POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Introducción

La dirección de **"NOMBRE EMPRESA…"**, entendiendo la importancia de una adecuada gestión y protección de los activos de información, y conforme a la *Resolución no. 6890 de 2022 de la Comisión de Regulación de Comunicaciones* ARTÍCULO 5.1.2.3 se compromete con la implementación del Sistema de Gestión de Seguridad de la Información siguiendo los estándares ISO/IEC 27000 como lo indica la norma, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de **"NOMBRE EMPRESA…"**.

2. Objeto

Disminuir mediante el *Sistema de Gestión de Seguridad de la Información,* el impacto generado por los riesgos identificados de manera sistemática, mediante la protección de la información basados en los tres principios de seguridad de la información: integridad, confidencialidad y disponibilidad; determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de **"NOMBRE EMPRESA…"**
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de nuestros clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de **“NOMBRE EMPRESA…”**
- Garantizar la continuidad del negocio frente a incidentes.
- **“NOMBRE EMPRESA…”** ha decidido definir, implementar, operar y mejorar de forma continua un *Sistema de Gestión de Seguridad de la Información*, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

3. Alcance

La presente política general de seguridad y privacidad de la información es de aplicación y obligado cumplimiento para todos los empleados de **“NOMBRE EMPRESA…”** así como para aprendices, practicantes, proveedores, contratistas, terceros y la ciudadanía en general.

4. GLOSARIO

- **Sistema de Gestión de Seguridad de la Información**: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Confidencialidad**: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad**: Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad**: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Controles**: Medida que permite reducir o mitigar un riesgo

5. Políticas de seguridad y privacidad de la información

Para lograr el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información, **“NOMBRE EMPRESA…”** establecen las siguientes políticas:

5.1 **“NOMBRE EMPRESA…”** definirá las responsabilidades frente a la seguridad de la información y estas serán compartidas, publicadas y

aceptadas por cada uno de los empleados, proveedores, socios de negocio y/o terceros.

5.2 **“NOMBRE EMPRESA…”** se compromete a proveer los controles de seguridad necesarios para que la información Corporativa sea accedida únicamente por los funcionarios o terceras las partes autorizadas con base en las funciones de su rol frente a los procesos formalmente definidos.

5.3 **“NOMBRE EMPRESA…”** protegerá la información generada, procesada o resguardada por los procesos del negocio, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

5.4 **“NOMBRE EMPRESA…”** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5.5 **“NOMBRE EMPRESA…”** protegerá su información de las amenazas originadas por parte del personal.

5.6 El personal administrativos y directivos de **“NOMBRE EMPRESA…”** deben conservar su escritorio limpio, ordenado y libre de información que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento. De igual manera, son responsables por la debida diligencia para prevenir el acceso no autorizado a la pantalla de su equipo, bloqueando la pantalla de su computador en los momentos que no se esté utilizando.

5.7 **“NOMBRE EMPRESA…”** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

5.8 **“NOMBRE EMPRESA…”** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

5.9 **“NOMBRE EMPRESA…”** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

5.10 **“NOMBRE EMPRESA…”** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

5.11 **“NOMBRE EMPRESA…”** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

5.12 **“NOMBRE EMPRESA…”** debe aplicar controles criptográficos, tanto en almacenamiento como en tránsito, para aquella información que en el inventario de activos de información de la Institución se encuentre clasificada como confidencial o que esté valorada con la criticidad más alta en la dimensión de integridad, haciendo uso del método criptográfico más apropiado para cada situación y utilizando en todo momento algoritmos catalogados como fuertes. Todas las llaves/claves de cifrado deben ser protegidas para evitar su divulgación no autorizada y su posible uso fraudulento posterior.

5.13 **“NOMBRE EMPRESA…”** diferenciará el uso de dispositivos móviles con fines corporativos propiedad de aquellos dispositivos propiedad del empleado. Para los primeros, se establece que la información creada, procesada, almacenada o accedida en o desde el dispositivo móvil debe contar con los controles establecidos de acuerdo con su clasificación, tal como se haría en los demás equipos de la entidad, aplicando para su protección las mismas restricciones y condiciones explícitas en las demás políticas de seguridad de la información. Para los segundos, se establece que su uso para fines corporativos está libremente permitido, excepto para aquellos casos en los cuales se pueda tener cualquier tipo de acceso desde el dispositivo móvil a información clasificada en los niveles más altos de criticidad para confidencialidad, integridad o disponibilidad.

