase ejecucion y sus documentos
2	

DESARROLLO DE LA REUNIÓN

En esta reunión se realizo una descripción de la fase ejecucion del SGSI y de de los documentos obligatorios y actividades que respectan a esta fase a ser desarrollada en el alcance del procedimiento Inscripciones y Admisiones.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Marisol Zuñiga	Prof. Especializado	Darca	
2	Deisy Imbachi	Estudiante	Fiet	Deisy F. Imbachi
3	Fabio Cerón	Estudiante	Fiet.	

OBSERVACIONES

NOMBRE QUIEN PRESIDE

Deisy Imbachi

FIRMA DE QUIEN PRESIDE

NOMBRE SECRETARIO

Fabio Cerón

FIRMA SECRETARIO

Fig. 30. Acta – Cuarta Reunión

Universidad del Cauca

Gestión de la Calidad
Gestión de la Calidad Administrativa
Acta General para Actividades Universitarias

Código: PE-GS-2.2.1-FOR-22	Versión: 0	Fecha de Actualización: 17-01-2017

Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad		Estudiantes Deisy Imbachi y Fabio Ceron	
Fecha	21	03	2017	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	6PM	8 PM	Division de Admisiones, Registro y Control – DARCA	05

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI ☐ NO ☐**
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Determinar compromisos por parte del jefe de DARCA.
2	

DESARROLLO DE LA REUNIÓN

En esta reunion se determinar los compromisos por parte del jefe de DARCA para desarrollar la fase ejecución del SGSI en el procedimiento Inscripciones y Admisiones.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Manisol Zuniga	Prof. Especializado	DARCA	
2	Deisy Imbachi	Estudiante	FIET	Deisy F. Imbachi
3	Fabio Ceron	Estudiante	FIET.	

COMPROMISOS

No	COMPROMISO	RESPONSABLE	FECHA COMPROMISO	FECHA DE REALIZACIÓN
1	Apoyar el establecimiento de la Politica	Jefe DARCA	21-03-2017	
2	Integrar requisitos del SGSI a procesos DARCA	Jefe DARCA	21-03-2017	
3	Importancia de SGSI efectiva compromiso SI	Jefe DARCA	21-03-2017	
4	Motivar a los funcionarios a contribuir con SGSI	Jefe DARCA	21-03-2017	
5	Promover la mejora continua	Jefe DARCA	21-03-2017	

Fig. 31. Acta – Quinta Reunión (p.1)

Universidad del Cauca

Gestión de la Calidad
Gestión de la Calidad Administrativa
Acta General para Actividades Universitarias

Código: PE-GS-2.2.1-FOR-22	Versión: 0	Fecha de Actualización: 17-01-2017

OBSERVACIONES

GSI: Gestion de la seguridad de la información.
GSI es importante que este conforme a los requisitos del SGSI

NOMBRE QUIEN PRESIDE: Fabio Cossio

FIRMA DE QUIEN PRESIDE

NOMBRE SECRETARIO: Deisy Imbachi

FIRMA SECRETARIO

Fig. 32. Acta – Quinta Reunión (p.2)

Anexo E. CUESTIONARIO DE AUTOEVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MARCO DE REFERENCIA PROPUESTO

Criterio 1: *Liderazgo*			
Sub-criterio	**Cuestionario**	**Repuesta**	
		Si	**No**
1.1. El líder supervisa y revisa la política de seguridad de la información el alcance definido	▪ ¿La alta dirección se involucra activamente en la creación de la política de seguridad de la información?.		**X**
	▪ ¿La alta dirección se involucra activamente en la actualización de la política de seguridad de la información?.		**X**
1.2. El líder impulsa el establecimiento y mejora continua de la política del SGSI en el alcance definido, y su rendimiento.	▪ ¿La alta dirección supervisa que la política se haya establecido?		**X**
	▪ ¿La alta dirección impulsa garantiza que los recursos para establecer la política de seguridad de la información estén asegurados y disponibles?		**X**
1.3. El líder revisa y gestiona el SGSI en el alcance definido a intervalos planificados.	▪ ¿La alta dirección revisa y gestiona los cambios internos y externos pertinentes con el SGSI?		**X**
	▪ ¿La alta dirección revisa y gestiona el programa de implementación del SGSI?		**X**
	▪ ¿La alta dirección revisa los resultados de las mediciones y de la auditoria interna del SGSI.		**X**
	▪ ¿La alta dirección revisa las oportunidades de mejoramiento a auditoría interna del SGSI?		**X**
1.4. Comunicación y apoyo de los planes y las actividades de Seguridad de la información.	▪ ¿La alta dirección comunica al talento humano los planes y actividades en relación con el SGSI?		**X**
	▪ ¿La alta dirección brinda apoyo a las actividades en seguridad de la información, especialmente a las de capacitación?		**X**
	▪ ¿La alta dirección brinda los recursos necesarios para desarrollar los planes de tratamiento de riesgos?		**X**
	▪ ¿La alta dirección se involucra activamente en la realización de los planes?		**X**
Criterio 2: *Programa de Implementación del SGSI*			
Sub-criterio	**Cuestionario**	**Repuesta**	
		Si	**No**
2.1. Desarrollo del programa de implementación de SGSI	▪ ¿Se han establecido objetivos de seguridad de la información?		**X**
	▪ ¿Los objetivos trazados son coherentes con la política de seguridad de la información?		**X**
	▪ ¿Se ha establecido un plan para lograr los objetivos de seguridad de la información?		**X**
	▪ ¿El plan anteriormente establecido asigna los recursos y los responsables necesarios para realizar las actividades?		**X**
	▪ ¿El plan establecido determina un tiempo de ejecución y la manera de evaluación?		**X**
Criterio 3: *Competencia y Toma de conciencia*			

