Resultados del diagnóstico de Seguridad de la información basado en el anexo A de la norma estándar ISO 27001:2013 y ley 1581 de 2012 de protección de datos personales y cumplimiento legal de GEL/ Gobierno en línea.

UNIVERSIDAD DEL QUINDÍO

Elaborado por:	Revisado por:	Aprobado por:
José E. García Castro	**Martha C. Sánchez**	**John E. Martínez García**
Consultor	Gerente del Proyecto	Consultor Senior

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
0.0	27/09/2017	Emitido para aprobación
1.0	29/09/2017	Revisado
2.0	30/09/2017	Aprobado

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 DECLARACION DE CONFIDENCIALIDAD

La información contenida en este documento es de carácter confidencial y sólo puede ser utilizada por la *Universidad del Quindío* para los fines que estime pertinentes en marco del Proyecto "*CONSULTORIA: Diagnóstico para seguridad y privacidad de la información bajo cumplimiento GEL / Gobierno en Línea",* cualquier retención, difusión, distribución o copia de este documento sin la autorización del propietario, es prohibida y sancionada por la ley.

2 LIDER PROYECTO UNIVERSIDAD DEL QUINDIO

EL proyecto de diagnóstico fue liderado por el Ing. *Reinaldo Sierra Prieto* y su equipo de trabajo de la Oficina Asesora de Planeación y Desarrollo.

3 INTRODUCCIÓN

Conforme los lineamientos establecidos en marco de la Estrategia de Gobierno en línea en Colombia, plasmada en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015 y que comprende cuatro grandes propósitos entre los cuales esta garantizar ***la seguridad y la privacidad de la información***, se generó un diagnostico con el fin de determinar el grado de madurez actual de la gestión de seguridad y privacidad de la información al interior de la *Universidad del Quindío*.

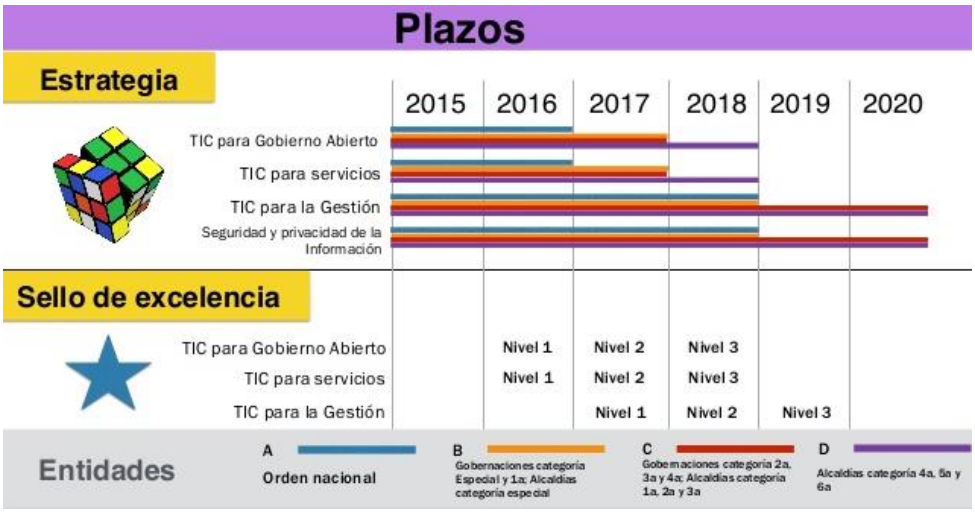


Ilustración 1. Plazos Estrategias GEL. Tomado de: http://estrategia.gobiernoenlinea.gov.co.

COMPONENTE	LOGROS TIC PARA GOBIERNO ABIERTO
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	DEFINICIÓN DEL MARCO DE SEG. Y PRIV.
	IMPLEMENTACIÓN DEL PLAN DE SEG. Y PRIV.
	MONITOREO Y MEJORAMIENTO CONTINUO

Tabla 1. Logros del Componente Seguridad y Privacidad de la Información.

4 OBJETIVO

Informe de resultados del diagnóstico de Seguridad de la información basado en el anexo A de la norma estándar ISO 27001:2013 y ley 1581 de 2012 de protección de datos personales y cumplimiento legal de GEL/ Gobierno en línea.

5 ALCANCE.

De acuerdo al diagnóstico elaborado con los macroprocesos determinados en el Plan de Proyecto presentado a la *Universidad del Quindío*, el informe cubre los siguientes aspectos:

a. Resultados del Diagnóstico de Seguridad de la Información con base en el Anexo A de la Norma estándar ISO27001:2013.
b. Resultados del Diagnóstico de Cumplimiento de la Ley de protección de datos personales Ley 1581 de 2012 - LEPD.
c. Nivel de Cumplimiento de componente seguridad y privacidad de la información de la estrategia Gobierno en Línea – GEL.
d. Hoja de Ruta.

Los documentos definición de la política y objetivos de Seguridad de la información y la definición del alcance del Modelo de seguridad de la información, se entregaran en documento aparte a este informe.

Macroprocesos Entrevistados:

MACROPROCESO
PLANEACION ESTRATEGICA. | GESTIÓN Y ASEGURAMIENTO DE LA CALIDAD
GESTION TICS

GESTION HUMANA
COMUNICACIONES ESTRATEGICA
CONTROL INTERNO
GESTION DOCUMENTAL
ADMINISTRACIÓN DEL CAMPUS
GESTION DE BIENESTAR INSTITUCIONAL
GESTION JURIDICA
GESTION DE APOYO ACADEMICO

Tabla 2.Información macroprocesos de la Universidad del Quindío.

6 DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN EL ANEXO A DE LA NORMA ESTÁNDAR NTC-ISO/IEC 27001:2013.

A continuación se presenta el resultado del diagnóstico del Sistema de Gestión de Seguridad de la Información bajo la norma NTC-ISO/IEC 27001:2013 y el nivel de madurez del mismo respecto a la norma, teniendo en cuenta los requerimientos/cláusulas obligatorias de la norma como los controles del anexo A.

Se revisan todos los requisitos de la norma NTC-ISO/IEC 27001:2013 listados a continuación:

- Contexto de la organización (Numeral 4 en la norma)
- Liderazgo (Numeral 5 en la norma)
- Planificación (Numeral 6 en la norma)
- Soporte (Numeral 7 en la norma)
- Operación (Numeral 8 en la norma)
- Evaluación de desempeño (Numeral 9 en la norma)
- Mejora (Numeral 10 en la norma)

Se revisan todos los Dominios de Control Anexo A de la norma NTC-ISO/IEC 27001:2013 listados a continuación:

- Políticas de Seguridad de la Información
- Organización de la Seguridad de la Información.
- Seguridad de los Recursos Humanos
- Gestión de Activos
- Control de Acceso
- Criptografía
- Seguridad Física y del Entorno.
- Seguridad de las Operaciones

- Seguridad de las Comunicaciones
- Adquisición, Desarrollo y Mantenimiento de Sistemas
- Relaciones con los Proveedores
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio
- Cumplimiento

6.1 METODOLOGÍA

Para la evaluación de los requisitos del SGSI y los controles del anexo A de la norma ISO 27001:2013, se diligencio una lista de chequeo, en donde se analiza y evalúa su nivel de madurez.

La lista de chequeo está conformada por diez columnas que permiten comparar lo requerido por la norma con lo establecido actualmente en la Universidad del Quindío. Las columnas indican los siguientes aspectos:

- **Ítem:** Contiene la numeración de los requisitos del SGSI y el Anexo A de la norma NTC-ISO/IEC 27001:2013.
- **Requisitos del SGSI y Controles del Anexo A:** Requisitos y controles del Anexo A de la norma NTC-ISO/IEC 27001:2013 a evaluar.
- **RE:** Es la respuesta que se obtiene durante la entrevista y/o revisión documental. Las respuestas pueden ser SI, NO, NA y PA, que se explican a continuación.
- **SI:** Se selecciona de forma automática en caso de que en la casilla de “RE” la respuesta sea “si”. Hace referencia a que el control está implementado según lo exigido por la norma.
- **NO:** Se selecciona de forma automática en caso de que en la casilla de “RE” la respuesta sea “no”. Hace referencia a que el control no está implementado.
- **NA:** Se selecciona de forma automática en caso de que en la casilla de “RE” la respuesta sea “na”. Hace referencia a que el control no aplica debido a su exclusión en la declaración de aplicabilidad.
- **PA:** Se selecciona de forma automática en caso de que en la casilla de “RE” la respuesta sea “pa”. Hace referencia a que el control está implementado según lo exigido por la norma, pero de forma parcial.
- **Cumplimiento control:** Consolida el porcentaje de cumplimiento de los numerales por requisito/cláusula/dominio y objetivo de control respectivamente.

- **Justificación:** Contiene la explicación del cumplimiento al requisito/cláusula/dominio de la norma.

Para la observación del nivel de madurez obtenido se utiliza la tabla No. 1 la cual describe y establece los correspondientes rangos de calificación:

Diagnóstico bajo la Norma NTC-ISO/IEC 27001:2013		
NIVEL DE MADUREZ	LIMITE INFERIOR	LIMITE SUPERIOR
Optimizado	91%	100%
Administrado	71%	90%
Definido	61%	70%
Repetible	41%	60%
Inicial	16%	40%
Inexistente	0%	15%

Tabla 3. Diagnóstico y Niveles de madurez

Definición de los Niveles de Madurez:

Nivel 0 - No Existente: Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

Nivel 1 - Inicial: Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

Nivel 2 - Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

Nivel 3 - Definido: Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida

utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

Nivel 4 - Administrado: Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se llega a utilizar la automatización y herramientas de una manera limitada o fragmentada.

