



Universidad de
CUNDINAMARCA



Jornada de Sensibilización en Seguridad y Privacidad de la Información

Sistema de Gestión
de Seguridad de la
Información



2024



SISTEMA DE GESTIÓN DE
SEGURIDAD
DE LA INFORMACIÓN
SGSI

Agenda

- 1.** Presentación del equipo
- 2.** Circular N° 016 de 2024-07-09
- 3.** ¿Porqué es importante participar en las Jornadas de Sensibilización?
- 4.** Modelo de Gestión Integral de Seguridad de la Información
- 5.** Preguntas y cierre



1.

Presentación del Equipo



**Maria del Pilar
Delgado Rodríguez**
Coordinadora del SGSI



**Brayan Esteban
Ortegon Palomino**
Frente de Protección de
Datos Personales



**Lesly Daniela
Reyes Pérez**
Frente de Protección de
Datos Personales



**Brenda Camila
Mesa Roza**
Frente de Protección de
Datos Personales



**Fabian Libardo
Parra Gutiérrez**
Frente de Seguridad de
la Información



**Francisco Javier
Romero Hernández**
Frente de Seguridad de
la Información



**Eimy Daniela Melo
Rodríguez**
Frente de Seguridad de
la Información



**Nicolas Mauricio
Bobadilla Reyes**

Circular N°016 de 2024-07-09

De la vicerrectoría administrativa y financiera



– SEDE FUSAGASUGÁ –

ADOr003_V8

Página 1 de 1

30.

CIRCULAR No.016

DE: MYRIAM LUCIA SANCHEZ GUTIERREZ

CARGO: VICERRECTORA ADMINISTRATIVA Y FINANCIERA

PARA: DIRECTORES DE ÁREA, JEFES DE OFICINA, LÍDERES DE PROCESOS, DECANOS Y COORDINADORES DE PROGRAMAS.

CIUDAD Y FECHA: FUSAGASUGÁ, 2024-07-09

ASUNTO: JORNADAS DE SENSIBILIZACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2024

En atención a lo aprobado en la sesión ordinaria de la Comisión de Gestión del 5 de junio de 2024, el Sistema de Gestión de Seguridad de la Información – SGSI, atendiendo lo dispuesto en el PLAN INSTITUCIONAL DE SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – ESG-SSI-PL01 y al aspecto por mejorar documentado en el informe final producto de la Auditoría Interna II, orientará la Jornadas de Sensibilización en la Universidad de Cundinamarca, se dará a conocer los avances de la Implementación del Sistema de Gestión de Seguridad de la Información y la Ley de Protección de Datos Personales. Por tal motivo se solicita la colaboración de los *Directores de Área, Jefes de Oficina, Líderes de Proceso, Decanos y Coordinadores de Programa* para contar con la participación de todos los funcionarios (administrativos y docentes) de la dependencia a su cargo.

Se estará notificando a cada líder de dependencia por medio de correo electrónico el día en que será agendado con su equipo de trabajo a la Jornada de Sensibilización en Seguridad y privacidad de la información. Es importante contar con la participación y el compromiso en las jornadas de sensibilización, para así disminuir el riesgo de que se materialicen eventos en Seguridad y Privacidad de la Información. De tener alguna inquietud, favor comunicarse mediante correo electrónico con el Sistema de Gestión de Seguridad de la Información – SGSI: sgsi@ucundinamarca.edu.co.

Cordialmente,

SANCHEZ
GUTIERREZ
MYRIAM LUCIA

MYRIAM LUCIA SANCHEZ GUTIERREZ
Vicerrectora Administrativa y Financiera

Vs. Bco Coordinadora SGSI- María del Pilar Delgado Rodríguez
Vs. Bco Directora de Sistemas y Tecnología - Ana Lucía Hurtado Mesa
Proyecto: Sistema de Gestión de Seguridad de la Información - SGSI

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2



¿Por qué es importante participar en las jornadas de sensibilización?

ISO 27001: 2022 numeral 7.3 – Toma de Conciencia

Tip 4: Todos los empleados deben conocer las Políticas de Tratamiento de Datos - SIC

Guía 14 “Plan de Capacitación, sensibilización y comunicación de Seguridad de la Información” - MSPi

ESG-SSI-PL01 - PLAN DE SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oportunidad de Mejora producto de la Auditoría Interna II del SGSI: “Aunque se han realizado capacitaciones del sistema a los colaboradores de la entidad, es importante que todos los funcionarios participen de estas sesiones y así poder evaluar su efectividad mediante indicadores que midan la asistencia y la adopción del conocimiento”.



3.

¿Por qué es importante participar en las jornadas de sensibilización?

Atendiendo el control del Anexo A 6.4 Proceso Disciplinario de la Norma ISO 27001:2022 “Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información”

La Dirección de Control Disciplinario, envió oficio al Sistema de Gestión de Seguridad de la Información el día 29 de mayo de 2023, el cual se ha venido aplicando. (4 eventos)

Me dirijo a usted, con el fin de dar claridad sobre los pasos a seguir en cuanto a la recepción de quejas y el procedimiento a seguir establecido en el Acuerdo 003 de 2020 “POR EL CUAL SE ADOPTA EL ESTATUTO DISCIPLINARIO DEL PERSONAL ACADÉMICO Y ADMINISTRATIVO DE LA UNIVERSIDAD DE CUNDINAMARCA, así:

“ARTÍCULO 50. Oficiosidad: La acción disciplinaria se iniciará y adelantará de oficio, o por información proveniente de servidor público o por otro medio que amerite credibilidad, o por queja formulada por cualquier persona, y no procederá por anónimos, salvo en los eventos en que cumpla con los requisitos mínimos consagrados en el Código Único Disciplinario” (subrayado, negrilla y cursiva fuera de texto)

1. En primer lugar, una vez se tenga conocimiento, de alguna presunta conducta irregular por parte de algún funcionario o estudiante, es un deber, de informar a la Oficina de Control Disciplinario.
2. Una vez recibida la queja o informe, en esta Dirección, evaluará lo correspondiente, es decir si apertura indagación o investigación o decisión inhibitoria¹

3. Si la decisión es de aperturar indagación o investigación disciplinaria, esta Dirección, adelantará labores investigativas, tendientes a verificar la presunta falta en que se pudo incurrir, para el caso puntual, se tipificará la siguiente falta descrita en el numeral 4 de artículo 10 del citado acuerdo que indica:

“Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.”

4. Dependiendo del material probatorio recaudado, la Dirección evaluará dicho material probatorio y consecuentemente adoptará la decisión de archivo o de formular pliego de cargos², para el caso de funcionarios de la Udec, para los estudiantes elaborará informe de recomendación.

Es necesario indicar que esta Dirección siempre estará a disposición de recibir cualquier información sobre irregularidades al interior de la Institución, no es necesario acudir a cualquier otra dependencia para dar a conocer sobre hechos que atenten contra el buen nombre y buen funcionamiento de la Universidad.

Lineamiento para la entrega de cargos, por desvinculación del funcionario o traslado de área

La entrega de cargo se debe realizar en compañía de la Dirección de Control Interno y el Sistema de Gestión de Seguridad de la Información - SGSI

Lineamiento a tener en cuenta:

Entrega a partir de los activos de la Información a cargo del funcionario.

- 1. Talento Humano**
- 2. Información** (Inventarios Documentales)
- 3. Software** (contratos)
- 4. Hardware** (Inventario de Activos físicos)
- 5. Servicios** (plataformas, correos, token, entre otros)
- 6. Infraestructura**

Legislación colombiana sobre delitos informáticos

LEY 1273 DEL 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.



Legislación colombiana sobre delitos informáticos

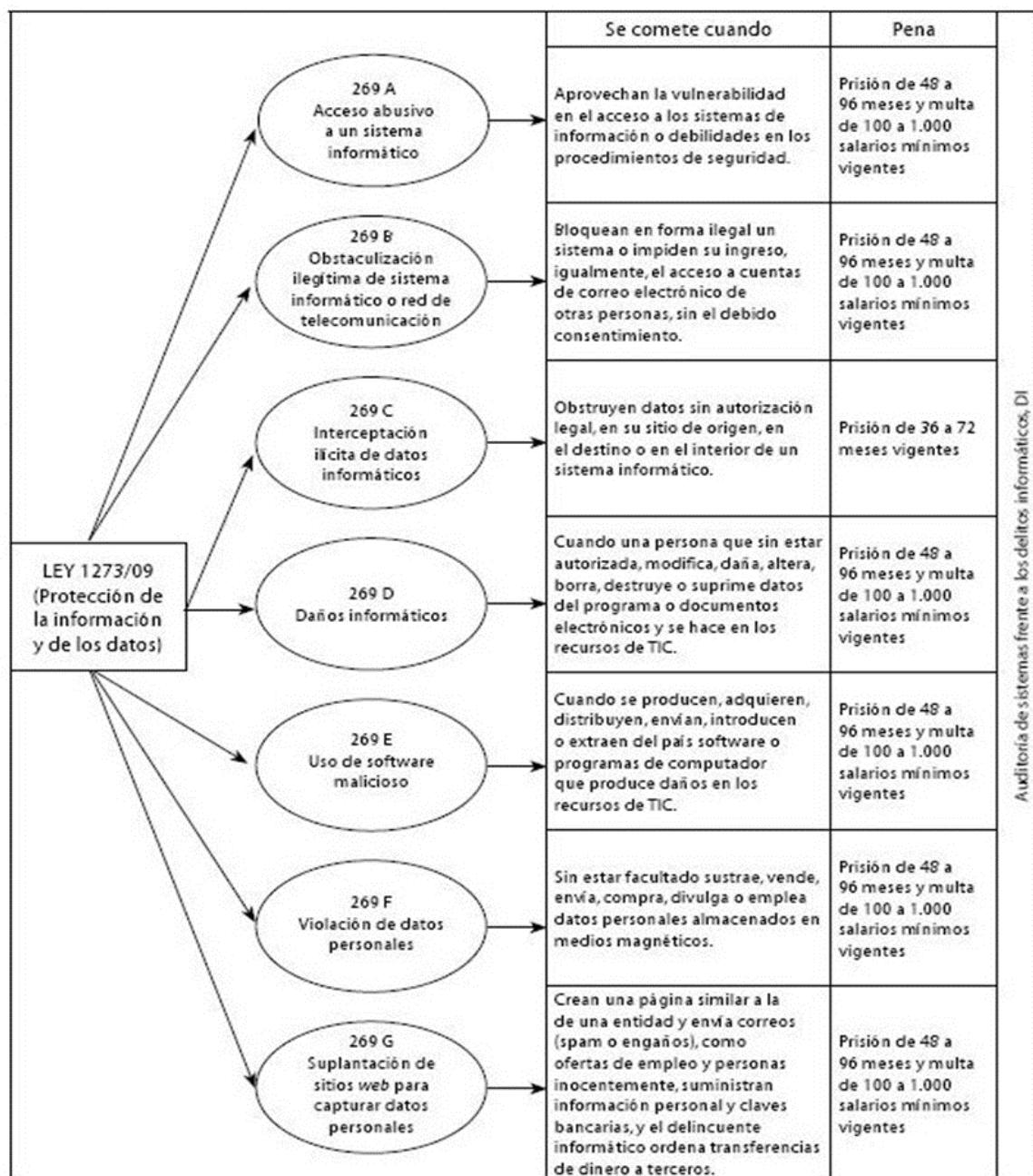


Figura 2. Legislación penal colombiana frente a los delitos informáticos (artículo 1 de la Ley 1273 de 2009).

Fuente: Elaboración de los autores, con base en la Ley 1273 de 2009. Congreso de la República (2009).

Marco legal para seguridad de la información

Ley 1712 del 2014

“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.” (Artículo 13, 20)

Decreto 1078 de 2015

“Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” (Título 9 “Políticas y lineamientos de tecnologías de la información”

Resolución 500 de 2021

“Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital”

Norma Técnica NTC-ISO IEC Colombiana 27001 de 2022

Organización Internacional de Normalización - Comisión Electrotécnica Internacional

Modelo de Seguridad y Privacidad de la Información - MSPI

El MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información

Marco legal para seguridad de la información

Resolución No. 088 del 2023

“Por la cual se establece el Sistema de Aseguramiento de la Calidad de la Universidad de Cundinamarca”.

Resolución No. 092 de 2023

“Por la cual se adopta el Sistema de Gestión de Seguridad de la Información – SGSI y se establecen lineamientos, objetivos y alcance en la Universidad de Cundinamarca”.

Resolución No. 140 del 2022

Por la cual se designa el coordinador del Sistema de Gestión de Seguridad de la Información - SGSI y la Protección de Datos Personales de la Universidad de Cundinamarca”.

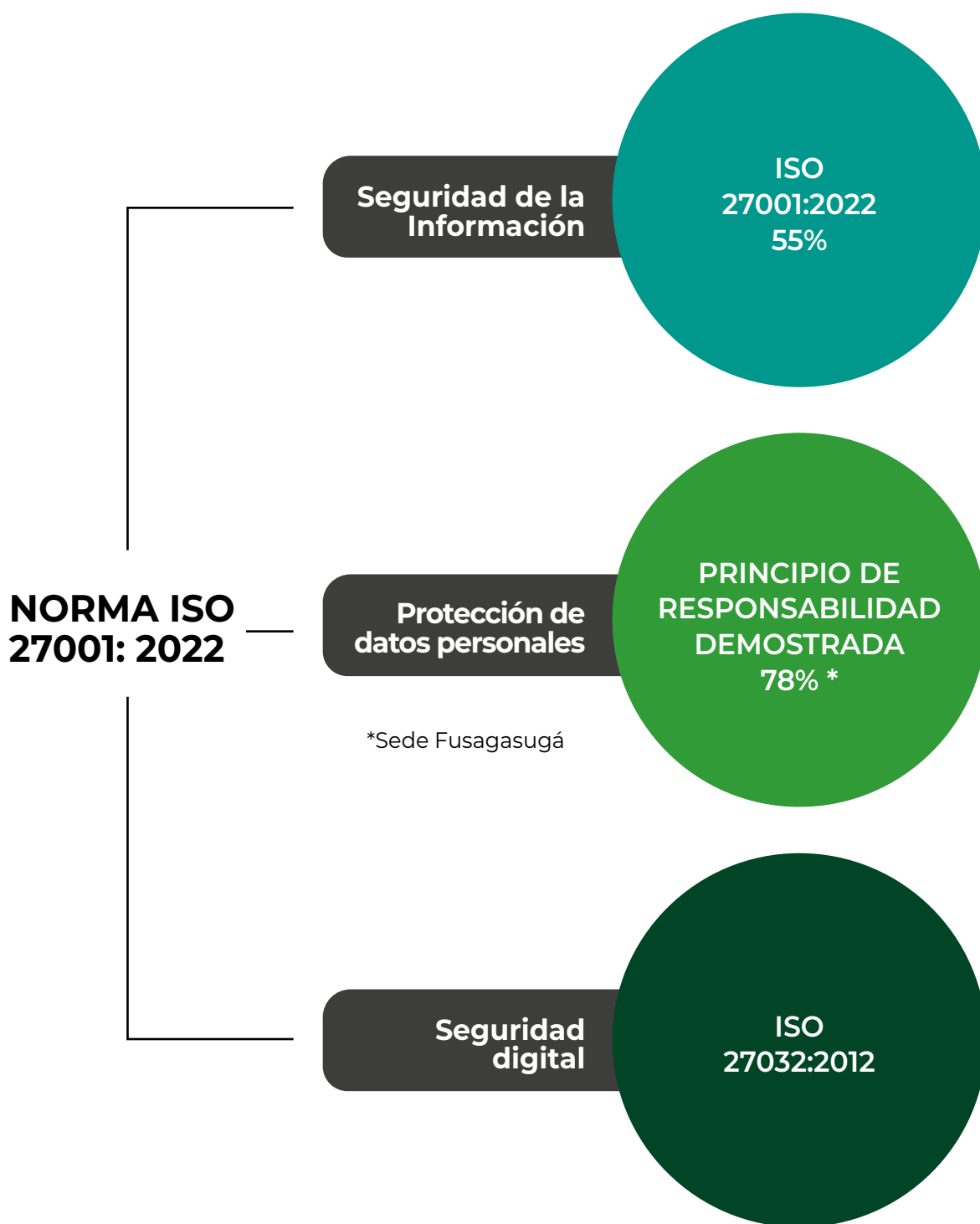
Resolución No. 027 de 2020

“Por la cual se establecen los roles y responsabilidades de los sistemas de gestión de la Universidad de Cundinamarca”.

I N T E R N A



Frentes del sistema de gestión de seguridad de la información

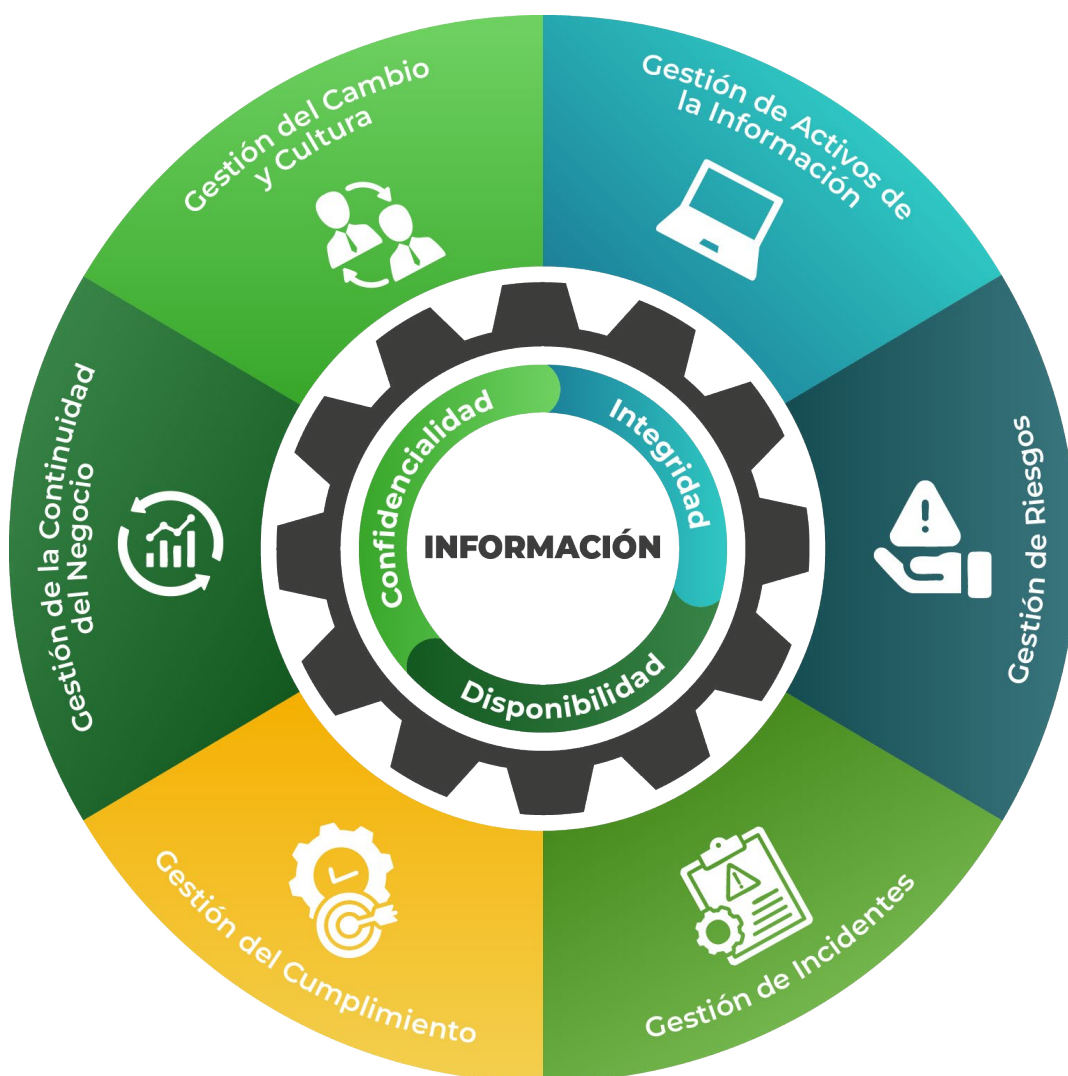


4.