Sub-criterio	Cuestionario	Repuesta	
		Si	No
3.1. Gestión de las competencias del talento humano	▪ ¿Se definen las habilidades y competencias específicas en seguridad de la información, que deben tener o desarrollar las personas del procedimiento *Inscripciones y Admisiones*?		**X**
	▪ ¿Se determinan (evalúan) las competencias en seguridad de la información que tienen las personas que están dentro del alcance del SGSI?		**X**
	▪ ¿Se desarrollen competencias en las personas (dentro del alcance del SGSI), basándose en educación y formación?		**X**
3.2. Educación y capacitación del personal	▪ ¿Se realiza planificación de capacitaciones en seguridad de la información de acuerdo a las necesidades del procedimiento Inscripciones y Admisiones?		**X**
	▪ ¿Existen y se desarrollan capacitaciones en seguridad de la información dentro de la organización, al menos una vez al año?		**X**
	▪ ¿Se evalúa al personal a mejorar sus competencias en seguridad de la información?		**X**
Criterio 4: *Recursos y alianzas*			
Sub-criterio	**Cuestionario**	**Repuesta**	
		Si	**No**
4.1. Gestión de recursos financieros para apoyar los programas de implementación del SGSI	▪ ¿Se asignan y distribuyen recursos financieros que apoyen el programa de implementación del SGSI y planes relacionados?		**X**
4.2. Gestión de recursos físicos	▪ ¿Se optimiza el uso de los recursos físicos tangibles incluidos edificios, equipos y materiales?	**X**	
	▪ ¿Se realiza una gestión adecuada de materiales, empleando una buena cadena de suministros?		**X**
4.3. Gestión de recursos tecnológicos	▪ ¿Se utiliza correctamente la tecnología?	**X**	
	▪ ¿Se implican grupos de interés en el programa de implementación del SGSI en relación con tecnologías existentes y novedosas?		**X**
4.4. Gestión de alianzas	▪ ¿Se establecen relaciones sostenibles con áreas externas a DARCA y proveedores, para el fortalecimiento del SGSI?		**X**
	▪ ¿Se adoptan políticas y procesos para relacionarse con áreas externas y proveedores?		**X**
	▪ ¿Se mejoran continuamente las alianzas existentes?		**X**
Criterio 5: *Procesos y procedimientos del SGSI*			
Sub-criterio	**Cuestionario**	**Repuesta**	
		Si	**No**
5.1. Los procesos correspondientes a la fase Ejecución del SGSI se diseñan y gestionan.	▪ ¿Se planifican, implementan y controlan los procesos del SGSI? ¿Qué procesos se implementan?		**X**
	▪ ¿Los procesos se llevan a cabo conforme a la planeación realizada?		**X**
	▪ ¿Antes de llevar a cabo los procesos, estos se comunican a los grupos de interés (personal, clientes, proveedores, área de tecnología)?		**X**
	▪ ¿El desarrollo del proceso es supervisado en aras de identificar ventajas competitivas presentes y futuras?		**X**

5.2. Desarrollo de los procedimientos de la fase *Ejecución* del SGSI.	▪ ¿Se establecen procedimientos adecuados para llevar a cabo los procesos del SGSI?		**X**
	▪ ¿Se comunican y se publican los procedimientos relativos al SGSI?		
	▪ ¿Los procedimientos contienen el conjunto de formatos que se requieren para llevar a cabo el proceso?		**X**
Criterio 6: *Resultados del SGSI*			
Sub-criterio	**Cuestionario**	**Repuesta**	
		Si	**No**
6.1. Resultado de auditoria interna	▪ ¿La alta dirección revisa el SGSI del procedimiento *Inscripciones y Admisiones* a intervalos planificados?		**X**
	▪ ¿Se realizan auditorías internas del SGSI?		**X**
	▪ ¿Se realizan las acciones correctivas correspondientes para eliminar las causas de una no conformidad?		**X**
6.2. Resultados de la medición y análisis	▪ ¿Se realizan mediciones a los controles implementados?		**X**
	▪ ¿Se analizan los resultados cualitativos y cuantitativos con base en indicadores de mediciones para determinar oportunidades de mejora?		**X**

TABLA XXX. Cuestionarios de autoevaluación de un SGSI

Criterio	Fortalezas	Debilidades	Oportunidades	Evidencias
1. Liderazgo				
2. Programa de Implementación del SGSI				
3. Competencia y Toma de conciencia				
4. Recursos y alianzas				
5. Procesos y procedimientos del SGSI				
6. Resultados del SGSI				

TABLA XXXI. Resultados generales de la aplicación de los cuestionarios de autoevaluación de un SGSI

Anexo F. PLANES DE ACCIÓN PARA EL PROCEDIMIENTO *INSCRIPCIONES Y ADMISIONES*

- **PLAN DE ACCIÓN ASOCIADO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.**

  Descripción: Este proyecto busca fortalecer el control de seguridad de información A.5.1.1 extraído del anexo A de la norma ISO/IEC 27001:2013 para ser aplicado en el procedimiento *Inscripciones y Admisiones*, perteneciente a DARCA de la Universidad del Cauca. La ejecución del control se enfoca en que la política sea comunicada a los empleados y las partes interesados.

  Objetivo:

  - Dar a conocer la política de seguridad de la información de la Universidad del Cauca a los funcionarios de DARCA.
  - Dar a conocer la política de seguridad de la información del procedimiento *Inscripciones y Admisiones* a los funcionarios de DARCA.