Nivel 5 - Optimizado: Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

6.2 RESULTADOS DEL DIAGNOSTICO REQUISITOS DE LA NORMA ISO 27001:2013

Se presenta a continuación el resultado del diagnóstico realizado a los requisitos de la norma ISO/IEC 27001:2013 conforme la información recolectada en las entrevistas realizadas. En la tabla No. 4 se muestra por cada categoría de requisitos de la norma, el porcentaje y el nivel de madurez que presenta. La información detallada se puede ver en el "ANEXO A - Matriz del resultado diagnóstico requisitos de la norma ISO/IEC 27001:2013".

Ítem	Aspectos del SGSI	Cláusulas	Meta	Promedio Cláusulas	Nivel de madurez Cláusulas
4..	Contexto de la Organización	21%	100%	31%	Inicial
5..	Liderazgo	3%	100%	2%	Inexistente
6..	Planificación	25%	100%	25%	Inicial
7..	Soporte	29%	100%	18%	Inicial
8..	Operación	33%	100%	33%	Inicial
9..	Evaluación del Desempeño	25%	100%	24%	Inicial
10..	Mejora	45%	100%	48%	Repetible
	TOTAL	25%	100%	26%	Inicial

Tabla 4. Resultado de los requisitos de la norma NTC-ISO/IEC 27001:2013

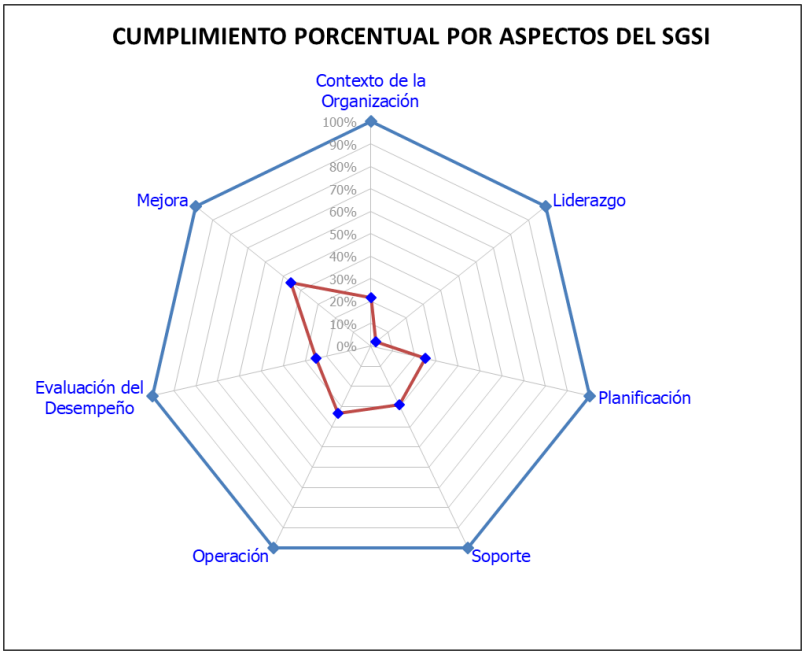


Imagen 1. Radar resultado de los requisitos de la norma NTC-ISO/IEC 27001:2013

De acuerdo con el diagnostico realizado, se consultaron ciento dieciséis requerimientos/cláusulas obligatorias de la norma, observando que el porcentaje del nivel de madurez del SGSI respecto a los requisitos de la norma es del 25%, correspondiente a un nivel de Madurez “Inicial”. Lo anterior indica que en la Universidad del Quindío, ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no se observan si existen procesos estándar desde la norma ISO 27001:2013 en su lugar se observa que existen enfoques desde el proceso de Gestión de Calidad y otros que tienden a ser aplicados de forma individual o caso por caso.

Aunque se reconoce la importancia del Sistema de Gestión de Seguridad de la Información, aún no se observa si se han desarrollado y documentado algunas actividades y/o procesos alrededor de la misma y otras actividades enmarcadas en el aspecto de implementación de un SGSI determinados en la “implementación de un sistema de gestión de seguridad de la información (SGSI), etapa planear, basados en el manual 3.1 gobierno en línea” no se observó apropiación o seguimiento de la misma, igualmente no se observa si se han realizado actividades para la integración al Sistema Integrado de Gestión desde el macroproceso de Gestión de TICs.

6.2.1 Resumen del Nivel de Madurez y Oportunidades de Mejora en Requisitos de la Norma ISO 27001:2013

Requisitos con el nivel de Madurez "Inicial"

a. Contexto de la Organización: Entre los aspectos más relevantes del GAP tenemos:

- Con respecto al conocimiento de la Organización y su contexto, se conoció que se cuenta con los contextos para los macroprocesos de la organización.

- Con respecto a las partes interesadas que son pertinentes al SGSI, se conoció que las partes interesadas no se han definido, ni sus requisitos.

- Al momento del Diagnóstico, no se observa si se ha definido el alcance del SGSI de manera documental, indicando las ciudades, las sedes, los límites del SGSI.

b. Planificación: Con respecto a las acciones para tratar riesgos y Oportunidades, se conoció:

- No se observa un Manual de Gestión de Riesgos del área de CENTRO DE SISTEMAS Y NUEVAS TECNOLOGÍAS – CSNT, el enfoque de riesgos del área, está dado en dar respuesta a riesgos del PLAN DE CONTINGENCIA INFORMARTICO DEL AÑO 2010.

- No se observa la existencia de la declaración de aplicabilidad.

- No se observa documento de Indicadores de Seguridad de la Información.

- No se observa un Plan Estratégico de Tecnologías de la Información alineado al Plan de Desarrollo Institucional (PDI) 2016 - 2025 "Por una Universidad del Quindío Pertinente, Creativa, Integrador. Con el cual buscan fortalecer la infraestructura tecnológica del campus universitario en cuanto a la adquisición y reposición de equipos de cómputo y audiovisuales, bases de datos y software, y sistema de seguridad integrado."

- No se observa manejo de los riesgos de Seguridad de la información asociados con la perdida de Confidencialidad, Integridad y Disponibilidad de información dentro del alcance del macroproceso de Gestión de TICs. Esto se observó en el macroproceso de Gestión Documental.

c. Soporte: Entre los aspectos más relevantes del GAP tenemos:

- Con respecto a determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI, se conoció que el Macroprocesos de Gestión Estratégica, está realizando el diagnostico de cumplimiento a la norma ISO 27001:2013, en el que se observara el GAP de cumplimiento y se generará una hoja de ruta que permita trazar un plan para la implementación de un MSPI.

- Con respecto a la toma de conciencia, se conoció que se han realizado charlas de sensibilización en materia de protección de datos personales.

d. Operación: Entre los aspectos más relevantes del GAP tenemos:

- Con respecto a la valoración de Riesgos de la Seguridad de la Información, se conoció una matriz de riesgos, No se observa si se les realiza el seguimiento a los riesgos y actualmente se observa que esta desactualizada.

e. Evaluación del Desempeño: Entre los aspectos más relevantes del GAP tenemos:

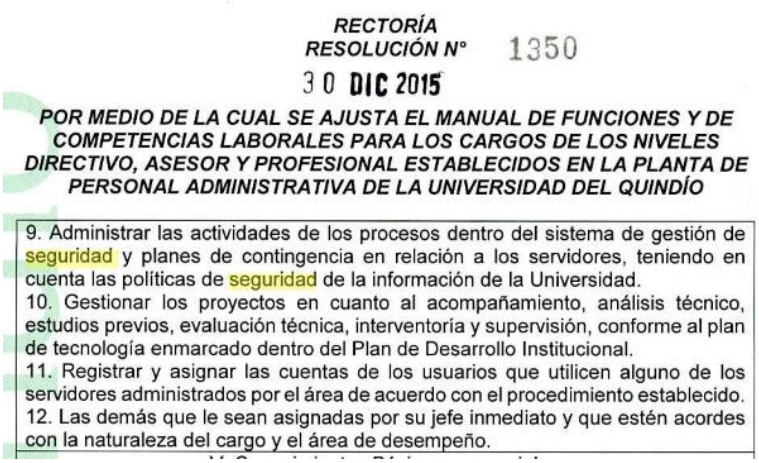
- Con respecto al seguimiento, medición, análisis y evaluación, se conoció que no se cuenta con la matriz de objetivos e indicadores, no se ha realizado la valoración de la eficacia de los controles, no se han definido programa de auditoría interna para el SGSI propiamente dicho y no se ha realizado la revisión por la dirección.

Requisitos con el nivel de Madurez “Inexistentes”

f. Liderazgo: Entre los aspectos más relevantes del GAP tenemos.

- No se observa un Manual del MSPI del CENTRO DE SISTEMAS Y NUEVAS TECNOLOGÍAS - CSNT, se observan documentos como el PLAN DE SEGURIDAD DE LA INFORMACIÓN 2010 – 2015 y un Borrador de Políticas de Seguridad de la Información, los cuales en el diagnostico no se observó que estos se hubieran difundido o publicado para las partes interesadas de la Universidad del Quindío.

- En resolución de rectoría, 1350 de diciembre 30 de 2015, se establecieron las funciones en tema del sistema de gestión de seguridad de la información al profesional especializado 2028 grado 18, como se observa en la siguiente imagen:



RECTORÍA
RESOLUCIÓN N° 1350
30 DIC 2015

POR MEDIO DE LA CUAL SE AJUSTA EL MANUAL DE FUNCIONES Y DE COMPETENCIAS LABORALES PARA LOS CARGOS DE LOS NIVELES DIRECTIVO, ASESOR Y PROFESIONAL ESTABLECIDOS EN LA PLANTA DE PERSONAL ADMINISTRATIVA DE LA UNIVERSIDAD DEL QUINDÍO

9. Administrar las actividades de los procesos dentro del sistema de gestión de seguridad y planes de contingencia en relación a los servidores, teniendo en cuenta las políticas de seguridad de la información de la Universidad.
10. Gestionar los proyectos en cuanto al acompañamiento, análisis técnico, estudios previos, evaluación técnica, interventoría y supervisión, conforme al plan de tecnología enmarcado dentro del Plan de Desarrollo Institucional.
11. Registrar y asignar las cuentas de los usuarios que utilicen alguno de los servidores administrados por el área de acuerdo con el procedimiento establecido.
12. Las demás que le sean asignadas por su jefe inmediato y que estén acordes con la naturaleza del cargo y el área de desempeño.