Modelo de gestión integral de seguridad de la información

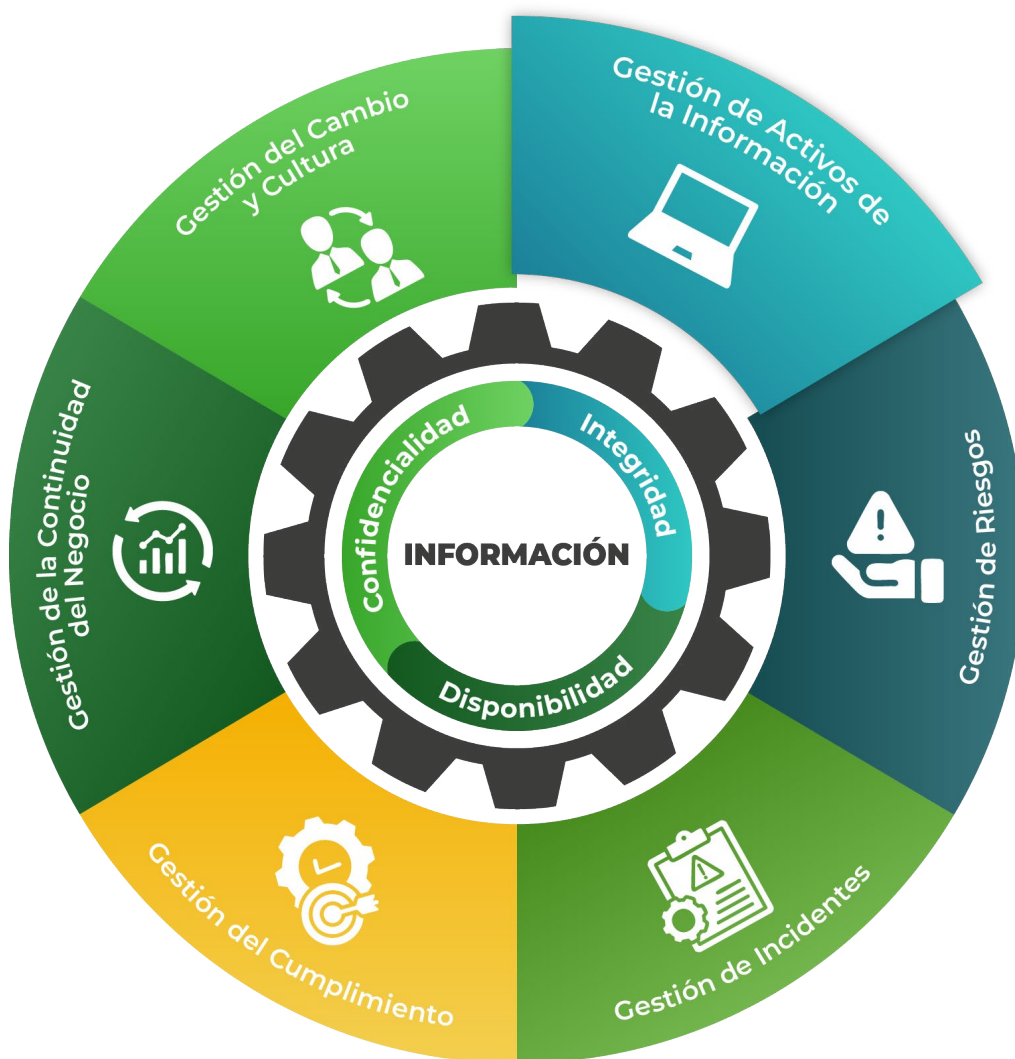
El Sistema de Gestión de Seguridad de la Información - SGSI opera a través de 6 etapas que agrupadas engranan la gestión de la estrategia de la triada de la información:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**



Modelo de gestión integral de seguridad de la información

En esta etapa se requiere identificar, valorar y clasificar los activos de información más importantes para la institución.



¿Qué es un activo de información?

Un activo de información, en el contexto de un Sistema de Gestión de Seguridad de la Información y con base en la norma ISO/IEC 27001 se define como: “Cualquier información o elemento relacionado con el tratamiento de esta (Información, Hardware, Software, Servicios, Talento Humano e Instalaciones) que tenga valor para la Institución”.

Principios para resguardar los activos de información

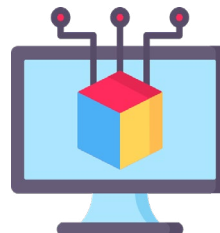


Tipos de activos de información



Tipo Información - IN:

Corresponden a este tipo datos e información almacenada físicamente o procesada electrónicamente, tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad



Tipo Software - SW:

Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la entidad y la prestación de los servicios, tales como: Software de aplicación, correo electrónico, sistema operativo, etc.



Tipo Hardware - HW:

Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la entidad, tales como: Servidores, routers, módems, Computadores (portátiles, escritorio), impresoras, Celulares Tablet, Teléfonos IP.



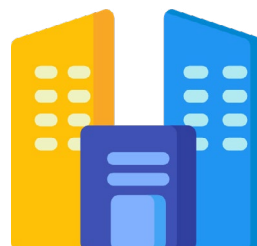
Tipo Talento Humano - TH:

Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información, Tales como: Contratistas, funcionarios, proveedores.



Tipo Servicios - SE:

Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.



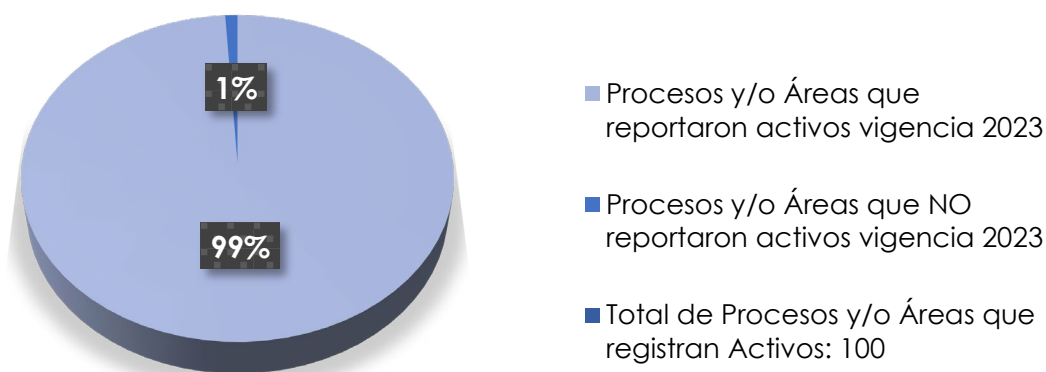
Tipo Instalaciones - IL:

Los lugares donde se almacenan o resguardan los sistemas de información y comunicaciones, tales como: Centros de cómputo, centros de cableado, Datacenter.

Resultados del Registro de Activos de la Información - Vigencia 2023

Estadísticas Registro de Activos de la Información

Registro de activos de la información - Vigencia 2023



100 Áreas habilitadas para el Registro de Activos de la Información.

99 Áreas realizaron el Registro de Activos de la Información en los plazos establecidos

1 Área no realizó el “Registro de Activos de la Información” (**Programa de Ingeniería Ambiental - Seccional Girardot**)

ACTIVOS DE LA INFORMACIÓN			
Aprobados	Aprobados, No Publicar	No Aplica	Total
3702	31	172	3905
94,8%	0,8%	4,4%	

Reporte del consolidado de activos de informacion vigencia 2023

Informe Registro de Activos de Información Vigencia 2023 "Índice de Información Clasificada y Reservada"

Sistema de Gestión de Seguridad de la Información <sgsi@ucundinamarca.edu.co>

Mar 31/10/2023 14:28

Para: ADRIANA ASENCIÓN TORRES ESPITIA <aatorres@ucundinamarca.edu.co>; CAROLINA GOMEZ FONTECHA <cgomezf@ucundinamarca.edu.co>

CC: DIRECCIÓN DE PLANEACIÓN INSTITUCIONAL <planeacion@ucundinamarca.edu.co>; CONTROL INTERNO UDEC <controlinterno@ucundinamarca.edu.co>

4 archivos adjuntos (3 MB)

ESG-SSI-F034_V1 CONSOLIDADO DE ACTIVOS DE LA INFORMACIÓN VIGENCIA 2023 1.xlsx; ESG-SSI-F034_V1 CONSOLIDADO DE ACTIVOS DE LA INFORMACIÓN VIGENCIA 2023 - INF. PÚBLICA 1.xlsx; ESGI-SSI-F034_V1 CONSOLIDADO DE ACTIVOS DE LA INFORMACIÓN VIGENCIA 2023 - INF. PÚBLICA CLASIFICADA O RESERVADA 1.xlsx; Consolidados Activos de Información 2023.rar;

13.1

Fusagasugá, 2023-10-31

Doctora

ADRIANA ASENCIÓN TORRES ESPITIA

Directora de Planeación Institucional

Ciudad

Doctora

CAROLINA GOMEZ FONTECHA

Directora de Control Interno

Ciudad

Asunto: Informe Registro de Activos de Información Vigencia 2023 "Índice de Información Clasificada y Reservada"

Respetadas Doctoras Torres y Gómez:

En virtud, de la Ley 1712 del 2014 "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". El Sistema de Gestión de Seguridad de la Información - SGSI, informa que, de acuerdo al cronograma establecido para la gestión de activos de información a nivel institucional, se adjunta para los fines pertinentes el Informe del Registro de Activos de Información de la siguiente manera:

- Consolidado general de Activos de Información denominado "Consolidado de activos de información vigencia 2023" compuesto por un total de 3.905 activos.
- Información Pública Clasificada y Reservada denominado "Consolidado de activos de información – información pública" compuesto con un total de 513 activos.
- Información Pública Clasificada y Reservada denominado "Consolidado de activos de información – información pública clasificada o reservada" compuesto con un total de 236 activos.
- Consolidado de activos reportados por cada uno de los procesos y sus áreas de acuerdo al Modelo de Operación Digital de la institución.

De igual manera, se informa que de acuerdo a lo establecido en el procedimiento ESG-SSI-P01 Gestión de Activos de la Información, está pendiente por realizar la presentación del consolidado del inventario de los activos de la información reportados por directores de área, jefes de oficina, líderes de procesos, decanos, coordinadores de programa y directores administrativos de seccionales y extensiones, en la próxima sesión ordinaria de la Comisión de Gestión, donde se hará la socialización de lo enunciado.

Pendiente de sus comentarios y/o sugerencias.

Cordialmente,

**Dirección de Planeación
Institucional y Dirección
de Control Interno**

Cronograma de las jornadas de entrenamiento para el registro de activos de información

Estratégico

Fecha: 01 de agosto del 2024
Jornada 1: 10:00 am – 12:00 pm.
Jornada 2: 4:00 pm – 6:00 pm.

Misional

Fecha: 30 de julio del 2024
Jornada 3: 10:00 am – 12:00 pm.
Jornada 4: 4:00 pm – 6:00 pm.

Apoyo

Fecha: 05 de agosto del 2024
Jornada 5: 10:00 am – 12:00 pm.
Jornada 6: 4:00 pm – 6:00 pm.

Seguimiento

Fecha: 09 de agosto del 2024
Jornada 7: 10:00 am – 12:00 pm.

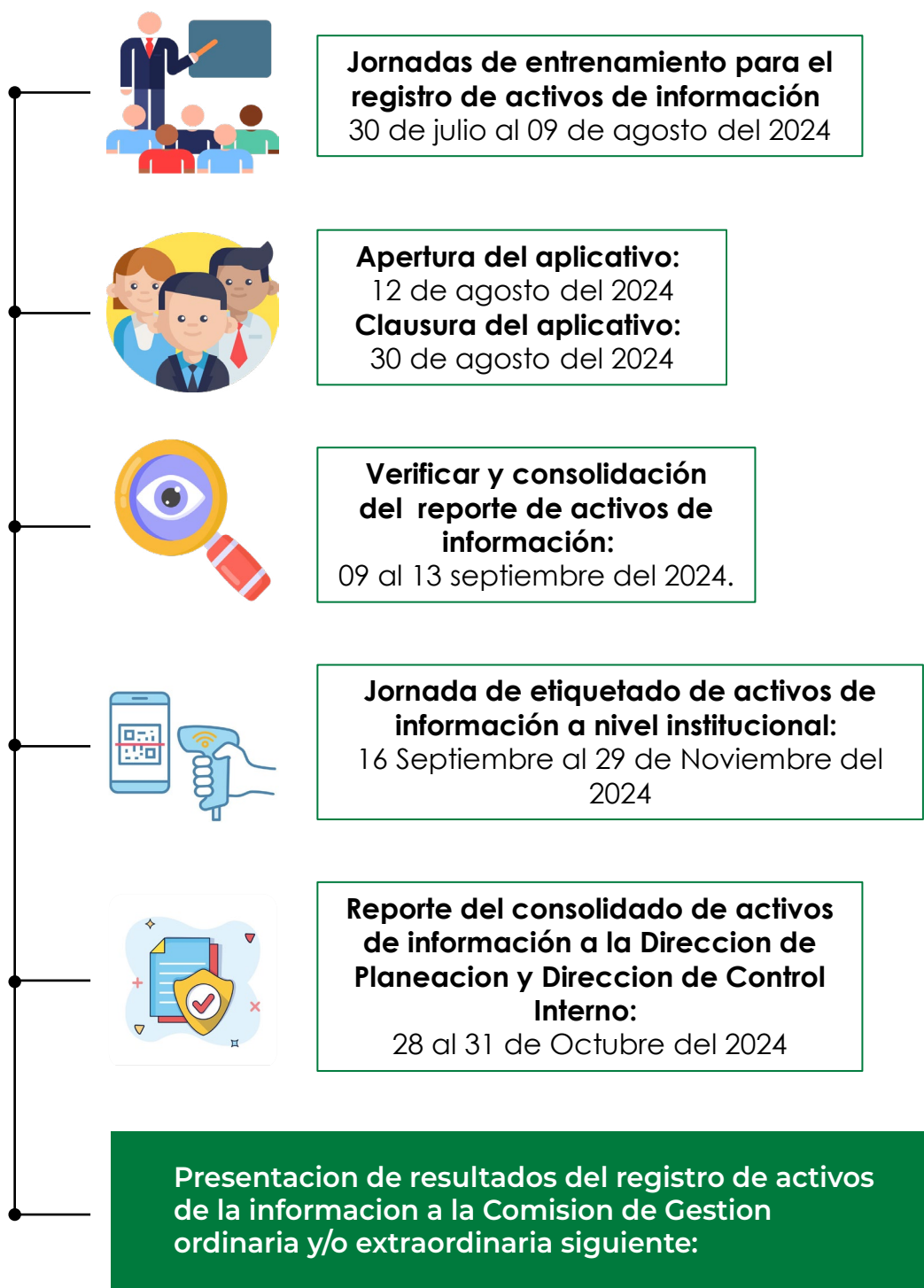
Unificado

Fecha: 09 de agosto del 2024
Jornada 8: 4:00 pm – 6:00 pm.

Virtual

Fecha: 02 de agosto del 2024
Jornada 9: 9:00 am – 11:00 am.
Jornada 10: 3:30 pm – 5:30 pm.

Actividades para el registro de activos de información



Hallazgos de la auditoría interna II del SGSI en el contexto de gestión de activos

Proceso y/o area responsable	Tipo de Hallazgo	Norma	Descripción del Hallazgo
Oficina de Desarrollo Académico Dirección de Investigación Programa de Administración de Empresas (Fusa) Oficina de Apoyo Financiero Programa Licenciatura en Ciencias Sociales (Fusa) Programa Ingeniería de Sistemas (Fusa) Unidad de Apoyo Académico Programa Ingeniería Ambiental (Girardot) Dirección de Bienestar Universitario (Girardot) Oficina de Admisiones y Registro (Girardot) Dirección Administrativa Seccional Ubaté Especialización en Gerencia para el Desarrollo Organizacional (Ubaté) Programa Contaduría Pública (Facatativá)	No Conformidad	ISO 27001:2013 Control A.8.2.1 " Clasificación de la información "	Si bien se tienen criterios de clasificación de información estos no son conocidos por los colaboradores. Divulgar los criterios y garantizar que los colaboradores los apliquen.

La **clasificación de activos** de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, de acuerdo con sus características particulares.

INFORMACIÓN PÚBLICA RESERVADA (ALTA)

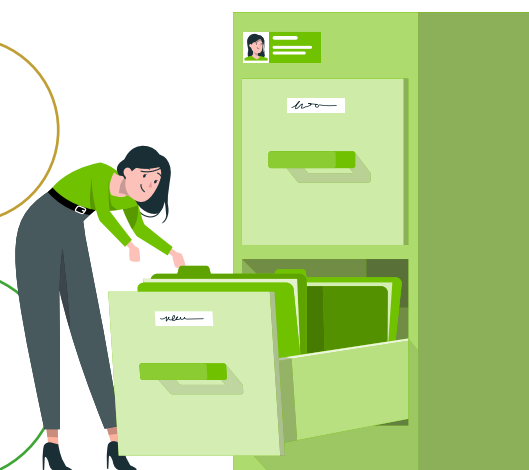
Información disponible sólo para un proceso de la entidad.