  Alcance: Este proyecto cubre al personal que labora DARCA (Profesional especializado).

  Fases: Este proyecto comprende las siguientes fases:

  - **Evaluación del estado actual del control:** Se analiza el estado en el que se encuentran el control A.5.1.1 en el marco del procedimiento *Inscripciones y Admisiones*.
  - **Elaboración de Capacitaciones:** En esta fase se diseñan las estrategias necesarias para que los funcionarios de DARCA conozcan las políticas de seguridad de la información de la Universidad del Cauca y las políticas de seguridad de la información del procedimiento *Inscripciones y Admisiones.*
  - **Ejecución de trabajos:** Llevar a cabo las actividades necesarias para emplear la estrategia diseñada.

Cronograma: El cronograma propuesto para este proyecto es de cuatro (4) meses:

Fase	Semana 1				Semana 2				Semana 3				Semana 4			
Evaluación del estado actual	X	X														
Estructuración de procedimientos			X	X	X											
Ejecución de trabajos					X	X	X	X	X	X						
Pruebas											X	X				
Entrenamiento												X	X			
Puesta en marcha													X	X	X	
Reporte															X	X

- **PLAN DE ACCIÓN ASOCIADO LA FORMACIÓN Y TOMA DE CONCIENCIA.**

  Descripción: Este proyecto busca fortalecer el control relacionado con el control A.7.2.2 extraído del anexo A de la norma ISO/IEC 27001: 2013 para ser aplicado en el procedimiento *Inscripciones y Admisiones,* perteneciente a DARCA de la Universidad del Cauca. La ejecución de este control se enfoca en proporcionar a los empleados de DARCA una formación acerca e disposiciones generales y normatividad de seguridad de la información.

  Objetivo:

  - Capacitar a los empleados de DARCA acerca de aspectos generales a tener en cuenta en su puesto de trabajo para preservar la confidencialidad, integridad y disponibilidad de la información.

  Beneficios: Se fortalecerán los conocimientos del personal de DARCA para mejorar las prácticas de la seguridad de la información desde sus labores diarias y comunes.

  Alcance: Este proyecto cubre únicamente al personal que labora en DARCA (Profesional especializado).

  Fases: Este proyecto comprende las siguientes fases:

  - **Evaluación del estado actual del control:** Se analiza el estado en el que se encuentran el control A.7.2.2 en el marco del procedimiento *Inscripciones y Admisiones*.
  - **Elaboración de Capacitaciones:** Se diseñan las capacitaciones de acuerdo a la metodología NIST 800-50.
  - **Ejecución de trabajos:** Se llevan a cabo las capacitaciones.

  Cronograma: El cronograma propuesto para este proyecto es de cuatro (4) meses:

Fase	**Semana 1**				**Semana 2**				**Semana 3**				**Semana 4**			
Evaluación del estado actual	X	X														
Estructuración de procedimientos			X	X	X											
Ejecución de trabajos					X	X	X	X	X	X						
Pruebas											X	X				
Entrenamiento												X	X			
Puesta en marcha														X		
Reporte														X		

Anexo G. PROCEDIMIENTOS PARA LA REALIZACIÓN DE CAPACITACIONES Y REVISIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Universidad del Cauca	Gestión Administrativa Gestión de Admisiones, Registro y Control Académico Estrategia de Formación en Conciencia de Seguridad de la Información		
Código:	Versión:	Fecha de actualización:	Página 1 de 1

1. PROCESO/SUBPROCESO RELACIONADO:	Gestión Administrativa/Gestión de Admisiones, Registro y Control Académico
2. RESPONSABLE(S):	No aplica
3. OBJETIVO:	Planear capacitaciones periódicas de concientización en temas actuales de seguridad de la información y el uso de equipos que soportan el procedimiento de aplicación de la prueba
4. ALCANCE:	No aplica
5. MARCO NORMATIVO:	No aplica

6. CONTENIDO:

No.	Descripción de la Actividad	Cargo Responsable	Punto de Control
1	***Identificar necesidades relacionadas con la seguridad informática en DARCA.*** Es importante que tanto el *Profesional Especializado* encargado de esta actividad como todos los funcionarios de DARCA estén continuamente identificando temas relacionados con la seguridad de la información y los riesgos a los que están expuestos los equipos que soportan el proceso y que necesiten ser socializados a todo el personal de la división. Para la obtención de información relacionada con las necesidades de la división, el *Profesional Especializado* puede hacer uso de diferentes métodos como encuestas, entrevistas, análisis de incidencias, tendencias del sector informático mundial o cualquier otro método que le resulte útil para este fin.		
2	**Prepara la jornada de conciencia de la seguridad.** Una vez obtenida la información sobre las necesidades relacionadas con la seguridad de la información y los riesgos que representan los equipos que soportan el procedimiento, el *Profesional Especializado* debe: 1. Clasificar los temas teniendo en cuenta su importancia y complejidad. 2. Diseñar una encuesta que permita medir el nivel de conocimiento que tienen los funcionarios de		

	DARCA en el tema seleccionado. 3. Buscar un asesor experto en el tema para que dicte la charla.		
3	**Realizar la jornada de conciencia en seguridad dos veces a año.** 1. Realizar la introducción al tema. 2. Aplicar la encuesta. 3. Realizar la charla. 4. Aplicar nuevamente la encuesta. 5. Finalizar la charla.		
4	**Evaluación de resultados.** Una vez realizada la charla se deben tabular los datos y sacar conclusiones de la actividad y socializar los resultados obtenidos.		
5	**Monitorear temas socializados.** Es necesario que el *Profesional Especializado* genere herramientas que le permitan medir la interiorización de los temas tratados en las charlas patrocinadas por la división.		