Imagen 2. Asignación funciones administración del sistema de gestión de seguridad.

Requisitos con el nivel de Madurez "Repetible"

a. Mejora: Entre los aspectos más relevantes del GAP tenemos:

- Con respecto a las no conformidades y acciones correctivas, se conoció que se han realizado auditoría al Macroproceso de Gestión de TICs y están documentadas y planeadas

6.3 *RESULTADOS DEL DIAGNOSTICO ANEXO A DE LA NORMA NTC-ISO/IEC 27001:2013*

Se presenta a continuación el resultado del diagnóstico de los controles definidos en el anexo A de la norma NTC-ISO/IEC 27001:2013. El porcentaje y nivel de madurez de cada uno se presenta en la tabla No. 5. La información detallada se puede ver en el "ANEXO A - Matriz del resultado diagnóstico requisitos de la norma NTC-ISO/IEC 27001:2013".

Ítem	Dominios	Controles	Meta	Objetivos de control	Nivel de madurez Dominios
A.5..	Política de Seguridad de la Información	25%	100%	25%	Inicial
A.6..	Organización de la Seguridad de la Información	57%	100%	48%	Repetible
A.7..	Seguridad en los Recursos Humanos	50%	100%	53%	Repetible
A.8..	Gestión de los activos	35%	100%	29%	Inicial
A.9..	Control de Acceso	46%	100%	38%	Inicial
A.10..	Criptografía	50%	100%	50%	Repetible
A.11..	Seguridad Física y del Entorno	30%	100%	32%	Inicial
A.12..	Seguridad de las Operaciones	50%	100%	63%	Definido
A.13..	Seguridad de las Comunicaciones	57%	100%	63%	Definido
A.14..	Adquisición, Desarrollo y Mantenimiento de Sistemas	73%	100%	52%	Repetible
A.15..	Relaciones con los Proveedores	50%	100%	50%	Repetible
A.16..	Gestión de incidentes de Seguridad de la Información	36%	100%	36%	Inicial
A.17..	Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio	25%	100%	33%	Inicial
A.18..	Cumplimiento	50%	100%	43%	Repetible
	TOTAL	47%	100%	44%	Repetible

Tabla 5. Resultados Diagnostico Controles Anexo A DE LA NORMA NTC-ISO/IEC 27001:2013.

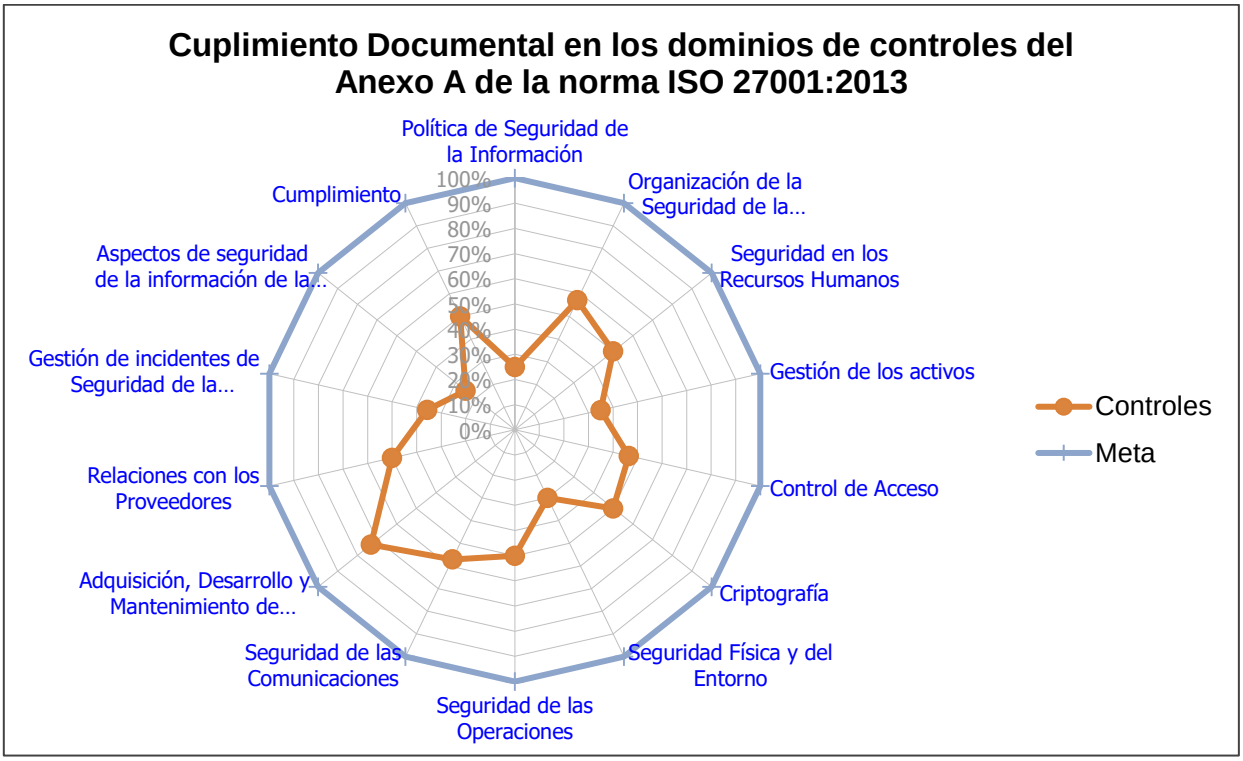


Imagen 3. Radar resultado de los controles del Anexo A de la norma NTC-ISO/IEC 27001:2013

De acuerdo el diagnostico realizado, se consultaron ciento catorce controles del Anexo A de la norma ISO27001:2013, observando que el porcentaje de madurez del SGSI respecto a los controles del Anexo A es del 44%, correspondiente a un nivel de Madurez “Repetible”. Lo anterior indica que en la Universidad del Quindío, en marco de los controles de Seguridad de la Información, se desarrollan actividades y/o procesos, sin embargo no se observa si han sido documentadas, ni se observa si hay entrenamiento o comunicación formal de la misma. Se observa que se deja la responsabilidad al funcionario.

6.3.1 Resumen del nivel de cumplimiento y de oportunidades de mejora en el Anexo A de la NORMA NTC-ISO/IEC 27001:2013

Requisitos con el nivel de Madurez “Inicial”.

a. **Política de Seguridad de la Información:** Entre los aspectos más relevantes del GAP tenemos:

- Que se observa la existencia de Políticas de Seguridad de la Información, pero están en borrador, no se observa revisión ni seguimiento.

b. **Gestión de los activos:** Entre los aspectos más relevantes del GAP tenemos.

- Con respecto al listado documentado de activos de información donde se identifiquen los responsables, se conoció que se encuentran para el macroproceso de Gestión Documental, para los activos de información hardware, software del macroproceso de Gestión de TICs, no se conoció el procedimiento, en el listado conocido, no se observan criterios de Integridad y Disponibilidad.

c. Control de Acceso: Entre los aspectos más relevantes del GAP tenemos.

- Con respecto al registro de usuarios y cancelación del registro de usuarios, se conoció que se tiene definido pero no se encontró documentado.

- Con respecto a la gestión de derechos de acceso privilegiado, se conoció que el macroproceso de Gestión de TICs hace uso de cuentas de usuarios con altos privilegios, se conoció que las cuentas privilegiadas de los sistemas tercerizados no se controlan. Se conoció que se tienen usuarios de red con cuentas de administrador en los equipos.

- Con respecto a la gestión de información de autenticación secreta de usuarios, se conoció que durante los procedimientos de creación de usuarios los sistemas de información tienen la opción de exigir el cambio de Password.

- Con respecto a la revisión de los derechos de acceso de usuarios, se conoció que existe el procedimiento, sin embargo la revisión no la ejecutan los propietarios de los activos.

- Con respecto al retiro o ajuste de los derechos de acceso, se conoció que en él se especifican los controles para el ajuste o retiro del usuario.

- Con respecto a sistema de gestión de contraseñas, durante las indagaciones, se conoció que en algunos sistemas de información no manejan complejidad en el uso de contraseñas. Se recomienda realizar una validación del cumplimiento para todos los sistemas de información del alcance del SGSI.

- Con respecto al uso de programas utilitarios privilegiados, se conoció que en las Políticas se tiene definido el no uso de los utilitarios privilegiados, sin embargo se observan que hay usuarios que hacen uso de ellos y no se observa si se tienen claramente documentados.

d. **Seguridad Física y del Entorno:** Entre los aspectos más relevantes del GAP tenemos.

- Con respecto al perímetro de seguridad física, se conoció que está se garantiza mediante un Firewall.se realiza el monitoreo de las conexiones.

- Con respecto al trabajo en áreas seguras, se conoció que aunque en algunos procesos se tienen definidos procedimientos para la realización de trabajos, no se han observado algunas áreas que podrían ser parte del perímetro de seguridad física.

- Con respecto a disposición segura o reutilización de equipos, no se observaron procesos para el borrado seguro.

- No se observaron políticas de ubicación y protección de equipos. No se observa si se informa a contratistas.

- No se observó la política para retiro e ingreso de activos, seguridad de equipos y activos fuera de las instalaciones, disposición segura o reutilización de equipos, equipos de usuarios desatendido y una política de escritorio limpio y pantalla limpia. Se observa un protocolo de atención al público con recomendaciones sobre escritorios de funcionarios que atienden público.

- Se observó vulnerabilidad en los controles de acceso a las instalaciones en general.

e. **Gestión de incidentes de Seguridad de la Información:** Entre los aspectos más relevantes del GAP tenemos.

-
- No se Observaron los controles para la recolección de las evidencias.

- Se observa que el proceso manejan incidentes relacionados con activos fijos.

- Se observa procedimiento, falta control y seguimiento.

f. **Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio:** Entre los aspectos más relevantes del GAP tenemos.