INFORMACIÓN PÚBLICA CLASIFICADA (MEDIA)

Información disponible para todos los procesos de la entidad.

INFORMACIÓN PÚBLICA (BAJA)

Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad.



Hallazgos de la auditoría interna II del sgsi en el contexto de gestión de activos

Proceso y/o area responsable	Tipo de Hallazgo	Norma	Descripción del Hallazgo
Sistema de Gestión de Seguridad de la Información - SGSI	No Conformidad	ISO 27001:2013 Control A.8.2.1 Etiquetad o de información.	No se evidenció aplicación de lineamientos para el etiquetado de información.

Activo Tipo Instalación



Activo Tipo Talento Humano



Activo Tipo Hardware



Activo Tipo Información

	MACROPROCESO DE APOYO	CÓDIGO: ADOF006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 7
	MODELO INFORMES	VIGENCIA: 2022-04-07
		PAGINA: 1 de 2

[INFORMACION PÚBLICA]	
	Diagonal 19 No. 20-29 Fusagasugá - Cundinamarca Teléfono: (01) E-mail: info@ucundinamarca.edu.co NIT: 890.080.002-2 Documento controlado por el Sistema de Gestión de la Calidad Asegúrese que corresponde a la última versión consultando el Portal Institucional

Hallazgos de la auditoría interna II del sgsi en el contexto de gestión de activos

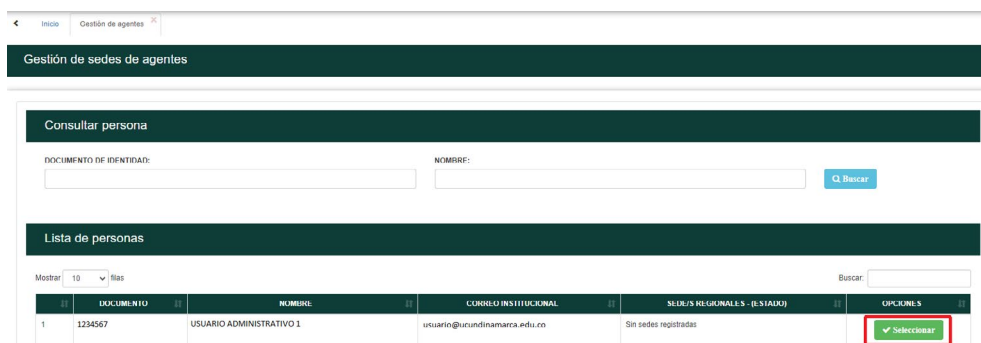
Tipo de Hallazgo	Norma	Descripción del Hallazgo
No Conformidad	ISO 27001:2013 Requisito: 8.1 Se han planificado, implementado y controlado los procesos necesarios para cumplir los requisitos y para implementar las acciones para tratar riesgos y oportunidades (6.1) Se debe implementar planes para lograr los objetivos del SGSI.	Si bien la universidad cuenta con una metodología para la gestión de riesgos, nos manifiestan que no se han levantado los activos y riesgos del proceso. Se deben identificar los activos de información del proceso. Posteriormente se deben analizar, evaluar y establecer los riesgos y planes de tratamiento para los riesgos.



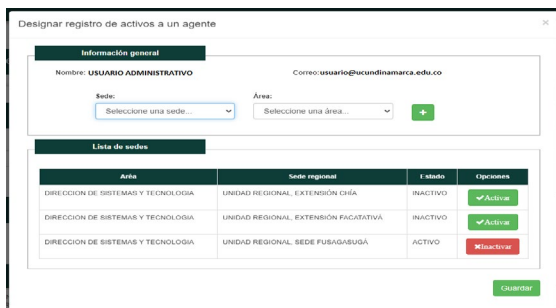
Ingreso a Plataforma Institucional



Dar clic en el Módulo Sistemas Integrados



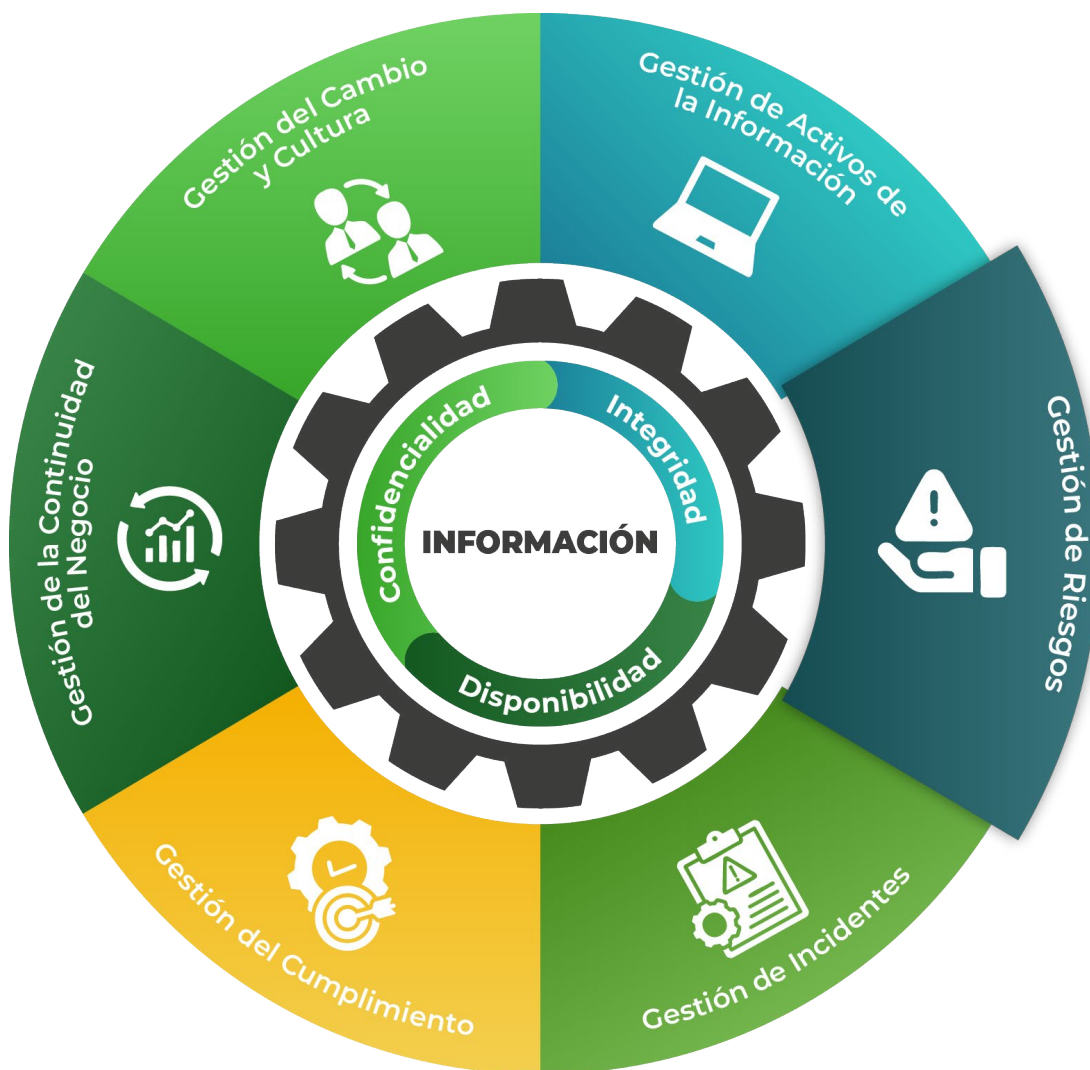
Buscar funcionario por número de documento o nombre completo y dar clic en el botón seleccionar.



En este apartado podrán seleccionar el proceso y/o área de sede, seccional y/o extensión, con el propósito de activar o inactivar la funcionalidad del registro de activos de la información al funcionario seleccionado.

Etapa 2: Gestión de Riesgos

Esta gestión es un conjunto de actividades para controlar y dirigir la identificación y administración de los riesgos de seguridad de la información, para así poder alcanzar los objetivos del negocio.



Gestión de riesgos de seguridad de la información

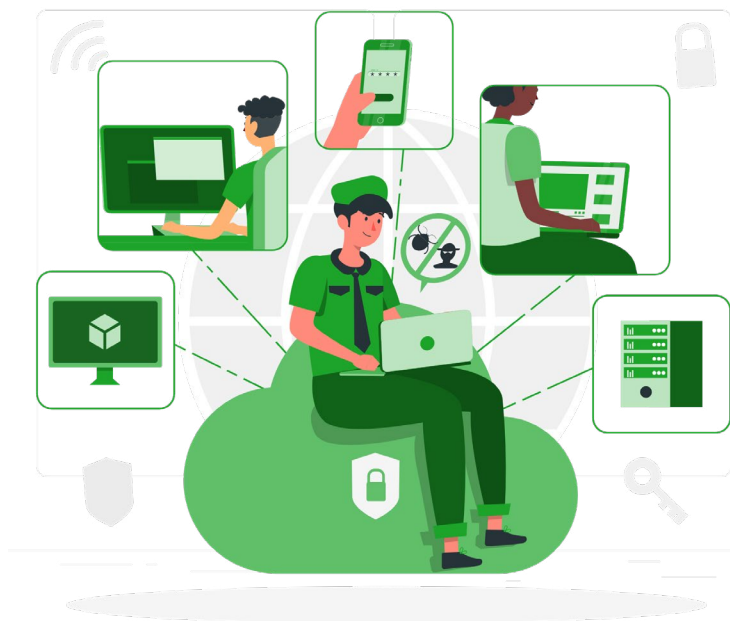
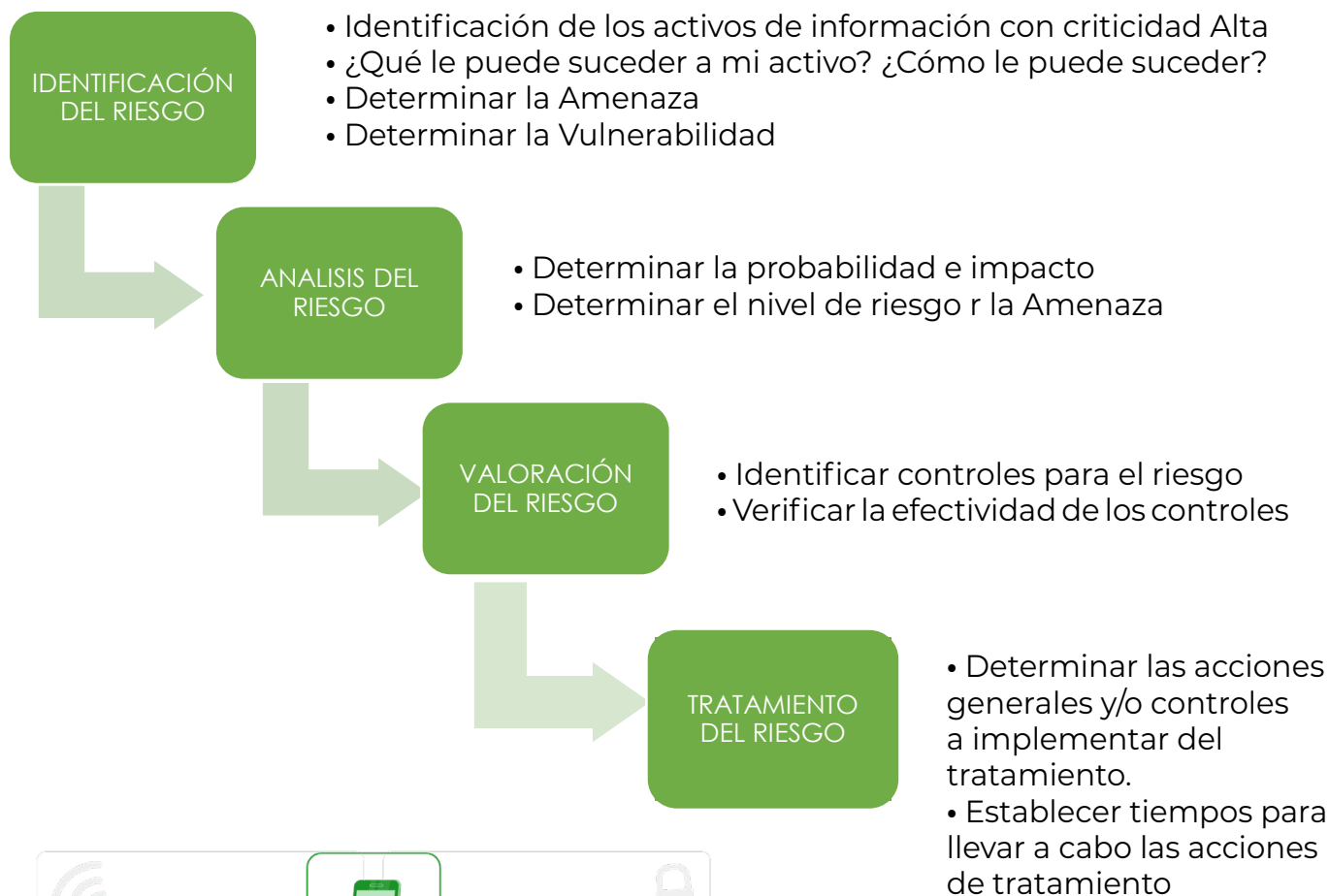
El Sistema de Gestión de Seguridad de la Información - SGSI, actualmente cuenta con el procedimiento **ESG-SSI-P12 - GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**, en donde por medio del cual se define las actividades a seguir para la gestión de riesgos de seguridad de la información en la Universidad de Cundinamarca, de acuerdo con su contexto y a lo definido en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas” del Departamento Administrativo de la Función Pública DAFP, la Guía No.7 “Gestión de Riesgos” del MinTIC y el estándar NTC/ISO/IEC 27001:2022.

¿Qué es un riesgo en seguridad de la información?

Es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias según la Norma ISO/IEC 27000.



Metodología utilizada para la gestión de riesgos de seguridad de la información



Documentos de Referencia:

ESG-SSI-M009 – Manual de Administración de Riesgos de Seguridad y Privacidad de la Información.

ESG-SSI-F039 - MATRIZ DE RIESGOS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Hallazgos encontrados para la gestión de riesgos en la auditoría interna ii

Durante el proceso de **Auditoría Interna II del Sistema de Gestión de Seguridad de la Información**, realizado en el primer semestre de 2024, se identificó la siguiente No Conformidad en 4 procesos y/o áreas de la Universidad de Cundinamarca, la cual se evidencia a continuación:

Proceso y/o área responsable	Tipo de Hallazgo	Norma	Descripción del Hallazgo
Sistema de Gestión de Seguridad de la Información - SGSI *	No Conformidad	ISO 27001:2013 Requisito 6.1.2 "Valoración de riesgos de seguridad de la información"	En la matriz de riesgos, solo es posible relacionar y evaluar un control por riesgo; lo cual no permite relacionar los controles transversales y otros controles aplicados; además genera imprecisión en la evaluación de efectividad del control, pues hay controles identificados como semiautomáticos, pero corresponden a dos controles uno manual y otro automático.

* El Sistema de Gestión de Seguridad de la Información – SGSI, atenderá este hallazgo por ser de su competencia. Valoración de Riesgos de Seguridad de la Información 6.1.2.



Jornadas de entrenamiento de las matrices de riesgos de seguridad de la información - primer semestre del 2024

El Sistema de Gestión de Seguridad de la Información - SGSI, construyó de manera concertada con los diferentes procesos y/áreas que conforman el Modelo de Operación digital de la Universidad de Cundinamarca, las matrices de riesgos de seguridad de la información a partir de los activos de información reportados en la vigencia 2023, las cuales fueron socializadas entre los días 25 de abril al 22 de julio del 2024, como se evidencia a continuación:

PROCESOS	ÁREAS	FECHA DE SOCIALIZACIÓN
Autoevaluación y Acreditación	Dirección de Autoevaluación y Acreditación	18 de junio del 2024
Comunicaciones	Oficina Asesora de Comunicaciones	21 de mayo del 2024
Planeación Institucional	Dirección de Planeación Institucional	04 de Junio del 2024
	Seccional Ubaté	10 de mayo del 2024
	Seccional Girardot	7 de mayo del 2024
	Extensión Chía	7 de mayo del 2024
	Extensión Facatativá	10 de mayo del 2024
	Extensión Soacha	
	Extensión Zipaquirá	31 de mayo del 2024
Proyectos Especiales y Relaciones Interinstitucionales	Dirección Proyectos Especiales y Relaciones Interinstitucionales	20 de mayo del 2024
Calidad	Sistemas Integrados - SGC	4 de junio del 2024
Seguridad de la Información	Sistemas Integrados - SGSI	23 de mayo del 2024
Ambiental	Sistemas Integrados - SGA	
Seguridad y Salud en el Trabajo	Sistemas Integrados - SST	11 de junio del 2024



Jornadas de entrenamiento de las matrices de riesgos de seguridad de la información