7. FORMATOS:	No aplica
8.ABREVIATURAS Y DEFINICIONES:	

9. REGISTRO DE MODIFICACIONES:

FECHA	VERSIÒN: No	CÒDIGO	MODIFICACIONES
23-05-2017	1		Primera versión

10. ANEXOS:	No aplica

ELABORACIÒN	REVISIÒN
Nombre: Deisy Imbachi – Fabio Cerón	Nombre:
	Responsable Subproceso
Cargo: Estudiantes	Cargo:

1. PROCESO/SUBPROCESO RELACIONADO:	Gestión Administrativa/Gestión de Admisiones, Registro y Control Académico
2. RESPONSABLE(S):	Profesional especializado – División de Admisiones, Registro y Control Académico.
3. OBJETIVO:	Revisar periódicamente las estrategias de seguridad, metas y objetivos.
4. ALCANCE:	Aplica a las actividades del sub-procedimiento Evaluación de la Prueba para el Sistema de Gestión de Seguridad de la Información – SGSI de DARCA de la Universidad del Cauca, inicia con la evaluación de las estrategias de seguridad, metas y objetivos de DARCA y finaliza con su actualización o cambio de la misma.
5. MARCO NORMATIVO:	**Norma NTC-ISO-IEC 27001 de 2013.** Establece los requisitos para un Sistema de Gestión de Seguridad de la Información. **Ley estatutaria 1266 de 2008**. Establece las disposiciones del Habeas Data y regula la información en bases de datos. **Ley estatutaria 1581 de 2012**. Protección de datos personales Decreto 1377 de 2013. Protección de datos, reglamente parcialmente la ley 1581 de 2012.

6. CONTENIDO:

No.	Descripción de la Actividad	Cargo Responsable	Punto de Control
1	***Analizar los elementos que se tuvieron en cuenta para definir cada una de las estrategias tomadas.*** Antes de revisar la efectividad de una estrategia es necesario evaluar la situación actual de la División verificando que los factores que llevaron a su formulación aún están vigentes.		
2	***Medición del desempeño de la división luego de aplicar la estrategia.*** Para determinar si la estrategia planteada es efectiva es necesario realizar mediciones para comprobar que tan cerca están de las metas y los objetivos de la División. Las mediciones deben ser planeadas teniendo en cuenta la información obtenida en la evaluación del paso anterior.		

3	**Realizar acciones correctivas.** Una vez realizadas las mediciones, se debe comparar los resultados obtenidos con los resultados esperados. A continuación, se deben tomar las acciones correctivas necesarias para ajustar las estrategias de forma que estén alineadas con las metas y los objetivos de la División.		

7. FORMATOS:	
8.ABREVIATURAS Y DEFINICIONES:	

9. REGISTRO DE MODIFICACIONES:

FECHA	VERSIÓN: No	CÓDIGO	MODIFICACIONES
21-05-2017	01		Primera versión.

10. ANEXOS:	

ELABORACIÓN	REVISIÓN
Nombre: Deisy Imbachi – Fabio Cerón	Nombre:
	Responsable Subproceso
Cargo: Estudiantes	Cargo:
Fecha: 21-02-2017	Fecha: DD-MM-AA
REVISIÓN	**APROBACIÓN**
Nombre:	
Responsable Proceso	

Anexo H. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

1. PROCESO/SUBPROCESO RELACIONADO:	Gestión Administrativa/ Gestión de Admisiones, Registro y Control Académico
2. RESPONSABLE(S):	Profesional Especializado – División de Admisiones, Registro y Control Académico
3. OBJETIVO:	Establecer lineamientos que le permitan a DARCA fortalecer la cultura de seguridad de la información de sus funcionarios, contratistas y proveedores.
4. ALCANCE:	Esta política de seguridad de la información aplica para la División de Admisiones, Registro y Control Académico - DARCA, sus funcionarios, contratistas, monitores y/o cualquier usuario externo que tenga acceso a la información a través de documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la institución.
5. MARCO NORMATIVO:	**Ley 1273 de 2009.** Esta ley modifica el código penal para crear un bien jurídico tutelado – denominado "protección de la información y de los datos" y se preserva los sistemas que utilicen tecnologías de la información y las comunicaciones. **Ley estatutaria 1266 de 2008**. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones **Ley estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales, dando a las entidades públicas o privadas un plazo máximo de 6 meses para la creación de políticas internas para el manejo de datos personales. **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012. **NTC-ISO/IEC 27001.** Norma Técnica Colombiana que especifica los requisitos para establecer, documentar, implementar, operar, seguir, revisar y mantener un sistema de Gestión de la Seguridad de la Información.

6. DEFINICIONES:

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos y procedimientos de DARCA y, en consecuencia, debe ser protegido.