- Con respecto a la continuación de la seguridad de la información, si se ha incluido dentro del PCN o el PRD, se conoció que se está en proceso de observar las brechas del cumplimiento de los planes de seguridad, no se conocen planes de continuidad para los sistemas de información.

Requisitos con el nivel de Madurez "Repetible".

a. Organización de la Seguridad de la Información: Entre los aspectos más relevantes del GAP tenemos.

- Se observan los roles, responsabilidad y autoridad a cumplir en el SGSI en el manual de funciones para el jefe del Macroproceso de Gestion de TICs, se tiene definido seguridad en resolución de rectoría sobre ética y buen gobierno.

- Con respecto a contacto con las autoridades y con grupos de interés especial, se conoció que se requiere realizar la revisión del documento del directorio de los contactos con las autoridades y grupos de interés para validar su actualización.

b. Seguridad en los Recursos Humanos: Entre los aspectos más relevantes del GAP tenemos.

- No se observó que en los acuerdos contractuales se incluyen, acuerdos de confidencialidad, derechos de autor, entre otros y las sanciones a tomar en caso de incumplimiento para los empleados. No se observa si se tienen para los empleados temporales (Contrato en misión) o que prestan servicios por medio de un proveedor.

- Con respecto a la difusión de los roles y responsabilidades en cuanto a la seguridad de la información hacia el personal, se conoció que en el contrato de trabajo se indican los deberes del colaborador en las cláusulas de referencia de seguridad de la información.

c. Criptografía: Entre los aspectos más relevantes del GAP tenemos.

- Con respecto a la gestión de llaves criptográficas, se conoció que los sistemas de Información y la aplicación de https://ecotic.uniquindio.edu.co/ecotic/#/home, https://sac.uniquindio.edu.co/sgasinu/inscripciones.jsp#home, tienen implementado el protocolo de transferencia seguro HTTPS. Adicionalmente, se conoció que se debe revisar el cumplimiento para la protección de los equipos y los otros servicios considerando la clasificación de la información. No se observa seguimiento sobre la validez de los certificados o vencimientos.

Imagen 4. Verificación certificado SSL.

- Se observan canales VPN para conexiones remotas y se hace control. No se observa si el proceso esta documentado.

d. **Adquisición, Desarrollo y Mantenimiento de Sistemas:** Entre los aspectos más relevantes del GAP tenemos:

- Con respecto al análisis y especificación de los requisitos de seguridad de la información, se conoció que se tiene un procedimiento de “Desarrollo y Mantenimiento de Sistemas de Información”.

- Con respecto a la seguridad en los proceso de desarrollo y soporte, se conoció que los procedimientos de desarrollo, cuentan con buenas prácticas en desarrollo seguro de software.

- Con respecto al procedimiento de contratación para desarrollo de software contratado externamente, se conoció que se cuenta con el procedimiento informal para controlar los desarrollos externos.

- Con respecto a las pruebas de seguridad y de aceptación de sistemas, se conoció que se cuenta con el procedimiento “Desarrollo y Mantenimiento de Sistemas de Información” que define aspectos de desarrollo y pruebas de aceptación de desarrollos externos. Sin embargo, no se observa si se especifican los aspectos de las pruebas relacionadas con la seguridad de la información.

e. Relaciones con los Proveedores: Entre los aspectos más relevantes del GAP tenemos.

- Con respecto al seguimiento y revisión de los servicios de los proveedores, se conoció que se realiza, no se observa acciones de seguridad de la información.

- Se observa que se tienen acuerdos de confidencialidad con los proveedores, no se observa si están documentados o establecidos por procedimiento del Sistema de Seguridad de la Información.

- Con respecto a la Gestión de cambios en los servicios de los proveedores, no se observa que se incluyan los aspectos de los cambios organizacionales, del servicio y de los ANS.

f. Cumplimiento: Entre los aspectos más relevantes del GAP tenemos.

- Con respecto a la observación de la legislación aplicable y de los requisitos contractuales, se conoció que se manejan los aspectos legales a través del Normograma.

Requisitos con el nivel de Madurez “Definido”.

a. Seguridad de las Operaciones: Entre los aspectos más relevantes del GAP tenemos.

- Con respecto a Gestión de Cambios, No se observa la existencia del comité de Arquitectura de TI y Empresarial que integre la Tecnología con la Arquitectura Empresarial; no se observa la existencia de estos comités.

- Con respeto a la Gestión de capacidad, se conoció que no se cuenta con el proceso de Gestión de la Capacidad.

- Con respecto a respaldo de la información, se conoció que se debe revisar si los procesos del alcance tienen este servicio. Adicionalmente, No se observa que se realizan pruebas de restauración en las backup.

- Con respecto a registro de eventos y la protección de la información del registro, se conoció que no se cuenta con el software que permita registrar los eventos relacionados con la seguridad de la información diferente al firewall y se custodie las evidencias.

b. Seguridad de las Comunicaciones: Entre los aspectos más relevantes del GAP tenemos.

- Con respecto a la seguridad de los servicios de red, se conoció que los canales del servicio para los macroprocesos se encuentran cifrados.

- Con respecto a la mensajería electrónica, se conoció que se cuenta con el servicio de correo de Gmail.

- Se conoció que se cuentan con controles de red que garantizan la seguridad de los servicios y de la información (Firewall, proxys) y se realiza segmentación de redes mediante Vlans y se manejan Registros de estas.

*6.4 **CONCLUSIONES DIAGNOSTICO CONTROLES ISO 27001:2013.***

✓ De acuerdo con el Diagnostico, se puede observar que el enfoque de seguridad de la información de la Universidad del Quindío está en los controles técnicos y se observan debilidades en los controles Administrativos para el cumplimiento del Sistema de Gestión de Seguridad y Privacidad de la Información (MSPI).

- ✓ Con respecto a los controles técnicos, se observan debilidades en los dominios de las Política de Seguridad de la Información, Gestión de Activos, Controles de Acceso, Seguridad Física, Gestión de Incidentes y Gestión de Continuidad de Negocio, con oportunidades de mejora para fortalecer los procesos existentes.

- ✓ Se deben fortalecer y documentar desde la perspectiva de seguridad de la información los dominios de Organización de la Seguridad de la Información, Seguridad en los Recursos Humanos, Criptografía, Adquisición, Desarrollo y Mantenimiento de Sistemas, Relaciones con los Proveedores y Cumplimiento.

- ✓ Se deben administrar los dominios de Seguridad de las Operaciones y Seguridad de las Comunicaciones, con el fin de ir ajustándolos a un Sistema de Gestión de Seguridad de la Información.

- ✓ Con respeto a los requisitos para el Sistema de Gestión de Seguridad de la Información, se observan importantes iniciativas de respaldo al proceso del MSPI por parte de la Alta Dirección y adecuados procesos para tratar riesgos.

6.4.1 Fortalezas, Oportunidades de mejora y Recomendaciones generales

a.Fortalezas

- ✓ El compromiso del personal de los macroprocesos de Planeación estratégica, Gestión TICs y de Gestión Calidad quienes tienen el compromiso de la alta dirección en el cumplimiento de los requerimientos de Ley en cuanto a Seguridad y Privacidad de la información.

- ✓ La experiencia en la implementación, mantenimiento y mejora de la Universidad del Quindío, en Sistemas de Gestión de la Calidad y Modelo Estándar de Control Interno.

- ✓ La experiencia en gestión documental por parte del personal líder de la Institución.

- ✓ El compromiso de las personas en atender los lineamientos de la alta dirección.

b. Oportunidades de mejora

- ✓ Aumentar la dedicación de tiempo por parte del personal con conocimientos y responsabilidad para desarrollar adecuadamente el MSPI.

- ✓ Comunicar a la Alta dirección (Consejo Superior, Rectoría, Vicerrectores) de la institución las actividades marco en Seguridad y Privacidad de la Información, con el fin de que se logren:

    - Aprobar la política y objetivos de seguridad de la información.
    - Establecer roles y responsabilidades de seguridad de la información.

- Comunicar tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas desde la perspectiva del MSPI
- Realizar revisiones del MSPI.

✓ Participación amplia y continua de los líderes de procesos según el alcance del MSPI.

✓ Comprender en detalle el proceso de planeación e implementación de un MSPI. Adquirir experiencia desde el Sistema de Gestión de Calidad ISO9001, NTGCP1000 y MECI, asistir a cursos de formación y continuar con asesoramiento de consultores externos especializados.

c.Recomendaciones generales

✓ Gestionar el proyecto de implementación del MSPI bajo la norma ISO 27001:2013, lineamientos de GEL y Ley 1581 de 2012, fijando los diferentes hitos en la implementación de un MSPI, con sus objetivos y resultados. Igualmente definir las necesidades de recursos y presentar a la Alta Dirección para aprobación.

✓ Con base en el diagnóstico, establecer el Sistema de Gestión de Seguridad y Privacidad de la Información para todos los procesos, según un alcance definido, y así dar cumplimiento al Decreto Nacional 2573 de 2014[1] y al Manual de Gobierno en línea versión 3.1 en lo que respecta al MSPI.

✓ Solicitar a la Dirección apoyo para liberar horas de un funcionario que ejerza como coordinador del MSPI.

[1] DECRETO 2573 DE 2014 (diciembre 12): Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- ✓ Concientizar y formar al personal. La dirección debe asegurar que todo el personal relevante de la institución y en especial los líderes de procesos, esté consciente de la importancia de sus actividades de seguridad y privacidad de la información y de cómo contribuye a la consecución de los objetivos de MSPI.

- ✓ Complementar la gestión de riesgos según el alcance definido para el MSPI.

- ✓ Definir y/o modificar los procedimientos y controles que afecten a la seguridad de la información.

- ✓ Definir el Comité de Seguridad de la información o incluir las responsabilidades del mismo en otro comité ya existente, preferiblemente en donde participe la Dirección de la institución.

- ✓ Formalizar el sistema de gestión de incidentes que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).