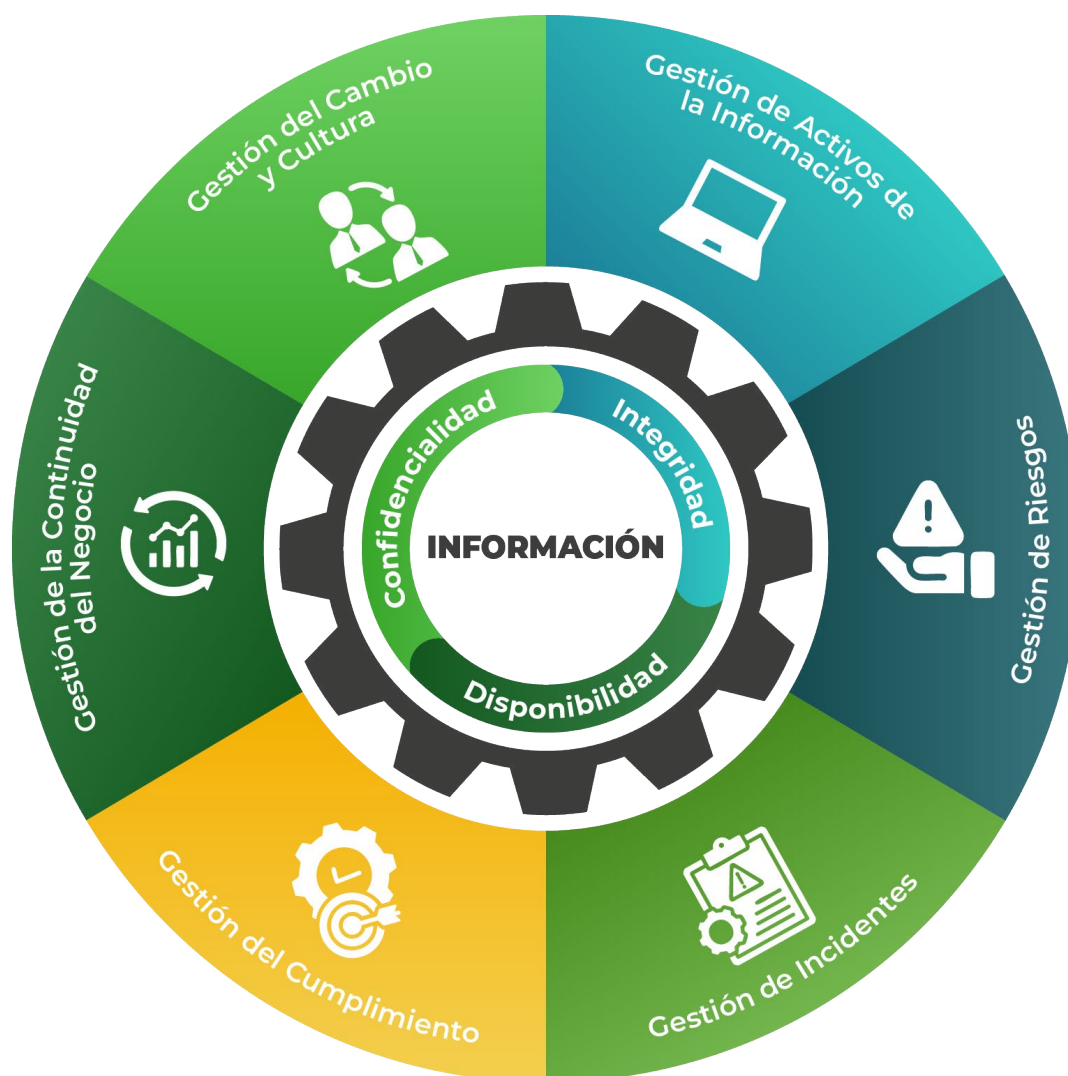
PROCESOS	ÁREAS	FECHA DE SOCIALIZACIÓN
Admisiones y registro	Oficina de Admisiones y Registro	27 de mayo del 2024
Bienestar Universitario	Dirección de Bienestar Universitario	
Ciencia Tecnología e Innovación	Dirección de Investigación Universitaria	12 de junio del 2024
Dialogando con el Mundo	Oficina Dialogando con el Mundo	23 de mayo del 2024
Formación y Aprendizaje	Facultad de Ingeniería	4 de julio del 2024
	Facultad de Ciencias del Deporte y la Educación Física	
	Facultad de Ciencias Administrativas, Económicas y Contables	21 de junio del 2024
	Facultad de Educación	
	Facultad de Ciencias de la Salud	12 de junio del 2024
	Facultad de Ciencias Sociales, Humanidades y Ciencias Políticas	
	Facultad de Ciencias Agropecuaria	
	Centro Académico Deportivo - CAD	13 de junio del 2024
	Vicerrectoría Académica	
	Oficina de Educación Virtual y a Distancia	26 de abril del 2024
	Oficina de Desarrollo Académico	25 de abril del 2024
	Dirección de Posgrados	2 de mayo del 2024
Graduados	Oficina de Graduados	11 de junio del 2024
Interacción Social Universitario	Dirección de Interacción Universitaria	23 de mayo del 2024
Apoyo Académico	Unidad de apoyo Académico	
Talento Humano	Dirección de Talento Humano	4 junio del 2024

Bienes y Servicios	Dirección de Bienes y Servicios	
	Oficina de Almacén	30 de abril del 2024
	Oficina de Compras	25 de abril del 2024
	Oficina de Recursos Físicos y Servicios Generales	25 de abril del 2024
Financiera	Vicerrectoría Administrativa Financiera	
	Dirección Financiera	22 de julio del 2024
	Oficina de Presupuesto	30 de abril del 2024
	Oficina de Contabilidad	31 de mayo del 2024
	Oficina de Tesorería	31 de mayo del 2024
	Oficina de Apoyo Financiero	26 de abril del 2024
Sistemas y Tecnología	Dirección de Sistemas y Tecnología	13 de junio del 2024
Documental	Archivo y Correspondencia	12 de junio del 2024
Jurídica	Dirección Jurídica	6 de Junio del 2024
Control Disciplinario	Dirección de Control Disciplinario	
Control Interno	Dirección de Control Interno	18 de julio del 2024
Servicio de atención al ciudadano	Oficina de Peticiones, Quejas y Reclamos	7 de junio del 2024

Procesos y/o áreas que se encuentran pendientes de socialización

Etapa 3: Gestión de Eventos y/o Incidentes

El objetivo principal de la Gestión de eventos y/o incidentes, es definir un proceso que permita manejar adecuadamente los eventos y/o incidentes de seguridad de la información, a través de un esquema que involucra las siguientes actividades: Preparación, Detección y análisis, contención, erradicación y recuperación y actividades post incidente.



Colombia sigue siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM

Forbes Staff | febrero 28, 2024 @ 1:02:39 pm

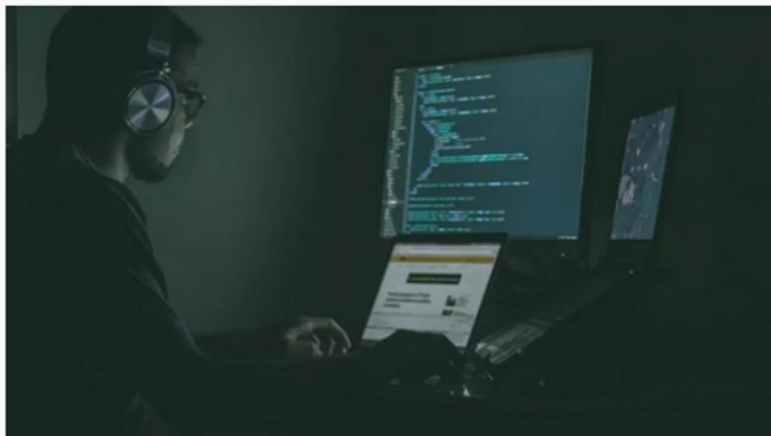


Foto: Pexels.

f América Latina enfrenta crecientes riesgos de ciberseguridad, según el Índice de Inteligencia de Amenazas 2024 de IBM.

Un reciente informe de Inteligencia de Amenazas X-Force de IBM para 2024, ha informado sobre una creciente crisis de identidad global a medida que los cibercriminales explotan cada vez más las identidades de los usuarios para comprometer empresas en todo el mundo.

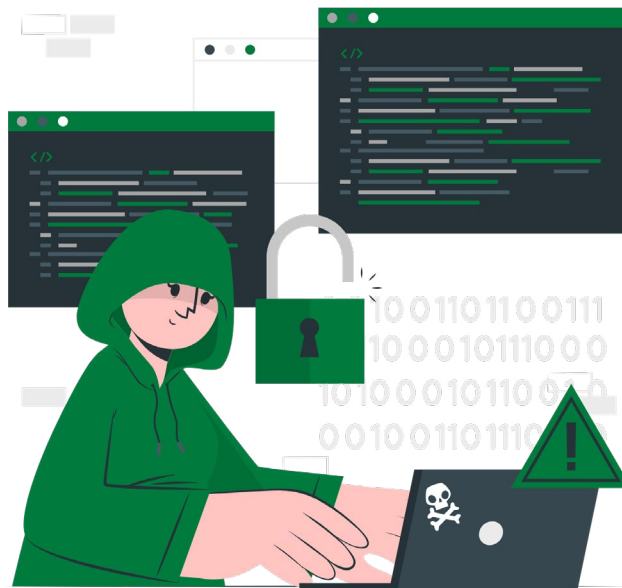
De acuerdo con ese informe, por segundo año consecutivo, Colombia se ha convertido en el país más atacado por ataques cibernéticos, con el 17% de los incidentes en la región.

El Índice de Inteligencia de Amenazas X-Force, compilado mediante el monitoreo de más de 150.000 millones de eventos de seguridad diarios en 130 países, ha destacado que el 71% de los ciberataques globales ahora se atribuyen a la explotación de identidad.

Gestión de incidentes de seguridad de la información

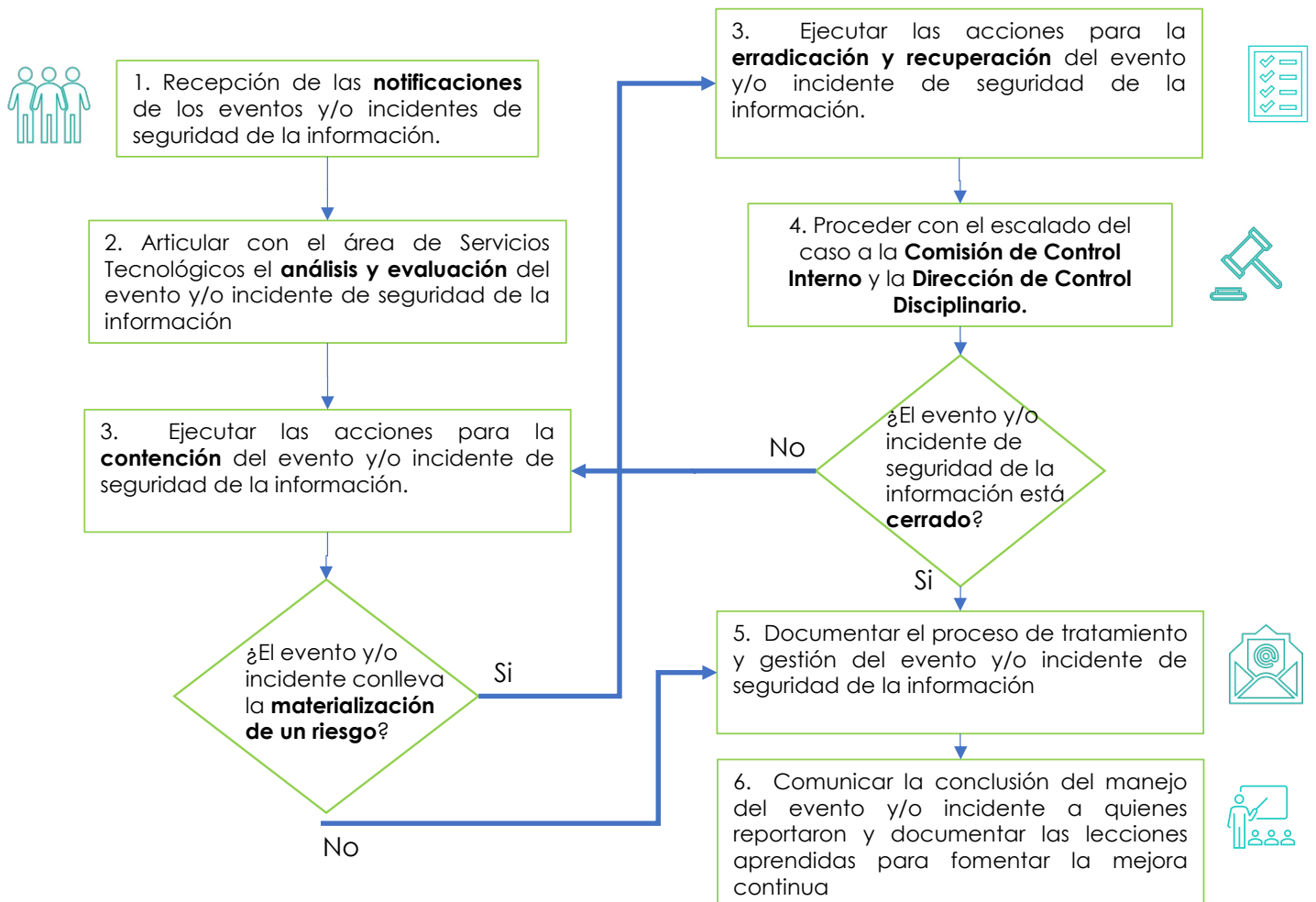
Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad de la información.

Guía No.21 para la
Gestión y Clasificación de
incidentes de Seguridad
de la Información. MinTic

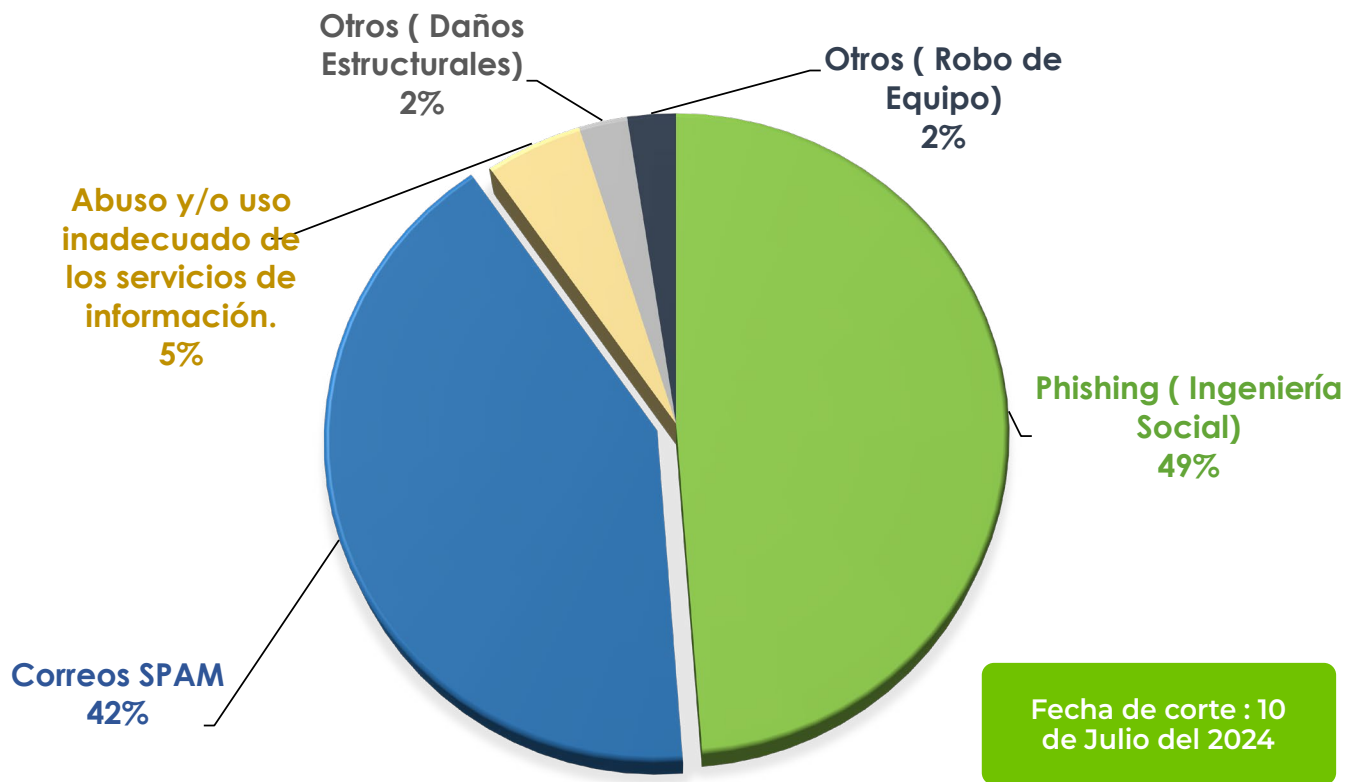


ESG-SSI-P09 Gestión de Incidentes de Seguridad de la Información

Ciclo de vida de los incidentes de seguridad de la información



Eventos y/o incidentes de seguridad de la información - vigencia 2024



Eventos y/o Incidentes de Seguridad de la Información	
Phishing (Ingeniería Social)	20
Correos SPAM	19
Abuso y/o uso inadecuado de los servicios de información.	2
Otro "Robo de Equipo" – Vandalismo en la portería.	1
Otros "Daños en la infraestructura" – Bloque D.	1
Otros "Accesos no autorizados" – WhatsApp	1
Total	44

Incidente de seguridad de la información - vigencia 2024

Verificación de autenticidad de la firma digital

	MACROPROCESO DE APOYO	CODIGO: ATHr206
	PROCESO GESTION TALENTO HUMANO	VERSION: 5
	ANEXO CONTRATACIÓN DE PERSONAL ACADÉMICO DE LA UNIVERSIDAD DE CUNDINAMARCA	VIGENCIA: 2019-05-16
		PAGINA: 4 de 4

LA UNIVERSIDAD
[Redacted]
[Redacted]

EL PERSONAL ACADÉMICO
[Redacted]
[Redacted]

EL SUPERVISOR
[Redacted]
[Redacted]

Información de error

Error al verificar la firma.

La firma contiene datos incorrectos, no reconocidos, dañados o sospechosos.
Información de soporte técnico: SigDict /Contents illegal data

[Detalles >>](#) [Aceptar](#)

Propiedades de la firma

La firma NO ES VÁLIDA.

Hora de firma: 2024/02/27 10:46:58 -05'00'

Resumen de validez

La firma no es válida porque hay errores en el formato o en la información contenida en esta firma.

El certificador especificó que se permite rellenar el formulario y agregar firmas y comentarios, pero no se permite realizar ningún otro cambio.

La identidad del firmante no se ha verificado todavía.

Viernes 10 de mayo del 2024

Un funcionario reporta al Sistema de Gestión de Seguridad de la Información – SGSI un incidente de Seguridad de la Información, por inconsistencias en firma digital.