Credenciales de acceso: representan el usuario y la contraseña mediante los cuales se determinan los derechos de acceso al sistema de los funcionarios de DARCA.
Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
Tercero: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
Privilegios de Acceso: son los permisos asignados a un funcionario que le da acceso a cierto tipo de información.
Acuerdo de no-divulgación: acuerdo mediante el cual uno de los firmantes (El que solicita acceso a cierta información) se compromete a no divulgar de ninguna forma la información que le ha sido confiada por parte del dueño de la información.
Virus: Programa introducido subrepticiamente en la memoria de una computadora que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada. (rae)
Copias de Seguridad: es una copia de archivos originales que se guarda en un dispositivo de almacenamiento diferente al que lo contiene, el cual permite recuperar información hasta cierto nivel en caso de pérdida del archivo original.
Procedimientos de Restauración: procedimiento utilizado para restaurar archivos almacenados en una copia de seguridad que se encuentra guardada en un dispositivo externo.
Codificar: transformación de datos mediante el uso de principios, medios y métodos con el fin de ocultar el contenido la información, establecer su autenticidad, prevenir su modificación no deseada, prevenir el uso no autorizado de esta.
Integridad: es la protección de la exactitud y estado completo de los activos.

7. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La dirección de DARCA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para DARCA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de DARCA
- Garantizar la continuidad del negocio frente a incidentes.
- DARCA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen los principios de seguridad que soportan el SGSI de DARCA:

7.1. ACCESO POR PARTE DE TERCEROS

Estas políticas definen los permisos de acceso y restricciones que tendrán todas las personas que sean ajenas a DARCA.

7.1.1. DARCA controlará el acceso a su información de todo personal considerado como un tercero, de manera que los permisos de acceso asignados sean como mínimo los de un usuario interno.

7.1.2. DARCA asignará un funcionario interno que será responsable de las acciones realizadas por el personal externo a su cargo.

7.1.3. DARCA exigirá a todo personal externo la firmar un acuerdo de no-divulgación antes de obtener acceso a información interna.

7.1.4. DARCA solicitará al área legal de la Universidad del Cauca la revisión de los contratos relacionados con servicios de tecnologías de información, y en el caso de que afecten la seguridad de la información o la red interna de la Universidad deben ser aprobados adicionalmente por el área de seguridad informática.

7.2. RESPONSABILIDADES OPERACIONALES

7.2.1. Protección contra virus

Las políticas de protección contra virus informáticos, especifica los cuidados mínimos esenciales que deben tener los funcionarios para proteger la información y las estaciones de trabajo de DARCA en todo momento.

7.2.1.1. DARCA exigirá que los equipos de cómputo asignados a los funcionarios de la división estén protegidos por software antivirus con capacidad de actualización automática de su base de firmas de virus.

7.2.1.2. DARCA exigirá que todos los archivos adjuntos recibidos a través de correo electrónico, deben ser revisados por el software antivirus antes de ser manipulados.

7.2.1.3. DARCA exigirá a sus funcionarios el uso software cuyas licencias hayan sido obtenidas por la Universidad del Cauca y formen parte de su plataforma estándar.

7.2.1.4. DARCA solicitará a sus funcionarios evitar compartir directorios o archivos en red, de ser necesario, solo deben estar disponibles en modo de solo lectura.

7.2.1.5. DARCA solicitará a sus funcionarios informar al área de TIC's en caso de que uno o varios equipos de cómputo sean afectados por un virus informático.

7.2.1.6. DARCA solicitará al área de TIC's la puesta en marcha de un proceso que permita determinar el origen de la infección y evitar la propagación del virus.

7.2.2. Copias de seguridad o respaldo

Estas políticas definen la responsabilidad que tienen todos los funcionarios de DARCA con el manejo de la información de que esta su cargo.

7.2.2.1. DARCA proporcionará medios de respaldo adecuados para asegurar la información importante de cada funcionario, de manera que se pueda recuperar luego de un desastre o falla de una estación de trabajo.

7.2.2.2. DARCA considerará los siguientes aspectos para realizar las copias de respaldo:

1. El tamaño del respaldo (por ejemplo, respaldo completo o diferencial).
2. La frecuencia con la que se realizan los respaldos (dependiendo de la necesidad de la división).
3. La importancia y la criticidad de la información involucrada para la operación de la división.

7.2.2.3. DARCA garantizará que las copias de respaldo sean almacenadas en un lugar fuera de la división, de manera que no se vean afectadas en caso de desastre.

7.2.2.4. DARCA garantizará que el lugar donde se almacenan las copias de seguridad cumpla con altos niveles de protección física y ambiental.

7.2.2.5. DARCA garantizará que los medios en los que se guardan los respaldos de información sean revisados y probados periódicamente para verificar su correcto funcionamiento.

7.2.2.6. DARCA garantizará que los procedimientos de restauración sean revisados y probados periódicamente para asegurar su efectividad y puedan ser completados dentro del tiempo asignados en los procedimientos operacionales de restauración.

7.2.2.7. DARCA supervisará que los respaldos de información sean codificados antes de ser almacenados para garantizar la integridad de los datos.

7.2.2.8. DARCA entregará a sus funcionarios la responsabilidad de la creación de copias de respaldo de archivos usados, custodiados o producidos por ellos mismos.

7.2.2.9. DARCA vigilará y registrará que los funcionarios entreguen al jefe de la división las copias de seguridad para su registro y custodia.

7.2.2.10. DARCA vigilará que los procedimientos de respaldo sean automatizados, para facilitar el proceso de respaldo y restauración.

7.2.2.11. DARCA vigilará que los procesos automatizados para el respaldo de información deben ser probados suficientemente antes de su implementación.

7.3. CONTROL DE ACCESO A DATOS

Estas políticas definen como se debe manejar el control de acceso a la información que se maneja al interior de DARCA.

7.3.1. Seguridad de contraseñas

Estas políticas definen los cuidados que deben tener los funcionarios de DARCA en la creación y uso de contraseñas.