- ✓ No reinventar la rueda: apoyarse lo más posible en estándares, métodos y guías ya establecidos, así como en la experiencia de otras organizaciones.

- ✓ Servirse de lo ya implementado en los otros sistemas de gestión o modelos como ISO 9001, NTCGP1000, MECI, para el MSPI.

- ✓ Reservar la dedicación necesaria diaria o semanal: el personal involucrado debe trabajar con continuidad en el mismo.

- ✓ Es importante adelantar labores de revisión y ajuste permanentes para que las actividades enmarcadas en Seguridad y Privacidad de la información se adapten a la realidad y las necesidades de la entidad en materia de seguridad de la información sean plenamente cubiertas.

Para más información acerca del Diagnóstico de Controles de la Norma ISO 27001:2013, ver el ANEXO1_DIAGNOSTICOCONTROLES_ISO27001.

7 RESULTADOS DEL DIAGNÓSTICO DE CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES LEY 1581 DE 2012 - LEPD.

A continuación se presentan los resultados del "Diagnóstico de cumplimiento de la ley de protección de datos personales ley 1581 de 2012 - LEPD" realizado en conjunto a los macroprocesos de la Universidad del Quindío y evaluar el nivel de madurez del mismo respecto a la Ley 1581 de 2012 LEPD, teniendo en cuenta los requerimientos obligatorios que define la Ley y sus decretos reglamentarios.

Se realiza análisis de brechas para el cumplimiento de la Ley 1581 de 2012 Protección de datos Personales, aplicables a la Universidad del Quindío, y sus macroprocesos de:

- Planeación estratégica.
- Gestión y aseguramiento de la calidad
- Gestión tics
- Gestión humana
- Comunicaciones estratégica
- Control interno
- Gestión documental
- Administración del campus
- Gestión de bienestar institucional
- Gestión jurídica
- Gestión de apoyo académico

*7.1 **METODOLOGIA***

El diagnostico de brechas incluyo labores de acercamiento y conceptualización general de los procesos y procedimientos adelantados por cada uno de los macroprocesos de la Universidad del Quindío en materia de tratamiento de información relativa a datos personales.

Se establece como metodología para realizar el diagnóstico del nivel de madurez al Proceso de Protección de Datos Personales de la Universidad del Quindío, la realización de entrevistas con los líderes de los macroprocesos, para conocer su acercamiento y conceptualización general de los procesos y procedimientos en materia de tratamiento de información relativa a Datos Personales y para la recolección de

información, registro y análisis de la misma que son los insumos para la elaboración del informe de Diagnostico.

Criterios de Niveles de Madurez

Para la observación del nivel de madurez obtenido se utiliza la tabla No. 7 la cual describe y establece los correspondientes rangos de calificación en cuanto a la Cumplimiento de Responsabilidad Demostrada.

NIVEL DE MADUREZ	CUMPLIMIENTO	CRITERIOS
No existente: No cumple, no se hace.	No cumple	Si Cumple es = 0%
Inicial / Ad hoc: La actividad no se realiza por falta de recursos, no se ha considerado su ejecución.	Parcial	Si Cumple es > 0% y <= 5%
Repetible pero intuitivo: La actividad no está completamente entendida, se ha planificado la ejecución a futuro.	Parcial	Si Cumple es > 5% y <= 25%
Proceso definido: La actividad se realiza de forma incompleta y limitada en alcance.	Cumple	Si Cumple es > 25% y <= 50%
Administrado y medible: Se hace cubriendo todo el alcance de la actividad pero no de la forma más óptima, requiere mejoras.	Cumple	Si Cumple es > 50% y <= 80%
Optimizado: No requiere mejoras, está funcionando de acuerdo con lo requerido por el proceso y conforme a las mejores practicas	Cumple	Si Cumple es > 80%

Tabla 6. Criterios de Nivel de Madurez

7.2 HALLAZGOS GENERALES

El esquema presentado, con el fin de otorgarle una mejor organización y evitar la dispersión de la información, se fragmenta en los diferentes servicios y procesos en los que se maneja información personal dentro de la Universidad del Quindío.

Cada una de las materias tratadas se encuentra analizada incluyendo cuatro apartes que permiten abarcar la situación de la entidad en torno al manejo de la información personal. Estas son:

- ✓ Macroproceso: Hace referencia al Macroproceso en la cual se observó algún asunto que representa un riesgo de incumplimiento.

- ✓ Riesgo Observado: Se presenta de manera sintética la situación encontrada en la Universidad del Quindío, que constituye o podría llegar a constituir un escenario de riesgo por incumplimiento a los postulados normativos en la administración de datos personales de acuerdo con la Ley 1581 de 2012 y los decretos reglamentarios.

- ✓ Principios: Principios del Art. 4 de la ley 1581 de 2012 y relacionado con el riesgo observado, que junto con la normatividad facilita el entendimiento del asunto observado.

- ✓ Sustento legal: Norma que desarrolla los principios y deberes en la administración de datos personales. Se relaciona con las obligaciones de los sujetos obligados y se nutren con los principios contenidos en el régimen de protección de datos en Colombia.

Macroproceso	Riesgo observado	Principios	Sustento Legal
Todos	No se observa si la Universidad del Quindío, ha establecido internamente un manual que contiene procedimientos específicos dirigidos a la protección de datos personales. Dentro de los asuntos a tratar en el manual correspondiente, es necesario incluir aspectos referentes al tratamiento de bases de datos temporales y no estructurados, indicando la obligatoriedad de su reporte al área que sea designada como oficial de privacidad y su finalidad.	Legalidad Transparencia	Ley 1581 de 2012 Art. 17 Lit. k) Decreto 1074/15 Cap. 25 Art. 4 Art. 11 Art. 18 Art. 26

Todos	No se observa si la Universidad del Quindío cuenta con un procedimiento específico dirigido al almacenamiento de los datos personales y las autorizaciones recopiladas para su administración.	Legalidad Seguridad	Ley 1581 de 2012 Art. 17 Lit. K) Decreto 1074 de 2015 Cap. 25 Art. 4 Art. 11 Art. 18 Art. 26
Todos	No se observa la existencia de controles periódicos que permitan una autoevaluación de cumplimiento a nivel técnico, organizacional y legal en temas de LEDP.	Legalidad Seguridad	Ley 1581 de 2012 Art. 17 Lit. o) Evidencia principio de responsabilidad demostrada
Todos	No se observa un inventario de bases de datos que cumpla las normas de protección de datos en materia de clasificación y tipificación.	Legalidad Transparencia	Ley 1581 de 2012 Art. 25 Decreto 1074 de 2015 Cap. 26 Art. 5 Art. 9 Circular Externa 02 del 3 de noviembre de 2015 SIC
Todos	En la Universidad del Quindío no se observa si se tiene establecido un proceso completo de actualización, verificación, supresión o eliminación de la información contenida en su base de datos en caso que un titular quiera ejercer ese derecho sobre sus datos personales.	Legalidad Veracidad o calidad Seguridad	Ley 1581 de 2012 Art. 8 Lit. a) y e) Art. 15 Art. 17o Lit a), j) y k) Art. 29 Decreto 1074 de 2015 Art. 4 Inc. Segundo Art. 9

			Art. 11 inc. Segundo Art. 13 No. 4 y 5 Art. 18 Art. 22
Todos	No se observa si se efectúan visitas de auditoría o verificación de un adecuado tratamiento de la información por parte de los terceros (encargados) como parte de una política de la entidad.	Acceso y Circulación Restringida Seguridad Confidencialidad	Ley 1581 de 2012 Art. 17 Lit d), i) Decreto 1074 de 2015 Art. 11 Art. 13
Todos	La Universidad del Quindío, maneja un catálogo de servicios de tecnología de la información que a pesar de contar con muchos procedimientos y controles a nivel tecnológico, no contempla procesos para información almacenada en medios físicos no automatizados. Esta dado al área de gestión documental.	Aspectos generales de seguridad de la información. Seguridad	Ley 1581 de 2012 Art. 17 lit. d Art 5 Art 6 Decreto 1074 de 2015 Cap. 25 Art. 3º Num 3 Art. 6º Art. 19º en proceso de regulación por la SIC Art. 26º Inciso final
Gestión del Campus	En la Universidad del Quindío se observa que tiene áreas de video vigilancia, y no ha dispuesto de los avisos.	Deber de Informar	Ley 1581 de 2012. Art. 12. Deber de informar al Titular.

Tabla 7. Hallazgos Generales LEPD.

*7.3 **HALLAZGOS ESPECÍFICOS***

- ✓ De acuerdo con la información suministrada por cada una de los macroprocesos, la Universidad del Quindío, realiza tratamiento de datos personales en dos sentidos: De terceros (Convenios/Clientes/Proveedores) y por otra parte información de personas relacionadas directamente con la Universidad del

Quindío, constituida básicamente por Aspirantes, Estudiantes, Graduados, Docentes y personal Administrativo.

- ✓ Se observó que la Universidad del Quindío, trabaja con datos sensibles, que para la Ley 1581 de 2012, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- ✓ Entre los datos sensibles que maneja la Universidad del Quindío están aquellos derivados de los programas sobre población vulnerable, Estudiantes matriculados o en proceso de admisión en programas de formación de la Universidad en condición de menor de edad, datos de estudiantes en condiciones de vulnerabilidad por seguimiento en programas de Bienestar Universitario, Atención Psicológica y de Salud, datos de personas que son objeto de estudios realizados en marco de investigaciones de los programas de formación de la Universidad y los registros que se realizan en marco del sistema de Circuito Cerrado de Cámaras y Actividades del macroproceso de Comunicaciones Estratégicas.

- ✓ El diagnóstico inicial levantado con las áreas por medio de la aplicación de entrevistas personales permite reconocer la existencia de ciertos riesgos en el tratamiento de la información. Se abordaron las entrevistas teniendo en cuenta los macroprocesos y estructura organizacional de la Universidad del Quindío.