Incumplimiento Acuerdo de Confidencialidad

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-F002
	PROCESO GESTIÓN SISTEMAS INTEGRADOS	VERSIÓN: 3
	ACUERDO DE CONFIDENCIALIDAD PARA MIEMBROS DEL TALENTO HUMANO, PASANTES Y MONITORES	VIGENCIA: 2021-12-06
		PAGINA: 6 de 8

DECIMA QUINTA. CONFIDENCIALIDAD DE INFORMACIÓN DE AUTENTICACIÓN: La UNIVERSIDAD DE CUNDINAMARCA entregará la PARTE RECEPTORA, credenciales de acceso a servicios, sistemas de información y bases de datos para uso exclusivo de acuerdo con las funciones descritas en el contrato (laboral o de prestación de servicios según sea el caso). Por tanto, la PARTE RECEPTORA se obliga a conservar en total reserva y confidencialidad estas credenciales, así como toda la información que llegare a conocer a través de los accesos que le sean habilitados. Así mismo, se obliga a reportar al Oficial de Seguridad de la Información, cuando tenga conocimiento de la ocurrencia de cualquier incidente con sus credenciales de acceso, que puedan poner en riesgo la disponibilidad, integridad y/o confidencialidad de la información a la que accede.

Incidente de seguridad de la información - vigencia 2024

Correo reportado al SGSI

De: CONTROL INTERNO UDEC <controlinterno@ucundinamarca.edu.co>
Enviado: viernes, 22 de marzo de 2024 6:13 p. m.
Para: [REDACTED]
Cc: Sistema de Gestión de Seguridad de la Información <sgsi@ucundinamarca.edu.co>
Asunto: [REDACTED]

Fusagasugá, 2024-03-22



Cordial saludo,

Una vez analizada la respuesta y soporte de justificación allegado referente a los [REDACTED] Y conforme las observaciones y comentario allegados a la Dirección de Control Interno se encuentra:

Se adquirió la [REDACTED] bajo la orden contractual [REDACTED] cuyo objeto es ADQUIRIR [REDACTED] REQUERIDOS PARA LOS F [REDACTED] Y 113 PRESENTADOS EN LA IV CONVOCATORIA INTERNA 2022-2. ESTOS PROYECTOS S [REDACTED]

El [REDACTED] solicita autorización a la [REDACTED] al argumentando que debido a la naturaleza del proyecto le exige salidas de campo a otra universidad (universidad Nacional de Colombia) y largas sesiones de escritura y edición musical y el uso simultaneo con otros programas los cuales exigen un **Pc idóneo** para tal fin, pronunciamiento realizado mediante oficio oficio (Anexo).

En respuesta la Dirección de investigaciones autorizó la [REDACTED] y uso en su computador personal para que pueda realizar la entrega de los productos compr [REDACTED] que se adquirió desde la [REDACTED] el desarrollo del mismo. Autorización que no tuvo en cuenta el cumplimiento normativo de la ley 1581 de 2012 protección de datos. Y desacatando el contenido de la acuerdo de confidencialidad de la Universidad de Cundinamarca ESG-SSI-F002 V.3 Clausula DECIMA QUINTA. CONFIDENCIALIDAD DE INFORMACIÓN DE AUTENTICACIÓN, Conllevando a un riesgo inminente en la posible pérdida custodia y protección de la información que como confidencialidad de la universidad de Cundinamarca contiene el computador personal del [REDACTED]

Viernes 22 de marzo del 2024

El 22 de marzo del 2024 llega al Sistema de Gestión de Seguridad de la Información – SGSI un reporte acerca de un incidente de Seguridad de la Información, por instalación de Software Institucional en equipo de cómputo personal.

Incumplimiento Acuerdo de Confidencialidad



MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-F002
PROCESO GESTIÓN SISTEMAS INTEGRADOS	VERSIÓN: 3
ACUERDO DE CONFIDENCIALIDAD PARA MIEMBROS DEL TALENTO HUMANO, PASANTES Y MONITORES	VIGENCIA: 2021-12-06
	PAGINA: 6 de 8

DECIMA QUINTA. CONFIDENCIALIDAD DE INFORMACIÓN DE AUTENTICACIÓN: La UNIVERSIDAD DE CUNDINAMARCA entregará la PARTE RECEPTORA, credenciales de acceso a servicios, sistemas de información y bases de datos para uso exclusivo de acuerdo con las funciones descritas en el contrato (laboral o de prestación de servicios según sea el caso). Por tanto, la PARTE RECEPTORA se obliga a conservar en total reserva y confidencialidad estas credenciales, así como toda la información que llegare a conocer a través de los accesos que le sean habilitados. Así mismo, se obliga a reportar al Oficial de Seguridad de la Información, cuando tenga conocimiento de la ocurrencia de cualquier incidente con sus credenciales de acceso, que puedan poner en riesgo la disponibilidad, integridad y/o confidencialidad de la información a la que accede.

Eventos de seguridad de la información vigencia 2024

Solicitud “Fiscalía General de la Nación”

De: Angelica Maria Avila Hoyos <angelica.avila@fiscalia.gov.co>

Enviado: viernes, 24 de mayo de 2024 9:56

Para: Vicerrectoría Administrativa y Financiera a un Clic <vicefinancieraundio@ucundinamarca.edu.co>

Asunto: ORFEO 2024840021345

Cordial saludo

Dentro del marco de las funciones asignadas a la Dirección Seccional Cundinamarca con el acostumbrado respeto me dirijo a usted para indicarle, referente al documento que antecede y que se encuentra adjunto, recibido de la subdirección de gestión documental identificado con TRD como CONSECUTIVOS DE CORRESPONDENCIA, procedo a remitir.

PRUEBA ELECTRÓNICA: Artículo 5. Ley 527 de 1999. Sobre el reconocimiento jurídico de los mensajes de datos. Corte Suprema de Justicia – Sala de Casación Penal. Sentencia de Tutela No. Interno 103902 del 9 de abril de 2019, sobre notificaciones judiciales hechas por medios electrónicos: “si bien es cierto no obra constancia de acuso de recibido del mensaje electrónico enviado... también lo es que tampoco obra motivo para considerar que no llegó a su destino, puesto que el mensaje no fue devuelto o revotado, lo cual permitió a la sala deducir que el procedimiento de notificación se surtió en debida forma.

Cordialmente,

ANGÉLICA MARÍA ÁVILA HOYOS

Dependencia de PQRS

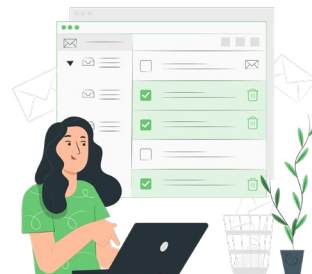
Dirección Seccional Cundinamarca

Fiscalía General de la Nación

Calle 17ª No 650-65 Piso 3 – Zona Industrial Montevideo



Cuidemos del medio ambiente. Por favor no imprima este e-mail si no es necesario.



¡ No todos los correos son sospechosos !

Suscripción “El Tiempo”

¡Bienvenido,

Has registrado tus datos en eltiempo.com

Te damos la bienvenida a **EL TIEMPO DIGITAL** como usuario registrado. A partir de este momento podrás acceder a más contenidos que los que disfrutas actualmente. Los podrás consultar en diferentes formatos multimedia, en cualquier momento y lugar.

Además, por ser usuario registrado podrás:



Compartir nuestros contenidos en redes y guardarlos para leerlos en el momento que quieras.

EMPEZAR



Suscribirte a 7 boletines que puedes activar según tus preferencias.

INSCRIBIRSE

¡ No enlazar el correo institucional con asuntos externos a lo académico y/o laboral !

SPAM “Davivienda”

De: Davivienda <ovedas@beneficos.davivienda.com>

Enviado: miércoles, 3 de julio de 2024 12:15

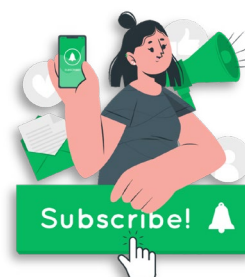
Para: LILIANA MILENA CASTRO BASTIDAS <liamcastro@ucundinamarca.edu.co>

Asunto: Queremos que su empresa siempre esté protegida

Si no puede visualizar correctamente este correo, haga clic aquí



Algunos correos se catalogan como “SPAM”

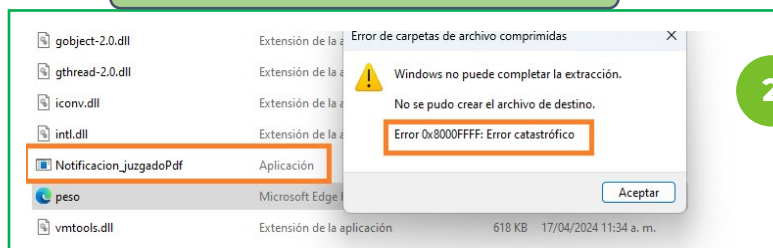


Caso de phishing “notificación del juzgado”

Correo reportado el 23 de mayo del 2024 al Sistema de Gestión de Seguridad de la Información - SGSI



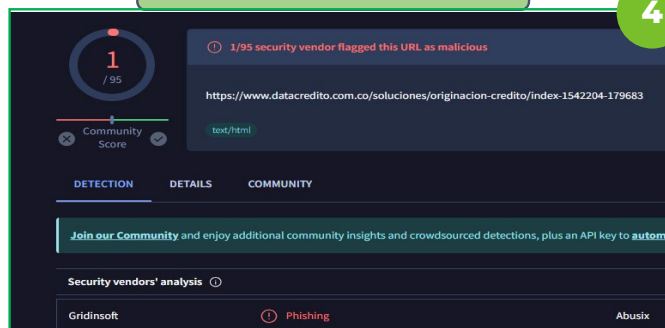
Análisis del archivo adjunto



Correos institucionales afectados (16)

Remitente	Destinatario	Asunto
desarrollosocial@guasca-cundinamarca.gov.co	direccionisu@ucundinamarca.edu.co	JUZGADO PENAL NUMERO 8 DE LA FISCALÍA...
desarrollosocial@guasca-cundinamarca.gov.co	interaccionuniversitaria@ucundinamarca.edu.co	JUZGADO PENAL NUMERO 8 DE LA FISCALÍA...
desarrollosocial@guasca-cundinamarca.gov.co	info@ucundinamarca.edu.co	JUZGADO PENAL NUMERO 8 DE LA FISCALÍA...
desarrollosocial@guasca-cundinamarca.gov.co	yrgonzalez@ucundinamarca.edu.co	JUZGADO PENAL NUMERO 8 DE LA FISCALÍA...
desarrollosocial@guasca-cundinamarca.gov.co	viceacademica@ucundinamarca.edu.co	JUZGADO PENAL NUMERO 8 DE LA FISCALÍA...
desarrollosocial@guasca-cundinamarca.gov.co	viceacademica_aunclic@ucundinamarca.edu.co	JUZGADO PENAL NUMERO 8 DE LA FISCALÍA...

Phishing detectado



Correo masivo informando el ataque informático



Acciones Correctivas

- Bloqueo del remitente
- Bloqueo del dominio
- Bloqueo de la dirección IP
- Registro en las bases de análisis de Microsoft
- Correo masivo informando el ataque informático

Casos de phishing y/o ingeniería social en la vigencia 2024

PHISHING DATACRÉDITO – 29 de mayo del 2024

De: DATA CREDITO EXPIRIAN <datacredito@airtm-app.awsapps.com>
Enviado el: lunes, 27 de mayo de 2024 11:40 p. m.
Para: ASPIRANTES POSTGRADOS <aspirantespostgrados@ucundinamarca.edu.co>
Asunto:

Referencia

Fecha de vencimiento

Monto

2024-0522254149-SA

PAGO INMEDIATO

\$557.551

<https://www.datacredito.com.co/soluciones/origination-credito/index-1542204-179683>



[Experian | Página no encontrada](#)

[pagenotfound](#)

www.datacredito.com.co

PHISHING FACTURA ELECTRÓNICA- 01 de julio del 2024

De: N°7568 <hiccug678@gmail.com>
Enviado: lunes, 1 de julio de 2024 4:55 p. m.
Para: Juan de Jesús Rojas Ramírez <jrojas@ucundinamarca.edu.co>
Asunto: S.FACTURA.

Tu archivo está disponible para pago,
descargue su factura para obtener más detalles.

Estimado.

Información del emisor

Fecha: [01/07/2024]

Razón Social: Sector Facturación y Facturación

Autenticación: 109409

Importe Pendiente: \$ 756.09

Tu archivo está disponible para pago, descargue su factura para
obtener más detalles sobre su factura.

[DESCARGAR FACTURA](#)

PHISHING INTERPOL - 09 de abril del 2024

From: SERVICIO EUROPOL <hgardiol@divinomaestrodepro.edu.pe>
Sent: Tuesday, April 9, 2024 6:58:38 AM
To: policia.europol.internacional@gmail.com <policia.europol.internacional@gmail.com>
Subject: Acusación contra ti

Tras una incautación por ciberinfiltración en su servidor, usted se ve sometido a varios procedimientos judiciales.

En este caso, su expediente también se enviará a las asociaciones antipedofilia y a los medios de comunicación para su publicación.

Número de teléfono :

* Envíe su respuesta a la dirección de correo electrónico de la Brigada que figura más abajo:
policia.europol.internacional@gmail.com

Documentos que debe adjuntar a su respuesta INTERPOL | Organización Internacional de Policía Criminal
- Documento de identidad



PHISHING BANCOLOMBIA – 31 de mayo del 2024

De: Alertas y Notificaciones <angeluzk@hotmail.com>
Enviado: viernes, 31 de mayo de 2024 15:42
Para: MARÍA NATALI URIBE RODRÍGUEZ <muribe@ucundinamarca.edu.co>
Asunto: Alertas y Notificaciones

Bancolombia | Informa

Suscripción Exitosa N°- 71263**

Estimado(a) Cliente: muribe@ucundinamarca.edu.co Bancolombia le informa Suscripción exitosa en HBO Max Premium por \$128.300.00 el día 31/05/2024 T.Debito * el monto será debitado automáticamente en 24 horas desde tu App.

En caso de que no fuiste tu y quieres cancelar la compra presione el siguiente enlace:

cancelar-compra.odoo.com/

Bancolombia S.A. todos los derechos reservados

¿Qué son los vigías de seguridad de la información?

Los **vigías de seguridad de la información** son funcionarios del Sistema de Gestión de Seguridad de la Información – SGSI, que actuarán como veedores de seguridad y privacidad de la información, con un alto grado de responsabilidad y una conciencia clara frente a los principios del SGSI, serán dinamizadores de los lineamientos (políticas) institucionales de seguridad de la información y de protección de datos personales de los titulares de la Universidad de Cundinamarca, de acuerdo con la normatividad legal vigente interna y/o externa

ESG-SSI-M004 “ MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN”



Funciones de los vigías de seguridad de la información



El o los Vigías de Seguridad de la Información – SGSI, es un **rol** que tienen los funcionarios del Sistema de Gestión de Seguridad de la Información – SGSI



La participación de los vigías del SGSI es vital para dinamizar y mantener una cultura de **apropiación** de los **conceptos y lineamientos** del SGSI a nivel institucional.



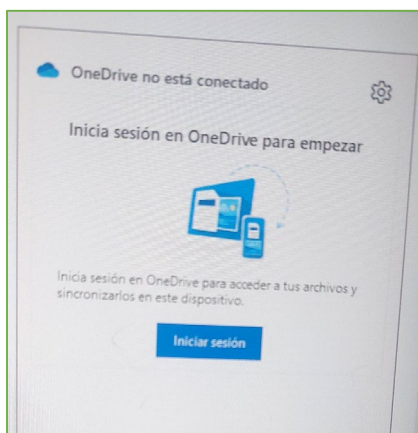
El o los vigías del SGSI, **realizan visitas** a las diferentes áreas a nivel institucional, donde de manera aleatoria **verificaran el cumplimiento** de los **lineamientos y directrices** documentadas y que deben ser comunicadas a la comunidad universitaria a través de los diferentes mecanismos de socialización



El o los Vigías de Seguridad de la Información – SGSI, **reportan los incidentes** de **seguridad de la información**, que evidencien al interior de la institución, al Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información con el fin de realizar el respectivo informe.