5.14 **“NOMBRE EMPRESA…”** establece que se deben generar copias de respaldo como mínimo para todos los activos de información clasificados en el nivel alto de criticidad para la categoría de disponibilidad, aplicando una

estrategia que tenga en cuenta los puntos y tiempos de recuperación adecuados para cada tipo de información y manteniendo durante el tránsito y almacenamiento de las copias los requerimientos de seguridad establecidos para los activos originales. Se debe asegurar mediante pruebas periódicas la consistencia, integridad y capacidad de recuperación de los respaldos.

5.15 **“NOMBRE EMPRESA…”** establece que la transferencia de información, tanto interna como externa, puede realizarse solo a través de los medios definidos y suministrados para tal fin por la institución, o por un cliente o proveedor, aplicando los controles necesarios para proteger la confidencialidad, integridad y disponibilidad de los activos de la información que sean objeto de la transferencia con base en su clasificación. Para ello, previo a ser transferidos, los activos de información deben haber pasado por un procedimiento de clasificación y etiquetado de la información de **“NOMBRE EMPRESA…”**

5.16 **“NOMBRE EMPRESA…”** establece que las aplicaciones y los sistemas de información que sean desarrollados, tanto por personal interno como por proveedores, para el uso en actividades misionales de la institución, deben incluir, en el ciclo de vida del desarrollo de la aplicación, los criterios de seguridad de la información que hagan frente a las amenazas más difundidas en el entorno de las redes de datos, dependiendo de la clasificación en el inventario de activos de información de la Universidad que posean los datos que van a ser procesados, almacenados o accedidos por el sistema a desarrollar.

5.17 **“NOMBRE EMPRESA…”** establece que la relación con sus proveedores debe siempre estar definida en un acuerdo mutuo que establezca específicamente la protección de la confidencialidad, integridad y disponibilidad de los activos de información que estén involucrados en el desarrollo del servicio o producto contratado.

*5.18*Los Incidentes de seguridad de la información presentados serán identificados y almacenados en el “Reporte de información de incidentes de seguridad de la información” conforme los *numerales 5.1.2.3.2. y 5.1.2.3.3 de la Resolución no. 6890 de 2022 Comisión de Regulación de Comunicaciones.*

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de **“NOMBRE EMPRESA…”**

6. ROLES Y RESPONSABILIDADES

“NOMBRE EMPRESA…”, define los roles y responsabilidades para la implementación del *Sistema de Gestión de Seguridad de la Información* y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados:

ROL / INSTANCIA / DEPENDENCIA	**RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)**
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos). • Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.
Grupo TIC	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Grupo TIC	• Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. • Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	Gestión de Seguridad de la Información en la Entidad.
Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Talento Humano	• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. • Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad. • Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Líderes de Proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Todos los funcionarios y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

7. SANCIONES

a. Cualquier violación a las políticas de seguridad de la información de **“NOMBRE EMPRESA…”** debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

c. (Si la entidad considera agregar más factores en este punto, puede hacerlo con base a las normas, leyes y estatutos vigentes).

8. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

“NOMBRE EMPRESA…” indica que realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.

9. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la (Alta Dirección/Instancia). La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
3. Si los Incidentes de Seguridad de la información reportados y almacenados, requieren que la política sea ajustada para dar cumplimiento a la norma.

10. ANEXOS

Anexo 1 : Formato de seguimiento de incidentes “Reporte de información de incidentes de seguridad de la información”.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Nombre: Cargo: Fecha:	Nombre: Cargo: Fecha:

Anexo 1
Reporte de información de incidentes de seguridad de la información

Fecha del Reporte: Seleccione una fecha.