- ✓ Al observarse que no está el procedimiento o documento del Sistema de Protección de Datos Personales de la Universidad del Quindío, los candidatos en procesos de selección de personal, no se observa si estos otorgan autorización por escrito para el tratamiento de sus datos personales a la Universidad del Quindío y por consiguiente tampoco para los encargados de datos personales (Terceros).

- ✓ No se observa un proceso claro para la recepción de hojas de vida en el que se informe de forma previa, expresa e informada al candidato de las finalidades de uso de sus datos, incluyendo la participación o no en procesos futuros.

- ✓ En Procesos de Bienestar a los trabajadores, se observa que tratan datos de hijos de los empleados tales como nombre y edad de los niños (Fecha de nacimiento). A pesar de ser datos públicos se debería contar con la autorización de padres o tutores.

- ✓ Se observa que se hacen campañas de actualización de Datos de los empleados pero no hay un procedimiento establecido conforme la ley 1581.

- ✓ Se observan algunos encargados de tratamiento de Datos personales como la Empresa de Seguridad, y no se observa el control específico de auditoria sobre terceros que tratan datos personales a nombre de la Universidad del Quindío.

- ✓ Se observa que se han implementado las medidas técnicas, humanas y administrativas que buscan otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, falta alinearlos a un Sistema de Gestión de Datos Personales.

- ✓ Para cumplimiento del Principio de confidencialidad que trata el numeral h del Art. 4 de la Ley 1581 de 2012 se observó que todas las personas que intervienen en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

- ✓ Se observó que en la Universidad se han realizado sensibilizaciones sobre cumplimiento de la Ley 1581 de 2012.

- ✓ Se observan esfuerzos desde los macroprocesos de Gestión Académica, Gestión Documental, Gestión Jurídica y Direccionamiento estratégico para el cumplimiento de los requerimientos de ley.

- ✓ Se observa que se ha implementado un proceso para la gestión y atención de PQRSF, en el cual se hace seguimiento a las peticiones.

*7.4 **Guía de Responsabilidad Demostrada – Accountability***

El principio fundamental de la Responsabilidad Demostrada - Accountability indicado por la OECD - Organización Internacional para la Cooperación Económica y el Desarrollo, indica que una entidad que recoge y hace tratamiento de datos personales debe ser el responsable del cumplimiento efectivo de las medidas que implementen los principios de Privacidad y Protección de Datos.

Este principio establece que los responsables del tratamiento de datos personales, deben contar con un programa Integral de Gestión de Datos Personales y estar preparados para demostrar a la autoridad la implementación efectiva de estas medidas en la organización.

El criterio de responsabilidad demostrada se introdujo en el sistema Colombiano de protección de datos personales en el artículo 26 del decreto 1377. Igualmente, en el artículo 27 dispuso que las políticas internas efectivas que se implementen, deberán garantizar que en la organización exista una estructura administrativa proporcional a la estructura del responsable para implementarlas, que se adopten mecanismos internos para poner en práctica las políticas que incluyan herramientas de implementación, entrenamiento y programas de educación, la adopción de procesos para la atención de reclamos y consultas de los titulares.

Por lo anterior, se realizó el diagnóstico del cumplimiento de la Universidad del Quindío ante la Guía de Responsabilidad Demostrada, específicamente en los elementos esenciales que deben ser incorporados a la organización para el desarrollo, implementación y seguimiento de un programa integral de Gestión de Datos Personales.

7.4.1 Resultados del diagnóstico de la Guía de Responsabilidad Demostrada – Accountability

Se presenta a continuación el resultado de la evaluación realizada a los elementos esenciales de la Guía de Responsabilidad Demostrada. En la tabla No. 8 se muestra por cada dominio del Accountability, el porcentaje y el nivel de madurez que se identificó. La información detallada del diagnóstico se puede ver en el "ANEXO2_DIAGNOSTICO_ACCOUNTABILITY_UNIQUINDIO"

Dominios	Diagnostico	Meta	NIVEL DE MADUREZ
DESDE LA ALTA DIRECCIÓN	40%	100%	DEFINIDO
PRESENTACIÓN DE INFORMES	0%	100%	NO EXISTE
PROCEDIMIENTOS OPERACIONALES	0%	100%	NO EXISTE
INVENTARIO DE LA BASES DE DATOS CON INFORMACIÓN PERSONAL	0%	100%	NO EXISTE
POLÍTICAS	33%	100%	DEFINIDO
SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	0%	100%	NO EXISTE
REQUISITOS DE FORMACIÓN Y EDUCACIÓN	50%	100%	DEFINIDO
PROTOCOLO DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES	0%	100%	NO EXISTE
GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES	0%	100%	NO EXISTE
COMUNICACIÓN EXTERNA	25%	100%	NO EXISTE
EVALUACIÓN Y REVISIÓN CONTINUA	0%	100%	NO EXISTE
DEMOSTRAR EL CUMPLIMIENTO	0%	100%	NO EXISTE

Tabla 8. Resultado del diagnóstico del Accountability

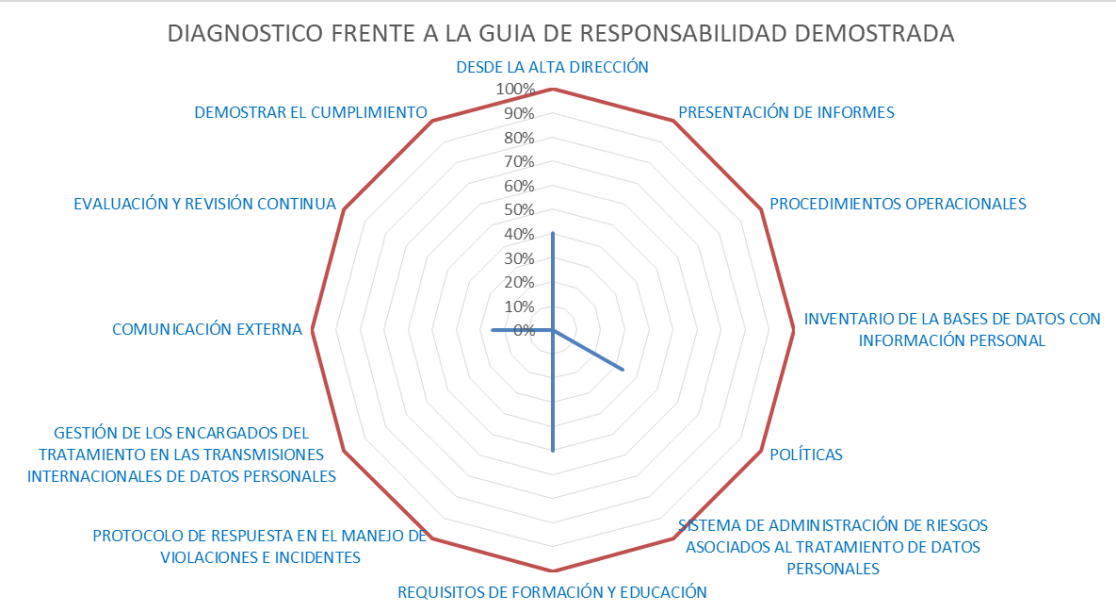


Imagen 5. Radar resultado del diagnóstico del Accountability

De acuerdo con la valoración realizada, el porcentaje del nivel de madurez para el cumplimiento del Accountability por parte de La Universidad del Quindío es del 12%, correspondiente a un nivel de Madurez “Repetible pero Intuitivo”. Lo anterior indica que en La Universidad del Quindío el cumplimiento del Accountability no está completamente entendido y se ha planificado la ejecución a futuro.

7.5 ***CONCLUSIONES PARA LA LEY 1581.***

- ✓ El contenido esencial en el derecho fundamental a la protección de datos se basa en un conjunto de reglas y principios de obligatorio cumplimiento para las organizaciones que tratan la información y que van dirigidas a proteger el dato personal considerado en sí mismo, a la vez que se limitan en el tiempo los tratamientos a que pueda ser sometido. Para ello se definen un conjunto de medidas preventivas de defensa, tanto jurídicas como organizativas y técnicas, que protejan a la información desde el mismo momento que se recolecta y en los tratamientos durante todo su ciclo de vida.

- ✓ En la Universidad del Quindío, se observa que ha implementado controles que buscan garantizar la protección de los derechos fundamentales (incluida la Privacidad) y desde el direccionamiento estratégico, se tiene la intención de dar cumplimiento con los requerimientos de la Lay 1581 de 2012 y su decreto reglamentario 1377 de 2013, Se observan esfuerzos institucionales que buscan garantizar no solo el cumplimiento de la Ley, sino de un Sistema de Gestión de Datos Personales.

- ✓ Se recomienda articular la implementación del Sistema de Gestión de Seguridad de la Información –SGSI- con la implementación de Ley Estatutaria 1581 de 2012: Protección de Datos Personales.

- ✓ Se sugiere formalizar el cargo de Oficial de Privacidad (o Protección de Datos) para la Universidad del Quindío, con funciones y tareas operativas, de puesta en marcha y mantenimiento del Programa Integral de Gestión de Datos Personales.

- ✓ En la Universidad durante el Diagnostico, o se observó la utilización de datos biométricos, relacionados con las Grabaciones de Video por razones de seguridad, en este aspecto, se debe definir la finalidad y el tiempo durante el cual se guardaran los datos. Se debe establecer que estas grabaciones sólo podrán ser consultadas por personal Autorizado directamente o cedidas a las fuerzas y cuerpos de seguridad del Estado. Los datos biométricos y sensibles serán tratados con mayor seguridad que los datos privados de conformidad con la Ley 1581 de 2012. Para la autorización para recolección de datos biométricos, la Universidad deberia informar mediante avisos que está siendo grabado, la finalidad y el tratamiento de este tipo de datos.

Para mayor información, ver
ANEXO2_DIAGNOSTICO_ACCOUNTABILITY_UNIQUINDIO

8 CUMPLIMIENTO COMPONENTE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – COMPONENTE GEL –

Por medio de lo establecido en el Decreto 2573 de 2014, se definieron los lineamientos, instrumentos y plazos de la Estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que presente mejores servicios con la colaboración de toda la sociedad.