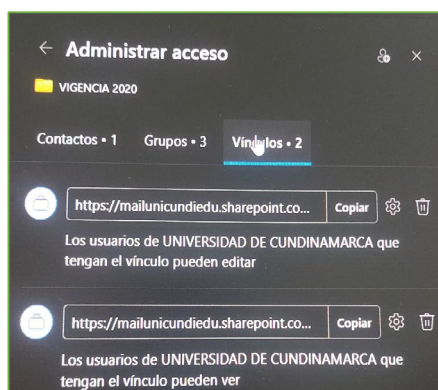


Funciones de los vigías de seguridad de la información



Equipos de cómputo
sin sincronización a
One Drive

8.13 Copia de
seguridad de la
información



Vínculos de la gestión
documental activos

8.3 Restricción de
acceso a la
información

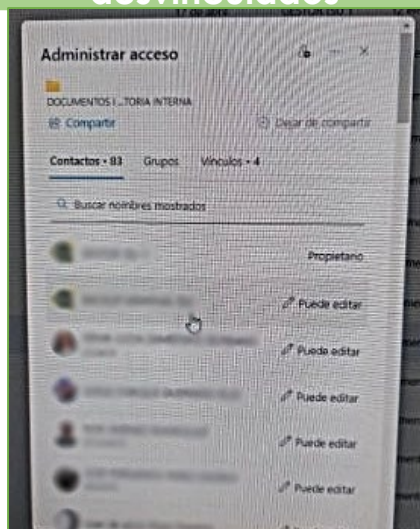
7.5 Protección contra
amenazas físicas
y ambientales

Gestión documental
sin protección



5.18 Derechos de
acceso

Derechos de acceso de
la gestión documental a
funcionarios
desvinculados



Cronograma de visitas de vigía de seguridad de la información vigencia 2024

Visitas del Rol de Vigías de Seguridad de la Información			
Programadas	7	Atendidas	
		No Atendidas	
Total			

Lineamientos Verificados

- Tratamiento de datos personales
- Tratamiento de datos sensibles
- Uso adecuado de correo institucional
- Manual de roles y responsabilidades
- Manual escritorio limpio y pantallas limpia
- Gestión de Activos de la Información
- Control de acceso físico a áreas seguras.
- Respaldo de la Información
- Revisión de derechos de acceso a la información
- Contacto por mensajería electrónica

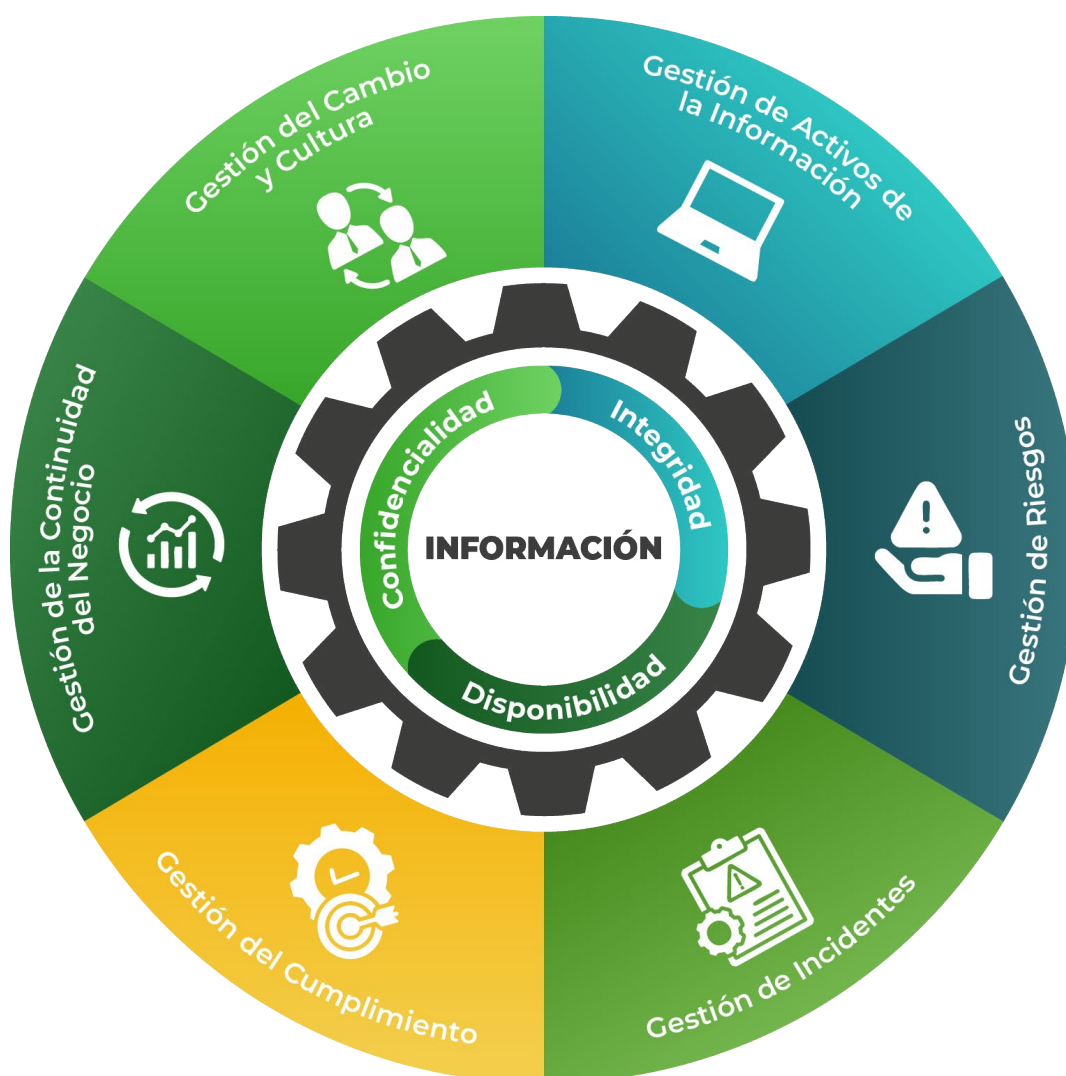
Documento de Referencia: **ESG-SSI-F035**

Reporte de verificación

PROCESO	ÁREA / OFICINA	FECHA DE VERIFICACIÓN
Gestión Documental	Oficina de Archivo y Correspondencia	2024-07-24
Dirección de Sistemas y Tecnología	Área de Servicios Tecnológicos	2024-07-24
Dirección de Bienes y Servicios	Oficina de Compras	2024-08-XX
	Oficina de Almacén	2024-08-XX
Sistemas Integrados de Gestión	Sistema de Gestión de Seguridad y Salud en el Trabajo - SST.	2024-07-17
Dirección Financiera	Oficina de Contabilidad	2024-07-17
Apoyo Académico	Unidad de Apoyo Académico	2024-07-18

Etapa 4: Gestión de Cumplimiento

La Universidad de Cundinamarca como institución pública del estado, debe asegurar el cumplimiento de la normatividad legal vigente, establecida para el tratamiento y protección de datos personales como se indica en la ley 1581 del 2012 y demás decretos reglamentarios.



Marco legal para la protección de datos personales

Constitución Política

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación

Ley 1581 de 2012

“Por la cual se dictan disposiciones generales para la protección de datos personales.”

Artículo 9º. Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

DECRETO 1377 DEL 2013

“Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.”

Capítulo II - SECCIÓN AUTORIZACIÓN
Artículo 4º. Recolección de los datos personales. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente

Marco legal para la protección de datos personales

LEY 1918 DE 2018

“Por medio de la cual se establece el régimen de Inhabilidades a quienes hayan sido condenados por delitos sexuales cometidos contra menores, se crea el registro de inhabilidades y se dictan otras disposiciones.”

ARTÍCULO 3. Registro de Inhabilidades por delitos sexuales contra menores de edad. Corresponde al Ministerio de Defensa-Policía Nacional, administrar la base de datos personales de quienes hayan sido declarados inhabilitados por delitos sexuales contra menores de edad; el Gobierno Nacional reglamentará la materia en un término inferior a 6 meses contados a partir de la vigencia de la presente ley.

Decreto 1074 del 2015

“Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo”.

Capítulo 25 – REGLAMENTA PARCIALMENTE LA LEY 1581 DE 2012 SECCIÓN 2 AUTORIZACIÓN Artículo 2.2.2.25.2.1. Recolección de los datos personales Artículo 2.2.2.25.2.2. Autorización

Decreto 090 del 2018

“Por medio de la cual se establece el régimen de Inhabilidades a quienes hayan sido condenados por delitos sexuales cometidos contra menores, se crea el registro de inhabilidades y se dictan otras disposiciones.”

ARTÍCULO 3. Registro de Inhabilidades por delitos sexuales contra menores de edad. Corresponde al Ministerio de Defensa-Policía Nacional, administrar la base de datos personales de quienes hayan sido declarados inhabilitados por delitos sexuales contra menores de edad; el Gobierno Nacional reglamentará la materia en un término inferior a 6 meses contados a partir de la vigencia de la presente ley.

Marco legal para la protección de datos personales



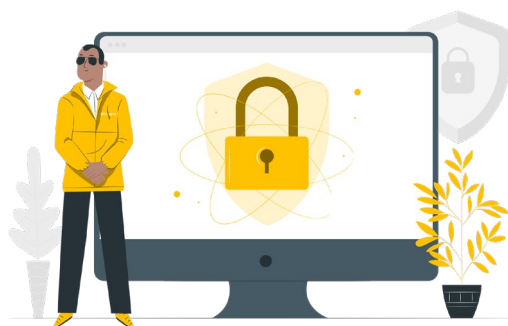
ARTÍCULO PRIMERO. ADOPTAR EL LINEAMIENTO PARA LA PROTECCIÓN DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA:

La Universidad de Cundinamarca en cumplimiento con lo dispuesto en la Ley estatutaria 1581 de 2012, el Decreto Reglamentario 1074 del 2015 y demás normatividad que tengan reacción y regulen la materia, adopta el presente lineamiento de Protección de Datos Personales, el cual será comunicado a todos los titulares.

PRINCIPIOS. Atendiendo el derecho constitucional que tienen todas las personas al conocimiento, actualización y rectificación de las informaciones que de ellas reposen en bases de datos o archivos, se dispone la implementación de los siguientes principios:

- ➡ Principio de Acceso y Circulación Restringida
- ➡ Principio de Confidencialidad
- ➡ Principio de Finalidad
- ➡ Principio de Legalidad
- ➡ Principio de Libertad
- ➡ Principio de Seguridad
- ➡ Principio de Transparencia
- ➡ Principio de Veracidad o Calidad

ALCANCE: Los principios, procedimientos y disposiciones contenidos en el presente lineamiento serán aplicables a los datos personales registrados en cualquier base de datos cuyo titular sea una persona natural que se encuentren en custodia de la Universidad de Cundinamarca, bien sea en calidad de Responsable o como Encargado del Tratamiento.



Rol de oficial de protección de datos personales

Abogado Dr. Christian Borrás Torres

  ADO001_V8
FUSAGASUGÁ
Página 1 de 1

12.
Fusagasugá, 2024 – 03 – 20

Señores
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN(SGSI)
Universidad de Cundinamarca

Asunto: Designación de Oficial de Protección de Datos

Respetuoso saludo:

De acuerdo con lo establecido en la normativa de protección de datos personales, Resolución 091 de 2023, en su artículo décimo cuarto dictamina: “OFICIAL DE PROTECCIÓN DE DATOS – El Oficial de Protección de Datos Personales, será designado por la dirección de la Universidad de Cundinamarca (...)”, y de acuerdo con la Obligación Específica 2.11: “Ejercer como Oficial de Protección Datos de la Universidad y desarrollar las obligaciones legales, normativas y reglamentarias nacionales, extranjeras” de la OPS017, por medio del presente documento, comunico oficialmente la designación del abogado **CHRISTIAN BORRAS TORRES**, identificado con la cédula de ciudadanía N° **1.136.886.191** expedida en Bogotá D.C., y portador de la Tarjeta Profesional N° **345761** del Consejo Superior de la Judicatura, como Oficial de Protección de Datos.

Lo anterior para que, el profesional ejerza las obligaciones inherentes del Oficial de Protección de Datos, responsabilizándose de desarrollar y asegurar el cumplimiento de las normativas legales, reglamentarias y contractuales en materia de protección de datos personales dentro de nuestra organización.

Cordialmente,

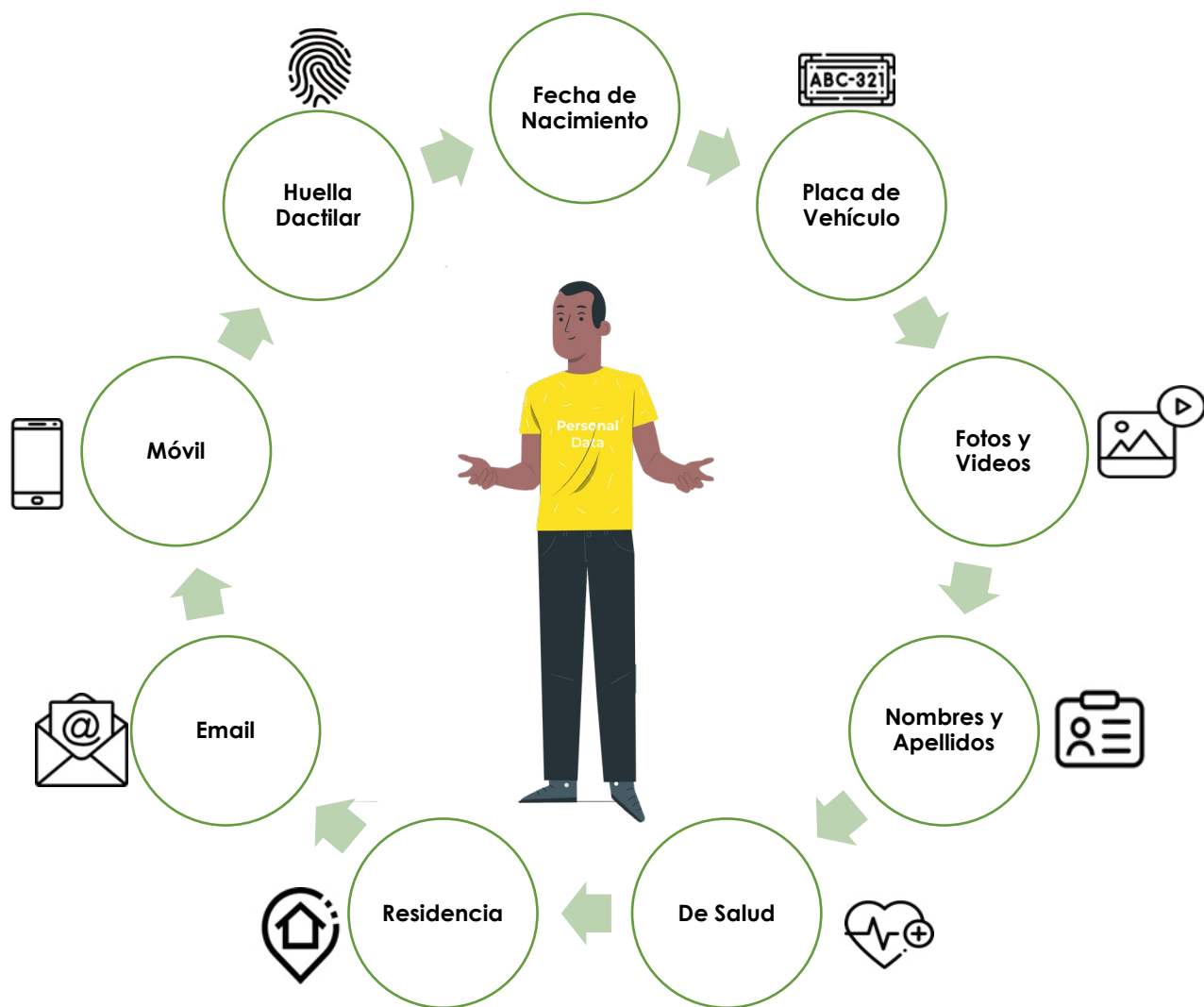

ISABEL QUINTERO URIBE
Secretaría General


JHENY LUCÍA CARDONA RICARD
Directora Jurídica

- 1 Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio – SIC
- 2 Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.
- 3 Revisar los contenidos de los contratos de transferencias internacionales de Datos personales que se suscriban con otros Responsables del Tratamiento, ubicados o no en territorio colombiano
- 4 Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio
- 5 Realizar seguimiento al Programa Integral de Gestión de Datos Personales.

Datos personales

Los Datos Personales son cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.



Semáforo de clasificación de datos personales



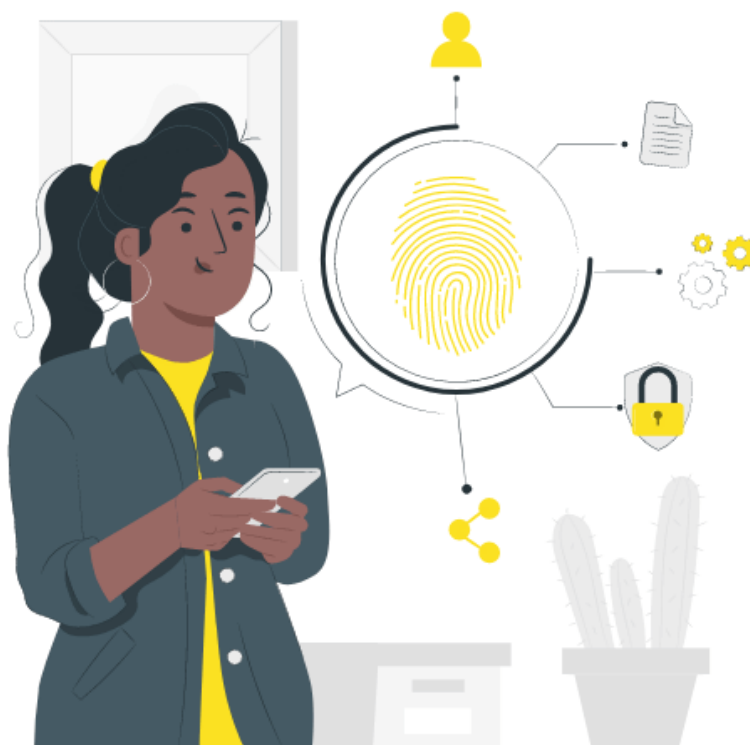
Ley 1581 de 2012

TÍTULO II PRINCIPIOS RECTORES

Artículo 4°. Principios para el Tratamiento de datos personales.

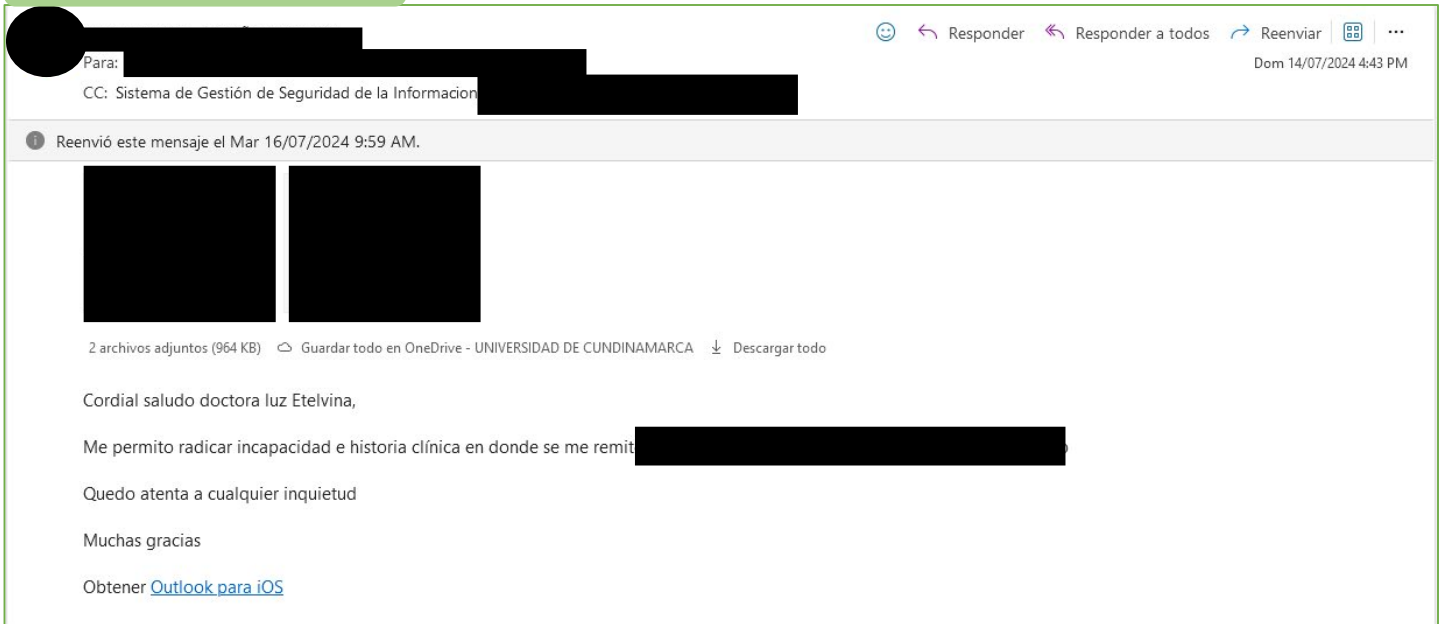
f) **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. **En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;**

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;



Ley 1581 de 2012

14 DE JULIO DEL 2024



El 14 de julio del 2024, llegó al correo del SGSI, una incapacidad medica con información sensible

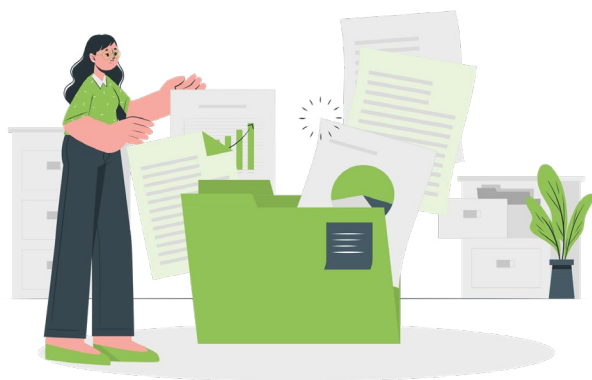


Guía de responsabilidad demostrada en el contexto del programa integral de gestión de datos personales – PIDG

La Guía para la implementación del Principio de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio – SIC es un documento que da una mayor orientación en el camino de construir un Programa Integral de Gestión de Datos Personales y se dirige a quienes estén sometidos al cumplimiento del régimen general de Protección de Datos Personales y sean vigilados por la SIC.