Datos de Contacto de la Entidad		
Nombre de la Entidad: Escriba el nombre de la entidad		
Dirección: Escriba la dirección física de la sede		**Sede:** Escriba el nombre de la sede
Sector: Escribir el nombre del sector al cual pertenece	**Ciudad:** Escriba la ciudad donde se encuentra la sede	**Departamento:** Escriba el Departamento al que pertenece la sede
Nombre de Quien Reporta: Escriba el nombre y apellidos de la persona que reporta el incidente		
Cargo: Escriba el cargo de la persona que reporta el incidente	**Número Contacto:** **Fijo:** Número Fijo. **Ext** Número de la extensión **Celular:** Número celular	
Correo Electrónico: Escriba su correo de corporativo		**Skype:** Escriba su usuario de Skype

Incidente	
Fecha y Hora del descubrimiento: Escriba la fecha y la hora de descubrimiento del incidente	**Nombre de la Persona que Detectó el Incidente:** Escriba el nombre y apellidos de la persona que detectó el incidente
Fecha y Hora de Detección: Escriba la fecha y la hora de inicio del incidente	**Nombre del administrador del Activo Informático:** Escriba el nombre y apellidos de la persona que administra el activo informático – Servidor, DB, Aplicación, Portal, etc.
Descripción Detallada: Realice una descripción detallada de lo sucedido, teniendo en cuenta los siguientes interrogantes: **Quién, Cómo, Cuándo, Dónde, Por qué y Para qué**	

Método de Detección:
Escriba como fue detectado el incidente

Acciones Realizadas:
Escriba que actividades ha realizado para contener el incidente

Acciones Pendientes:
Escriba que actividades planeadas para la contención del incidente, están pendiente de ejecutar

Clasificación del Incidente: **Seleccione la clase y tipo de incidente.**

Malware: Elija un elemento.
Disponibilidad: Elija un elemento.
Obtención de Información: Elija un elemento.
Intrusiones: Elija un elemento.
Compromiso de Información: Elija un elemento.
Fraude: Elija un elemento.
Contenido Abusivo: Elija un elemento.
Política de Seguridad: Elija un elemento.
Otros:
Escriba la clasificación del incidente, si no se encuentra en las listas desplegables

La respuesta al incidente fue efectiva:	**Duración del Incidente: Días** **Horas** **Minutos**

○ SI ○ NO		
Se Identifico el Responsable: ○ SI ◉ NO	**Nombre:** Escriba el nombre y apellidos de la persona responsable	**Área:** Escriba el nombre del área, al cual pertenece la persona responsable

Hardware y Software Afectado

Servicios Afectados: ☐ Misionales ☐ Estratégicos ☐ Financieros ☐ Tecnológico ☐ Soporte y Mejora

☐ Servidor ☐ PC ☐ Portátil ☐ BD ☐ Portal WEB ☐ Aplicación ☐ Correo ☐ Equipo Activo ☐ Otros

Descripción Detallada del Activo o Servicio Afectado:

Realice una descripción detallada del activo como: tipo de hardware, sistema operativo, tipo de licenciamiento, motor de base de datos, buzón de correo electrónico, servidor web, dirección ip, proveedor de servicio de internet. etc

Debido al Incidente:	Alguien no autorizado tuvo acceso a la información: ◉ SI ○ NO
	Se ha impedido a algún usuario el acceso a la información: ◉ SI ○ NO
	Se ha borrado, modificado y eliminado alguna información: ◉ SI ○ NO

Impacto del incidente: ☐ Financiero ☐ Reputacional ☐ Operacional ☐ Legal

Causa Raíz:

Escriba cual fue la causa raíz, por la cual se presentó el incidente.

Realizo Plan de Mejoramiento: ◉ SI ○ NO

Acciones Planificas para Solución Causa Raíz:

Escriba las actividades de manera secuencial, que permitirán eliminar y/o controlar la causa raíz.

Lecciones Aprendidas:

Escriba las lecciones aprendidas generadas en las etapas antes, durante y después del incidente

Después de realizar la contención y actividades de mitigación el incidente se encuentra: (•) Abierto ( ) Cerrado	**El incidente ya se había presentado:** ( ) SI (•) NO
Otros: Escriba cualquier otra información relacionada con el incidente, que no se encuentre contenida en este formato.	