7.3.1.1. DARCA rechazará la compartición de contraseñas.

7.3.1.2. DARCA rechazará la práctica de mantener registros (en papel, archivo digital o en un dispositivo móvil) de contraseñas, a no ser que este pueda ser almacenado de manera segura y el método de almacenaje haya sido aprobado.

7.3.1.3. DARCA requerirá que se cambien las contraseñas de seguridad cuando exista sospecha o indicio de que el sistema haya sido vulnerado.

7.3.1.4. DARCA rechazará el uso de contraseñas de cuentas personales para autenticarse en cuentas institucionales o equipos de cómputo.

7.3.2. Estructura de la contraseña

Estas políticas definen las reglas que se debe seguir para construir una contraseña de seguridad.

7.3.2.1. DARCA requerirá que las contraseñas de seguridad tengan una longitud mínima de ocho (8).

7.3.2.2. DARCA requerirá que las contraseñas de seguridad mezclen caracteres alfanuméricos, caracteres especiales, letras mayúsculas y minúsculas.

7.3.2.3. DARCA requerirá que los caracteres que conforman las contraseñas de seguridad no tengan ninguna relación.

7.3.2.4. DARCA requerirá que no se usen palabras incluidas en un diccionario como contraseña de seguridad.

7.3.2.5. DARCA requerirá que no se usen identificadores de usuario (p. ej. carnet, cargo, etc.) como contraseña de seguridad.

7.3.2.6. DARCA requerirá que no se usen secuencias comunes de caracteres (p. ej. "123456789" o "QWERTY") como contraseña de seguridad.
7.3.2.7. DARCA requerirá que no se usen detalles personales (p. ej. cedula, fechas de cumpleaños, números de teléfono, etc.).

7.3.3. Vigencia

Estas políticas definen el tiempo de vida de una contraseña.

7.3.3.1. DARCA determinará el periodo mínimo de vigencia de las contraseñas, el cual es recomendable no sea menor a treinta (30) días.
7.3.3.2. DARCA requerirá que todas las contraseñas deberán expirar dentro de un periodo que no debe exceder los noventa (90) días.

7.3.4. Reutilización de contraseñas

Estas políticas establecen consideraciones que deben ser tenidas en cuenta en relación a la reutilización de contraseñas.

7.3.4.1. DARCA rechazará la reutilización de alguna de las 5 últimas contraseñas de seguridad.
7.3.4.2. DARCA rechazará la reutilización de las mismas contraseñas de seguridad en intervalos regulares de tiempo.
7.3.4.3. DARCA rechazará que los usuarios con privilegios administrativos, reutilicen alguna de las últimas 13 contraseñas de seguridad.

7.3.5. Administración de acceso a funcionarios

Estas políticas definen la frecuencia con que DARCA debe revisar los derechos de acceso de sus funcionarios.

7.3.5.1. DARCA revisará los derechos de acceso de los funcionarios cada seis (6) meses, y después de cualquier cambio, como un ascenso o terminación del contrato.
7.3.5.2. DARCA revisará y reasignará los privilegios de acceso de los funcionarios cuando se realiza un cambio de cargo al interior de la Universidad.
7.3.5.3. DARCA revisará la asignación de privilegios a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados.
7.3.5.4. DARCA registrará los cambios en las cuentas privilegiadas periódicamente.

7.3.6. Responsabilidades del funcionario

Este conjunto de políticas define las responsabilidades de los usuarios frente a las estaciones de trabajo a su cargo y la información contenida en ellos.

7.3.6.1. DARCA exigirá que los equipos de cómputo de propiedad de la Universidad del Cauca, así como los servicios compartidos, solo podrán ser usados para actividades relacionadas con el quehacer de la Universidad.
7.3.6.2. DARCA exigirá que cuando un equipo de cómputo quede desatendido el funcionario debe cerrar previamente las sesiones activas.
7.3.6.3. DARCA exigirá que en caso que el equipo de cómputo quede desatendido por un corto periodo de tiempo, el funcionario debe bloquear el equipo de manera que solicite una contraseña para poder utilizarlo nuevamente.
7.3.6.4. DARCA exigirá a los funcionarios no permitir que otra persona utilice sus credenciales de acceso para realizar una actividad.
7.3.6.5. DARCA prohibirá realizar cualquier actividad utilizando credenciales de acceso de otro usuario.
7.3.6.6. DARCA garantizará que las consecuencias de una acción realizada desde un equipo de cómputo es responsabilidad del funcionario dueño de las credenciales de acceso utilizadas en dicha acción.

7.3.7. Seguridad de computadoras

Este grupo de políticas define las acciones que deben realizar los funcionarios que tienen a cargo uno o varios equipos de cómputo.

7.3.7.1. DARCA solicitará a sus funcionarios el correcto uso del equipo de cómputo que le fue asignado, así como de los programas en él instalados.
7.3.7.2. DARCA solicitará a sus funcionarios estar atentos a cualquier cambio realizado por el personal técnico sobre su equipo de cómputo (p. ej. instalación o desinstalación de software o hardware).
7.3.7.3. DARCA implementará el uso de candados y guayas de seguridad sobre todos los equipos de la división (p. ej. monitores, torres o equipos portátiles).

7.4. Control de acceso al sistema operativo

7.4.1. Limitaciones de horario

Este conjunto de políticas establece límites en los horarios en que puede estar activa una sesión en el sistema.

7.4.1.1. DARCA solicitará a la división de TIC's que las aplicaciones críticas tendrán que estar sujetas a periodos de acceso restringidos.
7.4.1.2. DARCA solicitará a la división de TIC's que el acceso a los sistemas, en un horario distinto al horario laboral establecido por la Universidad, tendrá que estar deshabilitado o suspendido.
7.4.1.3. DARCA solicitará a la división de TIC's que en caso de ser necesario el acceso a los sistemas de la Universidad fuera del horario laboral normal, este tendrá que ser autorizado y registrado por el administrador de seguridad.