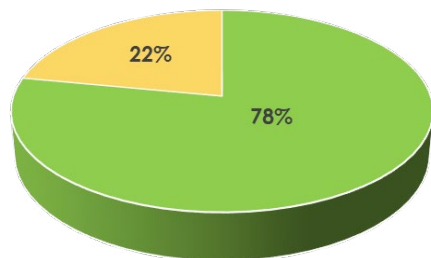
¿Qué es la Responsabilidad Demostrada o Accountability?

El principio fundamental conocido como responsabilidad demostrada hace referencia a que una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos.



Guía de responsabilidad demostrada en el contexto del programa integral de gestión de datos personales – PIDG

Promedio de Cumplimiento



■ Cumplimiento ■ Faltante

- Muy Alto (0% - 39%)
- Alto (40% - 69%)
- Medio (70% - 98%)
- Bajo (99% - 100%)

El 78% corresponde a una mirada desde la Sede Fusagasugá de la Universidad de Cundinamarca. A partir de las visitas de vigías de Seguridad de la Información en seccionales y extensiones se determinará si el porcentaje se mantiene, aumenta o disminuye.



FUNDAMENTOS BÁSICOS	REQUERIMIENTOS	CUMPLIMIENTO
Desde la alta dirección	10	95%
Oficial de protección de datos personales	19	82%
Presentación de informes	6	100%
Procedimientos operacionales	1	50%
Inventario de base de datos con información personal	15	93%
Políticas	9	83%
Sistema de administración de riesgos	7	50%
Formación y educación	4	100%
Protocolo de respuesta en el manejo de violaciones e incidentes de seguridad	6	100%
Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales	7	29%
Comunicación externa	4	100%
Plan de supervisión y revisión	2	50%
Evaluación y revisión de los controles del programa	12	83%
Promedio Ponderado		78%

Procedimientos de datos personales

ESG-SSI-PL01 - PLAN INSTITUCIONAL DE SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESG-SSI-PG01 - PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES - PIGDP

ESG-SSI-P03 – RECOLECCIÓN Y ALMACENAMIENTO DE DATOS PERSONALES

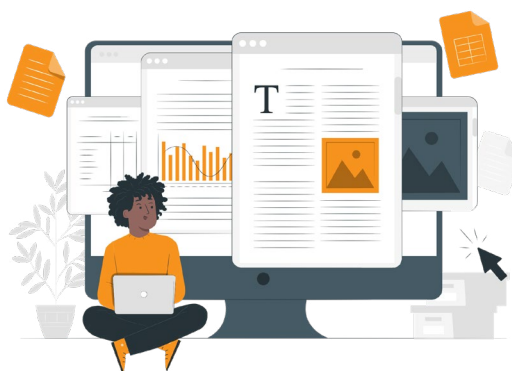
ESG-SSI-P05 - USO Y CIRCULACIÓN DE DATOS PERSONALES

ESG-SSI-P07 - TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

ESG-SSI-P13 - REGISTRO NACIONAL DE BASES DE DATOS

ESG-SSI-P15 - GESTIÓN DE DATOS PERSONALES

ESG-SSI-P16 - GESTIÓN DE RIESGOS PROTECCIÓN DE DATOS PERSONALES

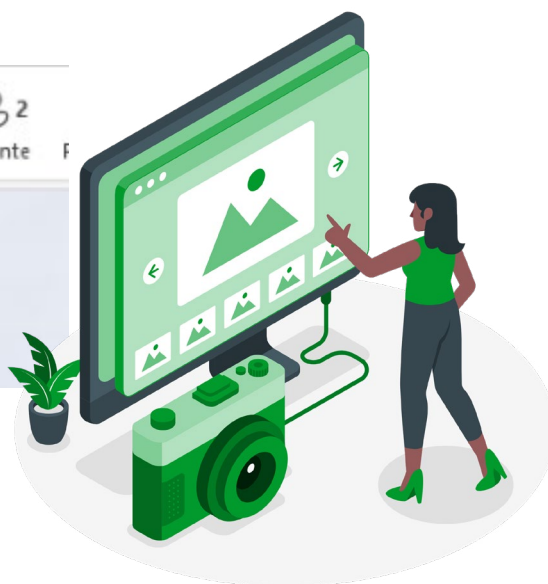
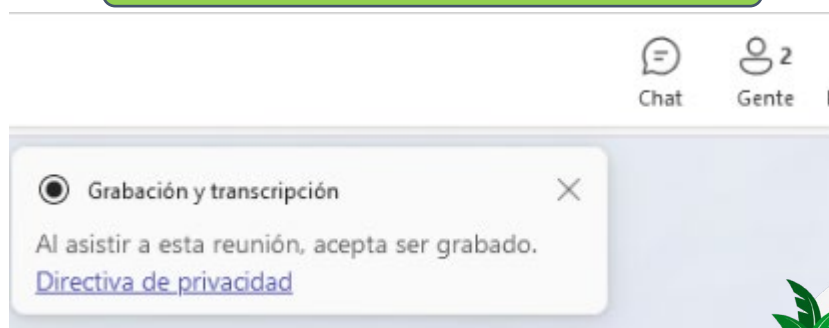


Lineamiento de protección de datos para las reuniones via teams, cuando se requiere encender cámara

FINALIDAD DOCUMENTADA
ESG-SSI-G007 "GUÍA DE
FINALIDADES PARA EL
TRATAMIENTO DE DATOS
PERSONALES DE LOS TITULARES
DE LA UNIVERSIDAD DE
CUNDINAMARCA"

Notificar vía Microsoft Teams, que con su participación autoriza realizar la grabación de la sesión, únicamente con fines académicos y/o laborales. Esta autorización incluye los derechos de imagen y voz, así como cualquier otro derecho de propiedad intelectual relacionado.

NOTIFICACIÓN MICROSOFT TEAMS



Transferencia internacional de datos personales

La Ley 1581 de 2012 en su artículo 26 prohíbe por regla general la transferencia internacional de datos personales de cualquier tipo a países que no garanticen un nivel adecuado de protección de los mismos, salvo las excepciones introducidas a esa regla.

Esta prohibición no regirá cuando se trate de:

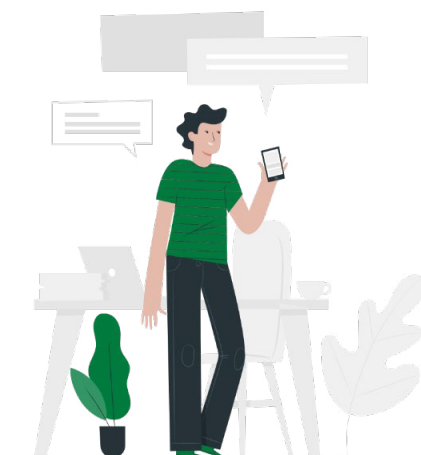
- a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;
- b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública
- c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable
- d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad
- e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular
- f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, la Ley facultó a la Superintendencia de Industria y Comercio – SIC para pronunciarse sobre las transferencias internacionales de datos mediante la Declaración de Conformidad.

ESG-SSI-P07 - TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

ESG-SSI-G003 - GUÍA PARA SOLICITAR DECLARACIÓN DE CONFORMIDAD ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

El proceso de solicitud de la Declaración de Conformidad será realizado por el Oficial de Protección de Datos Personales.



Transferencia internacional de datos personales

El día 17 de mayo de 2024 se recibió un correo desde la Oficina de Dialogando con el Mundo con el siguiente asunto “Solicitud de radicado ante la Superintendencia de Industria y Comercio del documento de transferencia internacional de datos de Brasil, Chile, Bolivia, Ecuador y Cuba.” con 6 documentos adjuntos en donde se relacionaban un enlace de SharePoint que contenía varios archivos entre ellos el ESG-SSI-F023 – SOLICITUD DECLARACIÓN DE CONFORMIDAD ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO – SIC.

Toda esta documentación fue revisada y se realizaron las observaciones pertinentes, sin embargo, no se obtuvo ninguna respuesta por parte de Dialogando con el Mundo.

Soacha, 2024-05-17

Doctora
María del Pilar Delgado Rodríguez
Universidad de Cundinamarca

Asunto: solicitud de radicado ante la Superintendencia de Industria y Comercio del documento de transferencia internacional de datos de Brasil, Chile, Bolivia, Ecuador y Cuba.

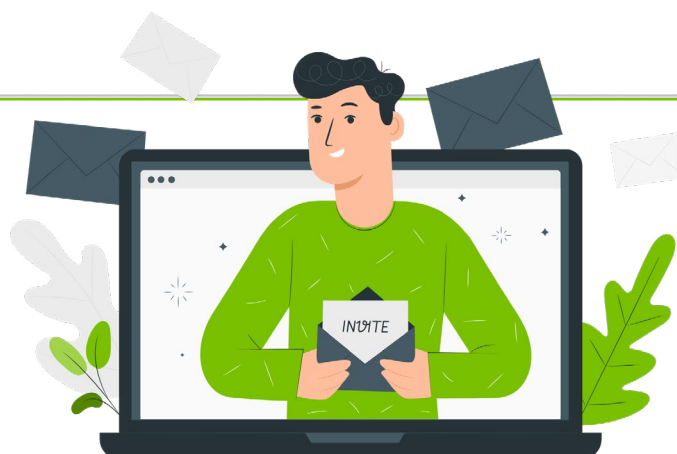
Atendiendo a la política del proceso misional Dialogando con el Mundo y al proceso de gestión de sistemas integrados en específico, al procedimiento de tratamiento de datos personales. Me permito solicitar radicar ante la Superintendencia de Industria y Comercio del documento de transferencia internacional de datos de Brasil, Chile, Bolivia, Ecuador y Cuba. Esto, como señala el Macroproceso estratégico. Proceso de gestión de sistemas integrados “versión 1, código ESG-SSI-G003, página 2 de 10” “el oficial de la oficina de tratamiento de datos quien reporte esto a la superintendencia de industria y comercio”.

Así, solicito de manera atenta realizar el reporte para los siguientes países que señala el procedimiento como son Brasil, Chile, Bolivia, Ecuador y Cuba. A continuación, reporto por país la información y documentación a radicar ante la Superintendencia de Industria y Comercio. Agradezco, remitir a través de este correo el radicado de la presente solicitud ante la Superintendencia de Industria y Comercio.

Solicito se me informe el correo al que debo habilitar para acceder a los documentos e información a reportar.

Adjunto,

- Carta general de entrega de datos y solicitud de reporte Ante superintendencia
- Carta de reporte Ante Super Intendencia país Brasil
- Carta de reporte Ante Super Intendencia país Ecuador
- Carta de reporte Ante Super Intendencia país Cuba
- Carta de reporte Ante Super Intendencia país Bolivia
- Carta de reporte Ante Super Intendencia país Chile



Registro nacional de base de datos

¿Por qué es importante registrar las bases de datos institucionales ante la Superintendencia de Industria y Comercio - SIC?



Al registrar las bases de datos ante la Superintendencia – SIC se cumple con lo establecido en la Ley 1581 de 2012 y en el Decreto 1074 de 2015, en su Capítulo 26. Además, evita sanciones para la Universidad de Cundinamarca.

Hemos cumplido a nivel institucional (100%)

Se realizó el registro de las bases de datos institucionales en la plataforma de la Superintendencia de Industria y Comercio – SIC, el día 21 de marzo de 2024 con el acompañamiento del Oficial de Protección de Datos Personales, el día 22 de marzo de 2024 fueron enviados los radicados a las áreas pertinentes por medio de correo electrónico y se entregó reporte final en la sesión ordinaria de la Comisión de Gestión del 5 de junio de 2024.

Superintendencia de Industria y Comercio - SIC?

24 Bases de Datos registradas en la SIC.

Bases de Datos Transversales:

Dirección de Talento Humano
Admisiones y Registro
Oficina de Graduados
Oficina de Compras

**RN REGISTRO NACIONAL
BD DE BASES DE DATOS**



Esg-ssi-p16 - gestión de riesgos protección de datos personales

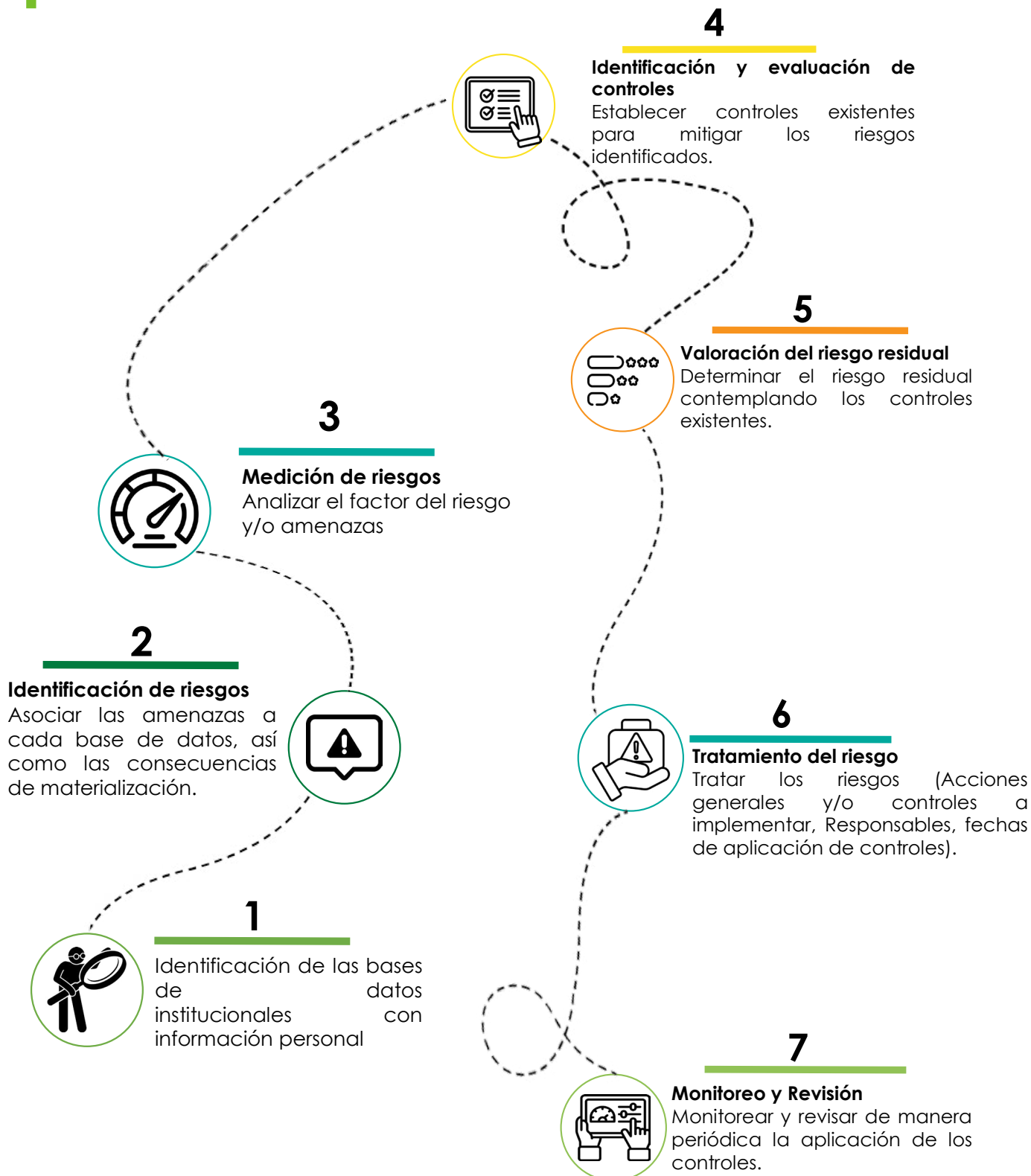
¿Qué es un Riesgo asociado a Protección de Datos Personales?

Es cualquier situación o evento que puede comprometer la confidencialidad, integridad y disponibilidad de la información personal de los titulares.



Riesgos vinculados a las bases de datos que albergan información personal de los titulares de la Universidad de Cundinamarca. Este enfoque se basará en la formulación de lineamientos y directrices que salvaguarden la privacidad de la información de los titulares. Esto se logrará mediante la identificación, evaluación, tratamiento y monitoreo de los riesgos, con el objetivo de prevenir su materialización.

Gestión de riesgos protección de datos personales

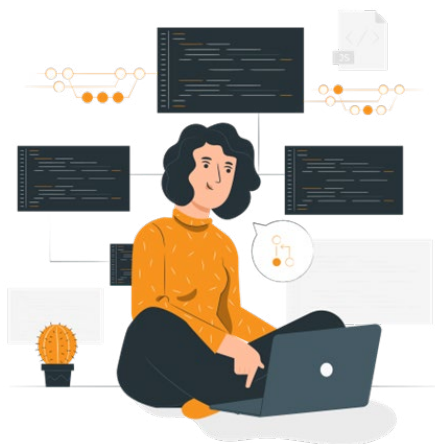


Transición a partir del nuevo lineamiento de protección de datos personales a partir del programa integral de gestión de datos personales - PIGDP

Teniendo en cuenta el Decreto 1074 de 2015 en su Artículo 2.2.2.25.2.2. Autorización “... En caso de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere a la sección 3 de este capítulo, referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos personales, los cuáles puedan afectar el contenido de la autorización, el Responsable del Tratamiento debe comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas...” y de acuerdo con el cambio de lineamiento de Protección de Datos Personales de la Universidad de Cundinamarca firmado el día 8 de agosto de 2023, se hace necesario revisar de manera general todos los componentes del Programa Integral de Gestión de Datos Personales – PIGDP, entre ellos los formatos de Autorización para el tratamiento de datos personales.