Es así como el Artículo 2.2.9.1.2.1 del Decreto 1078 de 20152, definió que los fundamentos de la Estrategia serán desarrollados a través de cuatro (4) componentes que facilitarán la masificación de la oferta y la demanda de Gobierno en Línea, y son: TIC para Servicios, TIC para el Gobierno abierto, TIC para la Gestión y Seguridad y Privacidad de la Información. Así mismo, el Artículo 2.2.9.1.2.2 señaló que los instrumentos para la implementación de la Estrategia de Gobierno en Línea son el Manual de Gobierno en Línea y el Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información. (Decreto 2573 de 2014, art 5).

En este sentido, mediante el Artículo 2.2.9.1.2.3 del Decreto 1078 de 2015 se definió que el responsable de coordinar, hacer seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en Línea será el representante legal y el responsable de orientar la implementación al interior de la Entidad será el Comité Institucional de Desarrollo Administrativo de que trata el Artículo 6 del Decreto 2482 de 2012, o las normas que lo modifiquen o sustituyan. (Decreto 2573 de 2014, art 8).

Por otro lado, el Articulo 2.2.9.1.3.1 del mencionado Decreto, respecto a la Medición y el Monitoreo señaló que: “El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno en Línea y de la Dirección de Estándares y Arquitectura de Tecnologías de la Información diseñará el modelo de monitoreo que permita medir el avance en las acciones definidas en el Manual de Gobierno en Línea que corresponda cumplir a los sujetos obligados, los cuales deberán suministrar la información que le sea requerida.” (Decreto 2573 de 2014, art 9).

Por lo anterior mediante este diagnóstico, se genera la información necesaria para verificar el porcentaje de cumplimiento del componente de seguridad y privacidad de la

información de la estrategia de gobierno en línea – GEL. Esto se medirá a través del cumplimiento de los siguientes logros:

COMPONENTE	LOGROS TIC PARA GOBIERNO ABIERTO
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	DEFINICIÓN DEL MARCO DE SEG. Y PRIV.
	IMPLEMENTACIÓN DEL PLAN DE SEG. Y PRIV.
	MONITOREO Y MEJORAMIENTO CONTINUO

Tabla 9. Logros del Componente Seguridad y Privacidad de la Información.

Seguridad y Privacidad de la Información: Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

8.1 METODOLOGIA

Para verificar el grado de aplicabilidad de los tres logros GEL, se tomaron los lineamientos del marco de referencia establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y se analizaron junto con el diagnostico, teniendo en cuenta la infraestructura, programas y proyectos del macroproceso TICS.

- El método de evaluación está determinado por los siguientes conceptos:

  - **Cumple**: Cumple totalmente con el sub-criterio formulado.
  - **No Cumple**: No Cumple totalmente con el sub-criterio formulado.
  - **Cumple Parcialmente**: Cumple parcialmente con el sub-criterio formulado.

- Entendiendo que la Estrategia GEL, establece el cumplimiento para 4 componentes, los cuales deben arrojar un porcentaje del 100%, cada uno de los componentes descritos tendrá un valor del 25%, valor que será desagregado a nivel de logros, criterios y sub-criterios[2].

[2] Para más información. Visitar página web http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8015.html.

- El análisis de las respuestas establecerá el cumplimiento del componente, Logro, Criterio y Sub-criterio.

- Cada pregunta formulada tiene asociado un peso de acuerdo al cumplimiento de cada sub-criterio. A continuación se muestra en la siguiente imagen, el modo de evaluación:

COMPONENTE		LOGRO		CRITERIO		SUBCRITERIO		CUMPLIMIENTO		
DESCRIPCION	***PESO***	***DESCRIPCION***	***PESO***	***DESC.***	***PESO***	***DESC.***	***PESO***	***CUMPLE***	***PARCIAL***	***NO***
Seguridad y Privacidad de la Información	**25%**	Definición del Marco de Seguridad y Privacidad de la Información	**8,30%**	Diagnóstico de Seguridad y Privacidad	4,15%	LI.ES.01	0.83%	**0.83%**	**0,415%**	**0,00%**
						LI.ES.02	0.83%	**0.83%**	**0,415%**	**0,00%**
						LI.GO.01	0.83%	**0.83%**	**0,415%**	**0,00%**
						LI.GO.04	0.83%	**0.83%**	**0,415%**	**0,00%**
						LI.ST.14	0.83%	**0.83%**	**0,415%**	**0,00%**
				Plan de Seguridad y Privacidad de la Información	4,15%	LI.ES.02	0,59%	**0,59%**	**0,296%**	**0,00%**
						LI.ES.06	0,59%	**0,59%**	**0,296%**	**0,00%**
						LI.ES.08	0,59%	**0,59%**	**0,296%**	**0,00%**
						LI.GO.01	0,59%	**0,59%**	**0,296%**	**0,00%**
						LI.GO.04	0,59%	**0,59%**	**0,296%**	**0,00%**
						LI.GO.09	0,59%	**0,59%**	**0,296%**	**0,00%**
						LI.SIS.22	0,59%	**0,59%**	**0,296%**	**0,00%**
		Implementación del plan de seguridad y privacidad de la información y de los sistemas de información	8,30%	Gestión de Riesgos de Seguridad y Privacidad de la Información	8.3%	LI.INF.15	4,15%	**4,15%**	**2,08%**	**0,00%**
						LI.SIS.22	4,15%	**4,15%**	**2,08%**	**0,00%**
		Monitoreo y mejoramiento continuo	8,30%	Evaluación del Desempeño	8,30%	LI.ES.13	2,08%	**2,08%**	**1,04%**	**0,00%**
						LI.GO.03	2,08%	**2,08%**	**1,04%**	**0,00%**
						LI.GO.12	2,08%	**2,08%**	**1,04%**	**0,00%**
						LI.GO.13	2,08%	**2,08%**	**1,04%**	**0,00%**

Tabla 10. Metodología de Evaluación Componentes GEL

8.1.1 DIAGNOSTICO CUMPLIMIENTO COMPONENTE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – COMPONENTE GEL –

Una vez realizado el análisis de aplicabilidad de los lineamientos que conforman los tres logros GEL establecidos en el MSPI y el diagnóstico del anexo A de la norma ISO/IEC 27001:2013[3], y el diagnóstico de cumplimiento de la Ley de Protección de datos personales - LEPD (ley 1581 de 2012), se obtuvieron los siguientes resultados a través de estimaciones porcentuales de avance según el detalle determinado por la información obtenida:

Detalle del Componente		Evaluación		
Logro	**Criterio**	**Pregunta**	**Estado**	**Peso**
Definición del marco de seguridad y privacidad de la información y de los sistemas de información Busca definir el estado actual del nivel de seguridad y privacidad y define las acciones a implementar.	**Diagnóstico de Seguridad y Privacidad** Busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información.	La Universidad ha establecido el estado actual de la gestión de la seguridad y privacidad de la información?	cumple	0,83%
		La Universidad ha observado el nivel de madurez de seguridad y privacidad de la información?	cumple	0,83%
		La Universidad ha observado vulnerabilidades técnicas y administrativas que sirven como insumo de la etapa de planificación?	parcial	0,42%
		La Universidad da cumplimiento a la legislación vigente relacionada con protección de datos personales?	no cumple	0,0%
		La Universidad ha adoptado buenas prácticas en ciberseguridad?	parcial	0,42%
	Plan de Seguridad y Privacidad de la Información Busca generar un plan de seguridad y privacidad alineado con el	La Universidad tiene definidas las necesidades y expectativas de las partes interesadas relacionadas con la seguridad de la información?	parcial	0,21%
		Existe aprobación por parte de la alta dirección en la implementación de seguridad de la información en la Universidad?	no cumple	0,00%

[3] ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) para cualquier organización sin importar su tipo o tamaño.

Detalle del Componente		Evaluación		
Logro	**Criterio**	**Pregunta**	**Estado**	**Peso**
	propósito misional.	La Universidad ha definido una política de seguridad y privacidad de la información, alcance y objetivos correspondientes?. Esta debe estar debidamente aprobada por la Dirección y socializada en la Universidad	parcial	0,21%
		La Universidad ha definido las políticas de seguridad de la información?. Estos deben estar documentados, socializados y aprobados por el comité.	parcial	0,21%
		La Universidad ha establecido un comité de seguridad de la información con los respectivos roles y responsabilidades?	no cumple	0,00%
		La Universidad ha realizado la observación, valoración y clasificación de los activos de acuerdo a la legislación aplicable?	parcial	0,21%
		La Universidad tiene integrado el Sistema de Gestión de Seguridad de la Información con el Sistema Integrado de Gestión y Documental?	parcial	0,21%
		La Universidad ha observado, valorado y tratado los riesgos de seguridad de la información?	parcial	0,21%
		La Universidad tiene establecido un plan de comunicaciones relacionado con los aspectos de seguridad de la información?	parcial	0,21%
		La Universidad ha elaborado un plan de diagnóstico para la implementación del protocolo IPV6?	cumple	0,42%
Implementación del Plan de Seguridad y Privacidad de la Información y de los Sistemas de Información Busca desarrollar las acciones definidas en el	**Gestión de Riesgos de Seguridad y Privacidad de la Información.** Busca proteger los derechos de	La Universidad ha implementado una estrategia para la implementación del tratamiento de riesgos de seguridad de la información	parcial	1,04%
		La Universidad ha desarrollado una declaración de aplicabilidad	no cumple	0,00%

Detalle del Componente		Evaluación		
Logro	**Criterio**	**Pregunta**	**Estado**	**Peso**
plan de seguridad y privacidad.	los usuarios de la Universidad y mejorar los niveles de confianza en los mismos a través de la observación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.	La Universidad ha establecido indicadores para medir la efectividad, eficiencia y eficacia respecto a la seguridad de la información	No cumple	0,00%
		La Universidad ha documentado un plan para la transición e implementación del protocolo IPv6	cumple	4,20%
Monitoreo y Mejoramiento Continuo Busca desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información.	**Evaluación del Desempeño** Busca hacer las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información.	La Universidad ha realizado procesos de revisión, seguimiento a la implementación del MSPI	No cumple	0,00%
		La Universidad ha realizado auditorias y revisiones independientes al MSPI	No cumple	0,00%
		La Universidad ha desarrollado/documentado planes de mejoramiento continuo respecto a la seguridad de la información?	parcial	1,04%
		La Universidad ha desarrollado pruebas de funcionalidad del protocolo IPv6?	no cumple	0,00%

Tabla 11. Cumplimiento GEL por Logro.