Anexo I. REGISTROS DE CAPACITACION Y COMUNICACIÓN DE LA POLITICA EN SEGURIDAD DE LA INFORMACIÓN

Universidad del Cauca

Gestión de la Calidad
Registro de asistencia a eventos Institucionales

Código: PE-GE-2.2-FOR-5 | Versión:2 | Fecha de actualización: 25-01-2016

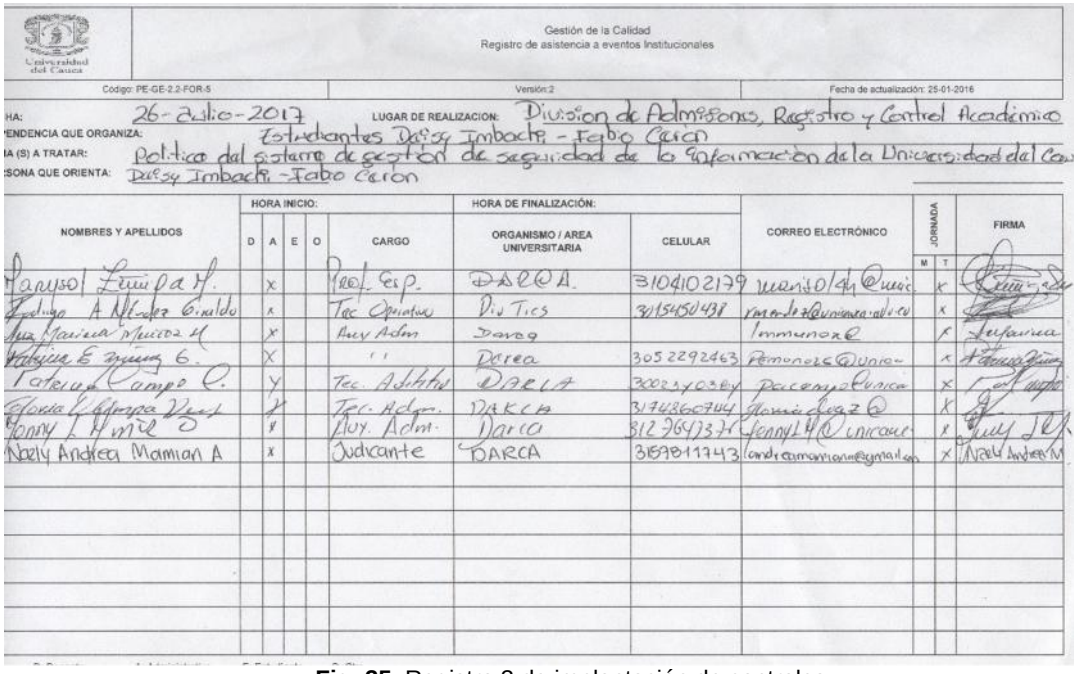
FECHA: 21-Julio-2017 LUGAR DE REALIZACION: Division de Admisiones, Registro y Control Académico
DEPENDENCIA QUE ORGANIZA: Estudiantes Deicy Dubocq y Fabio Cano
TEMA (S) A TRATAR: Politica del sistema de Gestion de seguridad de la Informacion de la Universidad
PERSONA QUE ORIENTA: Deicy Imbachi y Fabio Cano.

No.	NOMBRES Y APELLIDOS	HORA INICIO: D	A	E	O	CARGO	ORGANISMO / AREA UNIVERSITARIA	CELULAR	CORREO ELECTRÓNICO	JORNADA M	T	FIRMA
1	Guillermo Cortes Lopez		✓			Tec Administrativo	DARCA	3148860744	gcortes	✓		Guillermo Cortes
2	Gloria Vergara Diaz		✓			Tec. Hdm.	DARCA	3148860744	gloriadiaz@unicauca.edu.co	✓		
3	Silvia Constanza Zapata		✓			Sec. Ejec.	DARCA	3136672803	scmozapata@unicauca.edu.co	✓		
4	Yuri Mauricio Mendez M		✓			Aux Adm	Darca archivo		Immunoz@	✓		
5	Milton Jair Valencia		✓			Tec Adtivo	DARCA	3162657873	mjvalencia@unicauca.edu.co	✓		
6	Albeiro Perlaza Ordoñez		✓			Prof. Univ.	DARCA	3176446212	mireyaordonez@unicauca.edu.co	✓		
7	Hani A. Ponce T.		X			Tec. Operativo	" "	—	hharvi	X		
8	Ana Lucia Mera		✓			Aux Adm.	Darca	3149495801	analuciamera@unicauca.edu.co	✓		
9	Maria Isabel Torres G		✓			Secretaria	Darca	1114874115	isabeltg@unicauca.edu.co	X		
10	Mirysol Zuñiga M.		✓			Prof Depto	DARCA	3104102179	mirisol24y@unicauca.edu.co	✓		
11	Nadly Andrea Mamian A		✓			Judicante	DARCA	3157811743	andreamamiana@gmail.com	X		Nadly Andrea M
12	Paticia E. Munoz G.		✓			Asesor	Darca	3052294263 3145470655	Pemunoz@unicauca.edu.co	X		
13	Alejandra Hoyos		X			Tec. Adm.	DARCA	3204878676	cjhoyos@unicauca	X		
14	Paterina Campo		X			Tec. Admtiva	DARCA	3002340384	pacampo@unicauca.edu.co	✓		
15												
16												