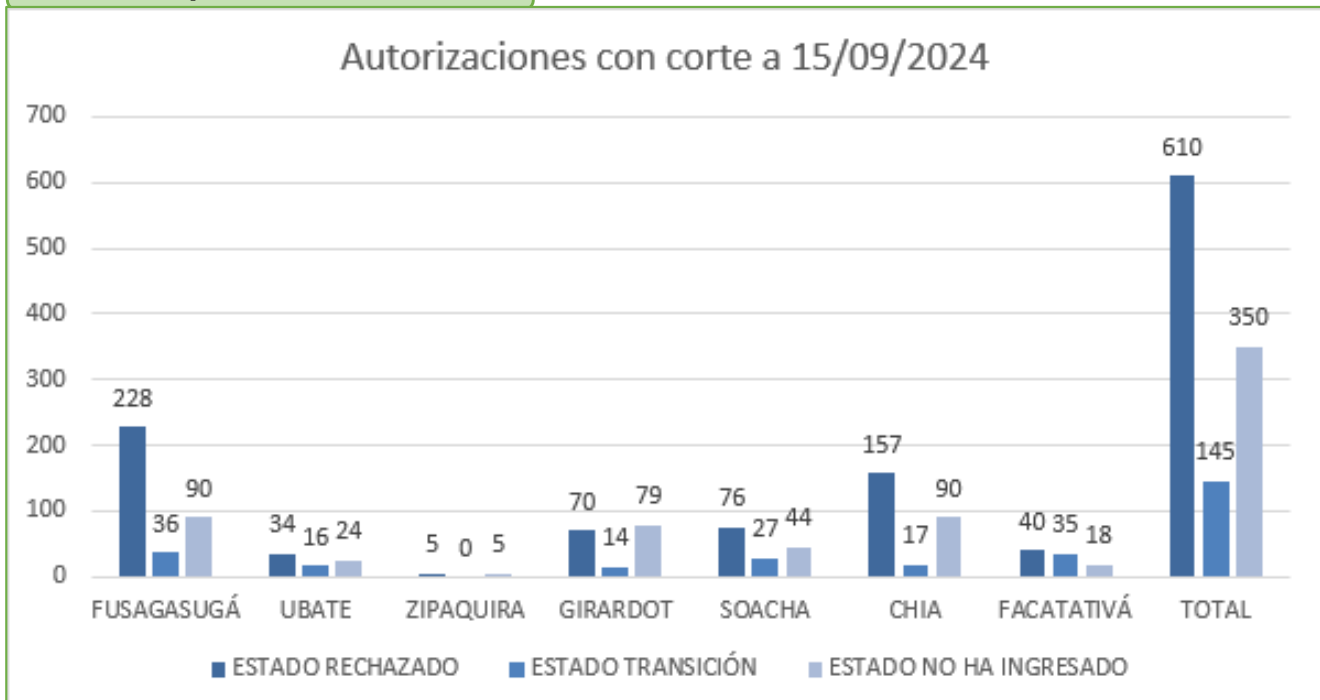
Cambios sustanciales:

- La autorización para administrativos, funcionarios y docentes será diferente a la de estudiantes mayores de edad.
- Las autorizaciones de participación de eventos académicos y/o culturales serán recopiladas en una sola.
- La autorización para graduados será eliminada teniendo en cuenta que todo el ciclo de vida de estudiante (aspirante, estudiante y graduado) se contempla dentro de la autorización de estudiante.



Gestión de autorizaciones

15 de septiembre del 2024



De acuerdo con el gráfico, en donde muestra un total de 1.105 autorizaciones en estado "Rechazado, Transición y No Aprobado"

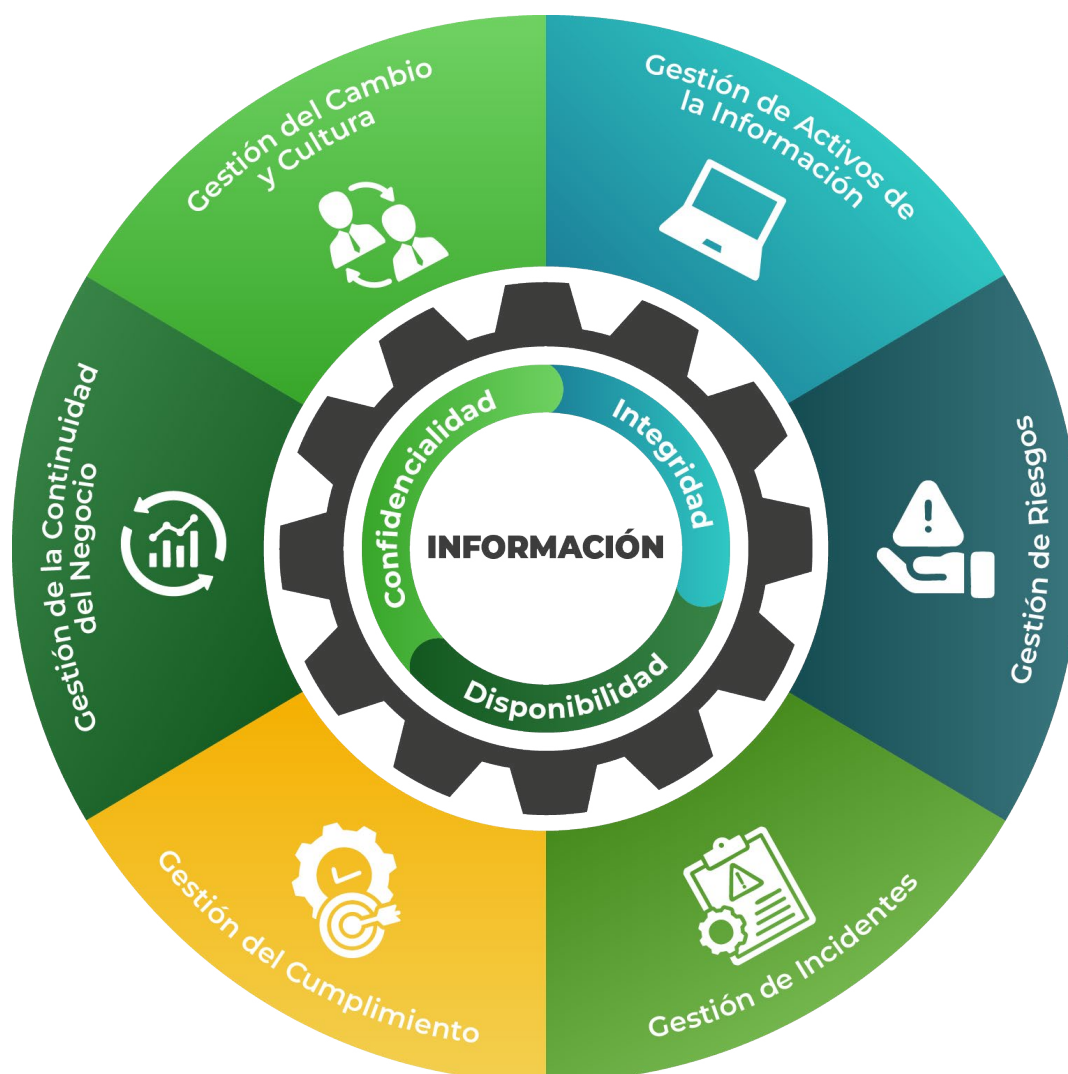


Campaña “Mis Datos Soy Yo”



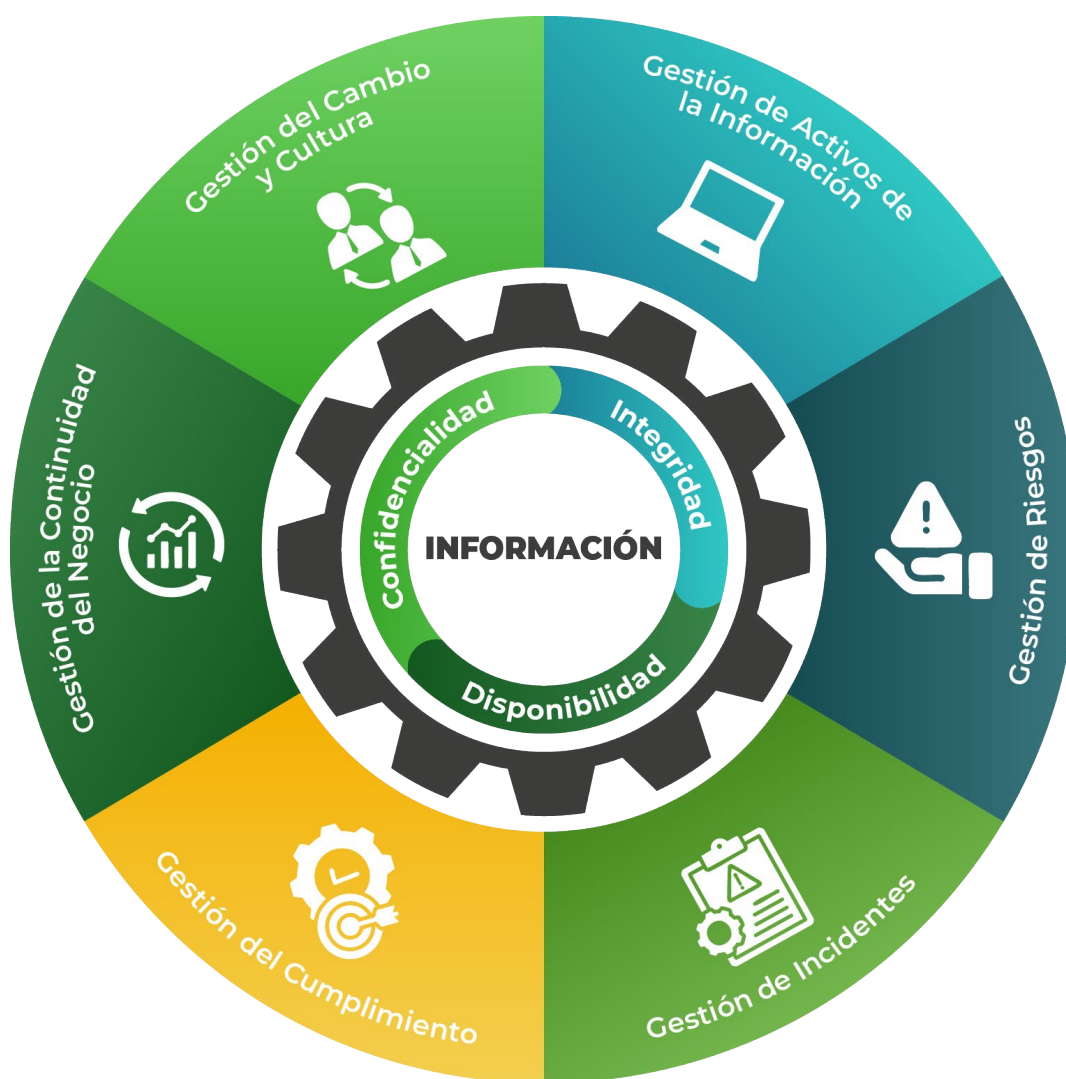
Etapa 5: Gestión de la Continuidad del Negocio

El Sistema de Gestión de Seguridad de la Información, establece los lineamientos de “Backup” o respaldo de información, de todos y cada uno de los procesos gestionados por el SGSI, con el fin resguardar la confidencialidad, integridad y disponibilidad de la información de la institución.



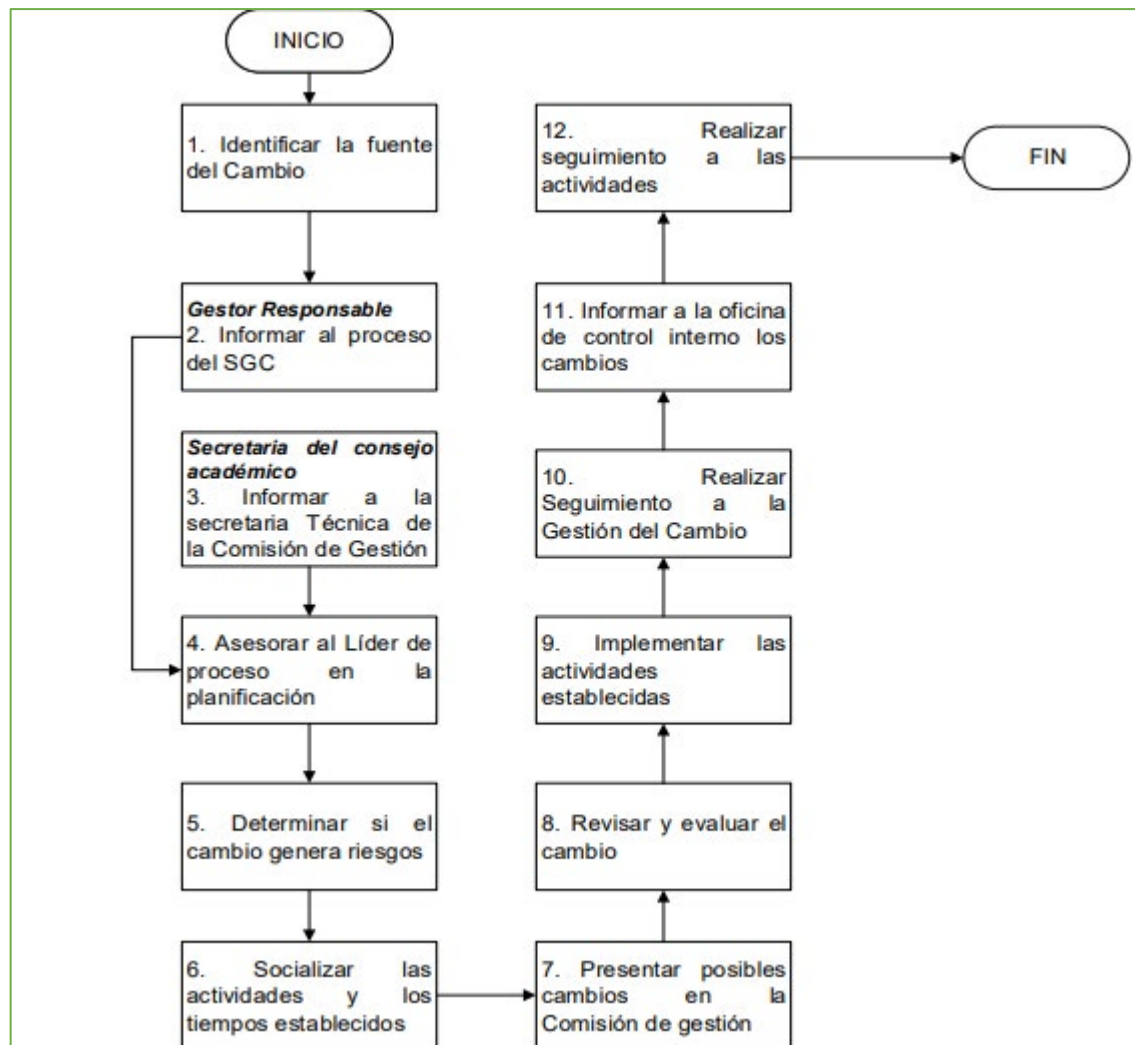
Etapa 6: Gestión del Cambio y Cultura

El Sistema de Gestión de Seguridad de la Información, establece los lineamientos de “Backup” o respaldo de información, de todos y cada uno de los procesos gestionados por el SGSI, con el fin resguardar la confidencialidad, integridad y disponibilidad de la información de la institución.



GESTION DEL CAMBIO - ESGP07

El Sistema de Gestión de Seguridad de la Información, se viene articulando con el procedimiento de Gestión del Cambio del Sistema de Gestión de Calidad



Ciberseguridad



Marco legal para la ciberseguridad

Decreto Único 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la información y las comunicaciones , adiciona el Título 21 a la Parte 2 del Libro 2



Decreto 338 de 2022 “Por medio del cual se establece los lineamientos generales para fortalecer la **gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales**, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital”

Marco legal para la ciberseguridad

Leyes

LEY 1273 DE 2009 - Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Decretos

DECRETO 338 DE 2022 “Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”

Normas ISO

NORMA ISO 27110 DE 2021 - Tecnología de la información, ciberseguridad y protección de la privacidad. Directrices para la elaboración del marco de ciberseguridad

NORMA ISO 27032 DE 2023 - Ciberseguridad. Orientación para la seguridad en internet.

Conpes

CONPES 3854 DE 2016 CONPES 3751 DE 2013

Principios de seguridad digital

1. CONFIANZA

La seguridad digital debe fomentar la confianza mediante la buena comunicación

2.COORDINACIÓN

Las actuaciones que se realicen deberán integrar de manera coordinada a las múltiples partes interesadas

3.COLABORACIÓN

ENTRE LAS MÚLTIPLES PARTES INTERESADAS. Se deben involucrar activamente a las múltiples partes interesadas

4.COOPERACIÓN.

En el marco de las relaciones nacionales e internacionales en materia de seguridad digital a través del ciberespacio

5. ENFOQUE BASADO EN LA GESTIÓN DE RIESGOS.

Para generación de confianza en el entorno digital

6. GRADUALIDAD

Desarrollo de herramientas estratégicas y operativas, para implementación gradual

7. INCLUSION

La seguridad digital debe incluir a todas las partes interesadas

8.PROPORCIONALIDAD.

Las acciones y operaciones en el ciberespacio serán proporcionales con la gestión dinámica de los riesgos derivados

9. SALVAGUARDA DE LOS DERECHOS HUMANOS Y LOS VALORES FUNDAMENTALES DE LOS CIUDADANOS

10.SALVAGUARDA DE LOS DERECHOS HUMANOS Y LOS VALORES FUNDAMENTALES DE LOS CIUDADANOS

Decreto 338 de 2022



SISTEMA DE GESTIÓN DE
SEGURIDAD
DE LA **INFORMACIÓN**
SGSI