El estado ideal de cumplimiento del componente de Seguridad y Privacidad de la Información para las vigencias de 2017 y 2018 es del 50% y 65% respectivamente. Después de realizado el diagnóstico sobre este componente, el porcentaje de cumplimiento es de 11,09%.

COMPONENTE	PESO COMPONENTE	LOGROS TIC PARA GOBIERNO ABIERTO	PESO LOGRO	PESO IDEAL
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	11,09%	DEFINICIÓN DEL MARCO DE SEG. Y PRIV.	**4,81%**	16,6%
		IMPLEMENTACIÓN DEL PLAN DE SEG. Y PRIV.	**8,3%**	16,6%
		MONITOREO Y MEJORAMIENTO CONTINUO	**4,2%**	16,6%

Tabla 12. Cumplimiento GEL por componente.

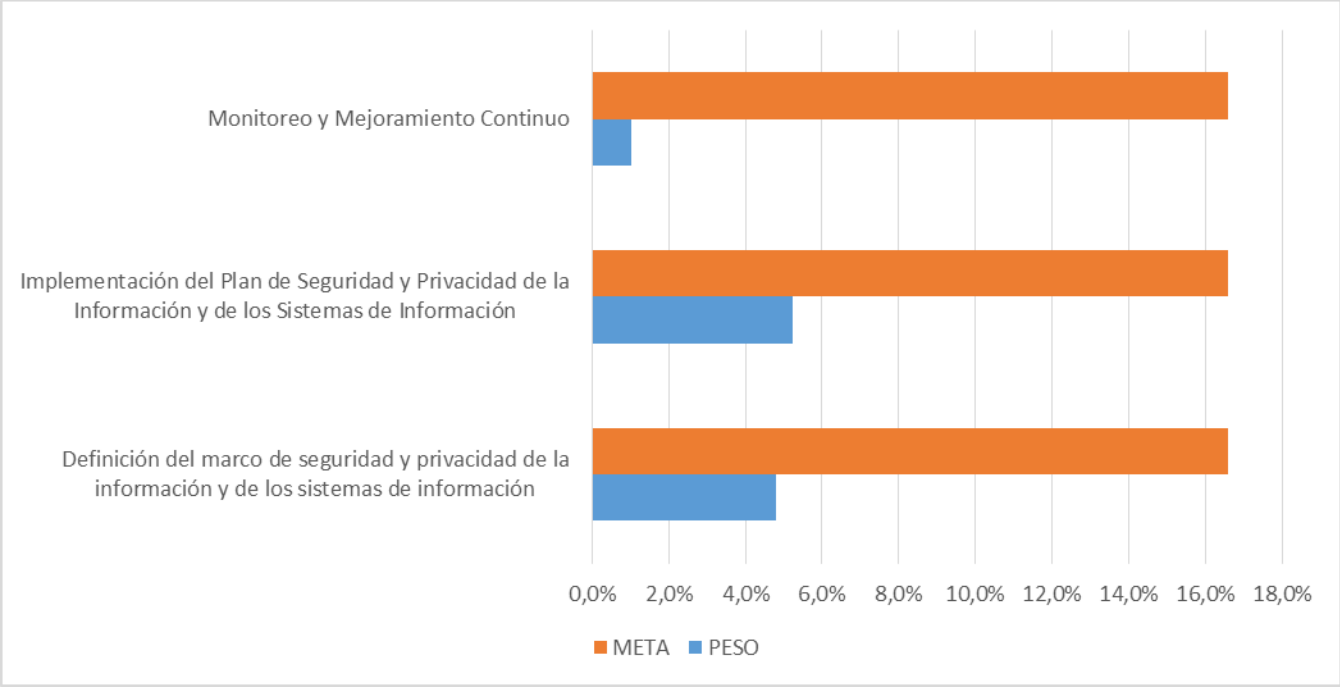


Imagen 6. Estado de cumplimiento por logros.

Para ver la calificación completa, ver ANEXO3_CALIFICACION_GEL

Para mayor información sobre la aplicabilidad de lineamientos de la estrategia GEL, consulte el ANEXO6_APLICABILIDAD LINEAMIENTOS

9 NORMATIVA REFERENTE.

- La Ley 1581 de 2011. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012

- Decreto 2623 de 2009, *"Por el cual se crea el Sistema Nacional de Servicio al Ciudadano".*

- Documento CONPES 3650 de 2010, del Consejo Nacional de Política Económica y Social. República de Colombia. Departamento Nacional de Planeación "Importancia Estratégica de la Estrategia de Gobierno en Línea".

- Circular 002 de 2011, del Ministerio de Tecnologías de la Información y las Comunicaciones, donde promueve la adopción del IPv6 en Colombia.

- Ley 1712 del 6 de marzo de 2014 del Congreso de la República, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- Decreto 2573 de 2014 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones."

- Decreto 1078 de 2015 del Ministerio de la Información y las Comunicaciones, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- Decreto 0103 de 2015 de la Presidencia de la República de Colombia, "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

10 DOCUMENTOS CONSULTA UNIVERSIDAD DEL QUINDIO

- El Plan de Desarrollo Institucional (PDI) 2016 - 2025 Por una Universidad del Quindío Pertinente, Creativa, Integrador. Con el cual buscan fortalecer la infraestructura tecnológica del campus universitario en cuanto a la adquisición y reposición de equipos de cómputo y audiovisuales, bases de datos y software, y sistema de seguridad integrado.

- INDICE INFORMACIÓN CLASIFICADA Y RESERVADA - FINAL UQ. Registro de activos de información - esquema de publicación de información - índice de información clasificada y reservada.

- Resolución de Rectoría 3375 del 15 de Agosto de 2017 "POR MEDIO DE LA CUAL SE ACTUALIZA LA ESTRUCTURA DEL SISTEMA INTEGRADO DE GESTIÓN DE LA UNIVERSIDAD DEL QUINDIO Y SE DICTAN OTRAS DISPOSICIONES". ARTÍCULO SEGUNDO. CARACTERISTICAS Y NECESIDADES: Para la observación de necesidades y características de la Institución tendientes a la actualización de la estructura del Sistema Integrado de Gestión, se tuvieron en cuenta los siguientes aspectos normativos: Decreto único reglamentario 1078 de 2015 (Componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL-ISO/IEC 27000).

- Acuerdo del Consejo Superior No.20 del 18 de diciembre del año 2015, por medio del cual se establece la estructura organizacional de la Universidad del Quindío, se determinan las funciones de sus dependencias y se dictan otras disposiciones.

- Resolución de Rectoría 0899 de 19 de agosto de 2010. Por medio de la cual se expiden normas sobre políticas éticas de confidencialidad en el desarrollo de las acciones de gestión.

- Resolución de Rectoría 2167 del 1 de septiembre de 2016. "POR MEDIO DE LA CUAL SE ACTUALIZA EL CODIGO DE ETICA Y EL CODIGO BUEN GOBIERNO DE LA UNIVERSIDAD DEL QUINDIO". Compromiso de Confidencialidad: la institución se compromete a que los servidores públicos que manejan información privilegiada firmen acuerdos de confidencialidad para que se asegure que la información que es reserva de la institución no sea publicada o conocida por

terceros. Ninguno de los grupos de interés puede directa o indirectamente utilizar información privilegiada y confidencial de la institución para sus propios intereses.

- Resolución de Rectoría 1350 de 30 de diciembre de 2015. POR MEDIO DE LA CUAL SE AJUSTA EL MANUAL DE FUNCIONES Y DE COMPETENCIAS LABORALES PARA LOS CARGOS DE LOS NIVELES DIRECT! VO, ASESOR Y PROFESIONAL ESTABLECIDOS EN LA PLANTA DE PERSONAL ADMINIS TRA TI VA DE LA UN! VERSIDAD DEL QUINDIO.

- Resolución de Rectoría 1366 del 4 de enero del 2016. "POR MEDIO DE LA CUAL SE ACTUALIZA EL REGLAMENTO PARA LA TRAMITACION INTERNA DE LAS PETICIONES, QUEJAS, RECLAMOS, SUGERENCIAS, DENUNCIAS V FELICITACIONES "PQRSDF" EN LA UNIVERSIDAD DEL QUINDIO"

Otros documentos:

- BORRADOR POLITICA SEGURIDAD DE LA INFORMACIÓN. POR MEDIO DE LA CUAL SE EXPIDE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DEL QUINDIO.

- Organigrama_uniQuindío2017

- Plan de Contingencia TIC 2010

- Plan Maestro de Seguridad y de Contingencia. PLAN DE SEGURIDAD DE LA INFORMACIÓN 2010 – 2015.

11 ANEXOS

11.1 ***ANEXO1_DIAGNOSTICOCONTROLES_ISO27001***

11.2 ***ANEXO2_DIAGNOSTICO_ACCOUNTABILITY_UNIQUINDIO***

11.3 ***ANEXO3_CALIFICACION_GEL***

11.4 ***ANEXO4_ALCANCE_SGSI***

11.5 ***ANEXO5_DEFINICION_POLITICA_SGSI***

11.6 ***ANEXO6_APLICABILIDAD LINEAMIENTOS***

11.7 ***DOC_HOJA_DE_RUTA_UNIQUINDIO***

11.8 ***DOC_HOJA_DE_RUTA_UNIQUINDIO_SEGURIDAD***