Fig. 33. Registro 1 de implantación de controles

Nombre	Cargo	Correo Electrónico	Firma
Gloria Vergara Diaz	Aux. Tecn	gloria diaz.	
Maria Isabel Torres	Secretaria	isabeltg@unicauca.edu.co.	
Guillermo Cortes Lopez	Tec Adm	gcortes@unicauca.edu.co	Guillermo Cortes
Paterina Campo	Tec. Adtivo	pacampo@unicauca.edu.co	
Milton Jair Valencia	Tec Adtivo	mjvalencia@unicauca.edu.co	
Silvia Constanza Zapata	Sec. Ejec.	scmozapata@unicauca.edu.co.	
Mercedes Belalcazar	Aux Adtivo	mercedesb@unicauca.edu.co.	
Nadly Andrea Mamian	Judicante	nadyandreama@unicauca.edu.co	Nadly Andr
Yuri Mauricio Mendez	Aux Adm	Immunoz@unicauca.edu.co	
Julio C. Diago	Coord. SIMCA	jdiago@unicauca.edu.co	
Rodrigo Mendez G	Tecn Operativo	rmendez@unicauca.edu.co	
Alejandra Hoyos	Tec. Adm.	cjhoyos@unicauca.edu.co.	
Ana Lucia Mera	Aux Administrativ.	Ana Lucia@Unicauca Edu.com	
Hani Ponce T	Ter. Operativo	hharvi // hharvi	
Mireya Ordoñez	prof-univers.	mireyaordonez@unicauca.edu.co	

Fig. 34. Registro 2 de implantación de controles



Gestión de la Calidad
Registro de asistencia a eventos Institucionales

Código: PE-GE-2.2-FOR-5 | Versión:2 | Fecha de actualización: 25-01-2016

HA: 26-Julio-2017 LUGAR DE REALIZACION: División de Admisiones, Registro y Control Académico
ENDENCIA QUE ORGANIZA: Estudiantes Daisy Imbachi - Fabio Cairon
IA (S) A TRATAR: Política del sistema de gestión de seguridad de la información de la Universidad del Ca
SONA QUE ORIENTA: Daisy Imbachi - Fabio Cairon

NOMBRES Y APELLIDOS	HORA INICIO: D	A	E	O	CARGO	ORGANISMO / AREA UNIVERSITARIA	CELULAR	CORREO ELECTRÓNICO	JORNADA M	JORNADA T	FIRMA
Paulso Leiva M.		x			Prof. Esp.	DARCA.	3104102179			x	
[illegible]		x			Tec Operativo	Div Tics	3015450438			x	
[illegible]		x			Auy Adm	Darca				x	
[illegible]		x			"	Darca	3052292463			x	
Tatiana Campo C.		x			Tec. Admtiv	DARCA	3002470384			x	
[illegible]		x			Tec. Adm.	DARCA	3174366744			x	
Jenny Lizeth [illegible]		x			Auy. Adm.	Darca	3127643776			x	
Nelly Andrea Mamian A		x			Judicante	DARCA	3169811743			x	

Fig. 35. Registro 3 de implantación de controles

Anexo J. PROCESOS Y PROCEDIMIENTOS RELATIVOS AL SGSI

Universidad del Cauca	Gestión Administrativa Gestión de Admisiones, Registro y Control Académico Procedimiento de Auditoría Interna		
Código:	Versión: 0	Fecha de Actualización: 28-07-2017	Página 1 de 1

1. PROCESO/SUBPROCESO RELACIONADO:	Gestión Administrativa/Gestión de Admisiones, Registro y Control Académico
2. RESPONSABLE(S):	Profesional especializado – División de Admisiones, Registro y Control Académico.
3. OBJETIVO:	El objetivo de este procedimiento es describir todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.
4. ALCANCE:	Este procedimiento se aplica a todas las actividades implementadas dentro del Sistema de Gestión de Seguridad de la Información – SGSI.
5. MARCO NORMATIVO:	**Norma NTC-ISO-IEC 27001 de 2013.** Establece los requisitos para un Sistema de Gestión de Seguridad de la Información. **Norma ISO-IEC 27006.** Establece los requisitos para la realización de auditorías.

6. CONTENIDO

6.1. PRINCIPIOS DE AUDITORÍA

Los principios de una auditoría representan la base sobre la que se desarrolla la misma, la cual entrega resultados confiables, objetivos, pertinentes y suficientes para que DARCA pueda tomar decisiones en base a dichos resultados.

A continuación, se presentan los principios que serán tenidos en cuenta para el desarrollo de una auditoría:

- **Presentación ecuánime:** Los resultados expuestos por la auditoria (conclusiones, informes y hallazgos) deben mostrar la veracidad y exactitud de la información presentada durante la auditoria.
- **Enfoque basado en la evidencia:** El proceso de auditoria es una actividad sistemática, que se basada en la toma de muestras de la información en un tiempo dado establecido para dicha auditoria. Toda muestra debe permitir verificar la fiabilidad de la auditoria.
- **Independencia:** Las tareas del auditor deben gozar de total libertad e independencia, y debe estar libre de cualquier conflicto de intereses e intervenciones externas. La independencia es la base de la objetividad e imparcialidad del resultado de la auditoría, es así como ésta puede mantenerse objetiva durante todo el proceso.
- **Confidencialidad:** Se debe garantizar la seguridad de la información durante todo el proceso de la auditoría de tal manera que la información manejada durante dicho proceso no sea utilizada de manera inapropiada.