# ANEXO C – POLÍTICA DE SEGURIDAD

| | | |
|---|---|---|
| Logo | Documento:<br>Política De Seguridad | Versión: 01<br>Código: PS-01 |
| SEGURIDAD DE LA INFORMACION | | Fecha de publicación:<br>Mes Dia Año |

| | |
|---|---|
| **Título del documento** | Política de Seguridad de la Información |
| **Aprobación** | Comité de Seguridad |
| **Lista de distribución** | Todos los funcionarios |

## POLÍTICA DE SEGURIDAD

La institución está comprometida con la protección de la confidencialidad, integridad, disponibilidad y confiabilidad de su información, así mismo con sus funcionarios, estudiantes, padres, contratistas y proveedores.

La institución ha implantado algunos dominios relevantes del SGSI "Sistema de Gestión de Seguridad de la Información" con la finalidad de definir lineamientos y procedimientos claros, acordes a los objetivos estratégicos de negocio saliéndole al paso a los cambios tecnológicos y marcos jurídicos vigentes por la legislación colombiana, teniendo en cuenta el derecho a la privacidad, y la protección de los datos personales fundamentales para cada individuo que forma parte de la sociedad.

La misión del SGSI es definir el escenario en el cual la información será protegida contra amenazas internas y externas, identificando las falencias y aplicando los correctivos necesarios en aras de proteger la información.

Con la implantación del SGSI se logra minimizar los riesgos principales identificados, a un nivel de aceptación definido por la Alta Dirección por medio de la aplicación de controles para proteger los activos de información.

La institución se compromete a establecer programas de capacitación a todos los funcionarios de la organización en búsqueda de la concientización a fin de minimizar la ocurrencia y el impacto generado por cualquier incidente de seguridad.

Las políticas de Seguridad de la Información deberán ser conocidas, aceptadas y cumplidas por todo funcionario, estudiante, padre de familia y contratista de la institución. El no cumplimiento

de alguna de ellas será considerado como un incidente de seguridad que generará la apertura de un procedimiento disciplinario para los funcionarios, estudiantes, padres de familia y podría ser causa de terminación de contrato firmado con la institucion.

Esta política será revisada con una frecuencia de dos veces al año o cuando existan cambios en el modelo de negocio o ante la ocurrencia de alguna condición que afecte la política, para asegurar que se mantiene ajustada y acorde a los requerimientos de la norma ISO/IEC 27001:2013.

Las principales directrices propuestas por la institución son:

- Proteger la confidencialidad, integridad y disponibilidad de la información no solo de la organización sino también de sus clientes, contratistas y proveedores.

- Establecimiento de controles para disminuir los riesgos críticos y de alto impacto para el negocio.

- Establecer al interior de la empresa los roles y responsabilidades acorde a lo que exige el modelo SGSI.

- Generar y mantener una cultura de Seguridad de la Información tendiente al análisis de riesgos mediante capacitaciones y sensibilización a los funcionarios y contratistas de la institución.

- Velar por el cumplimiento de las leyes, las regulaciones nacionales e internacionales que se encuentren relacionadas con los servicios que actualmente ofrece la organización.

- Ante cualquier incidente de seguridad que se presente deberá comunicarse mediante vía telefónica. Para ello, la institución educativa ha habilitado las líneas #xxx y #xxx.

A partir de la fecha de su publicación, esta política será efectiva y aplica para toda la organización.

Bogotá DC, noviembre 24 de 2022

**Rector**
**Institución educativa**

| | | Aplica | | Cumple | |
|---|---|---|---|---|---|
| | | Si | No | Si | No |
| SGSI | 4.0 CONTEXTO ORGANIZACIÓN | | x | | x |
| | 5.0 LIDERAZGO | x | | | x |
| | 6.0 PLANIFICACIÓN | x | | | x |
| | 7.0 APOYO | x | | x | |
| | 8.0 OPERACIÓN | x | | | x |
| | 9.0 EVALUACIÓN RENDIMIENTO | x | | x | |
| Anexo A | A.5 POLÍTICAS SEGURIDAD DE LA INFORMACIÓN | x | | | x |
| | A.6 ORGANIZACIÓN SEGURIDAD DE LA INFORMACIÓN | x | | | x |
| | A.7 SEGURIDAD RECURSOS HUMANOS | x | | x | |
| | A.8 GESTIÓN ACTIVOS | x | | | x |
| | A.9 CONTROL DE ACCESO | x | | | x |
| | A.10 CRIPTOGRAFÍA | x | | | x |
| | A.11 SEGURIDAD FÍSICA Y AMBIENTAL | x | | | x |
| | A.12 SEGURIDAD OPERATIVA | x | | | x |
| | A.13 SEGURIDAD COMUNICACIONES | x | | | x |
| | A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA | | x | | x |
| | A.15 RELACIONES DEL PROVEEDOR | x | | | x |
| | A.16 GESTIÓN INCIDENTES SEGURIDAD de la INFORMACIÓN | x | | | x |
| | A.17 GESTIÓN DE LA CONTINUIDAD, ASPECTOS SEGURIDAD DE LA INFORMACION | x | | | x |
| | A.18 CUMPLIMIENTO | | x | | x |

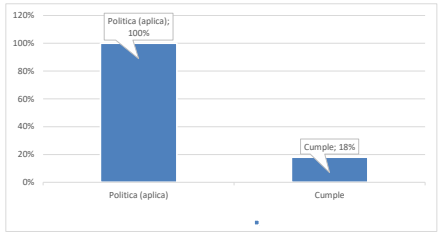
Politicas (Aplican)

| | |
|---|---|
| 0 | 0% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 0 | 0% |
| 1 | 5% |
| 1 | 5% |
| 1 | 5% |
| 0 | 0% |

| Politica (aplica | Cumple |
|---|---|
| 100% | 18% |

0,17

| | | |
|---|---|---|
| 17 | 100 | 17,6470588 |
| 3 | 17,6470588 | |
| | 0,17647059 | |



| Item | Activos | Marca | Observaciones | Categoría | Responsable de TI | Responsable | Nivel de criticidad | Nivel de impacto | Nivel de prioridad | Valor del equipo | Coste de indisponibilidad x hora |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | EQUIPOS DE COMPUTO | DELL | ADMISIONES Y SECRETARÍA GENERAL | Computo | Soporte técnico | ADMISIONES Y SECRETARÍA GENERAL | Media | Medio | Media | | $2.982.549 |
| 2 | EQUIPOS DE COMPUTO | DELL | COMPRAS | Computo | Soporte técnico | COMPRAS | Media | Medio | Media | | $2.982.549 |
| 3 | EQUIPOS DE COMPUTO | DELL | DIRECCIÓN | Computo | Soporte técnico | DIRECCIÓN | Alta | Medio | Alta | | $3.621.666 |
| 4 | EQUIPOS DE COMPUTO | DELL | TESORERÍA, CONTABILIDAD Y ADMINISTRACIÓN FINANCIERA | Computo | Soporte técnico | TESORERÍA, CONTABILIDAD Y ADMINISTRACIÓN FINANCIERA | Alta | Medio | Alta | | $3.621.666 |
| 5 | EQUIPOS DE COMPUTO | DELL | COORDINACIÓN ACADEMICA Y SALONES DE CLASE | Computo | Soporte técnico | COORDINACIÓN ACADEMICA Y SALONES DE CLASE | Alta | Medio | Alta | | $3.621.666 |
| 6 | EQUIPOS DE COMPUTO | DELL | TECNOLOGÍA | Computo | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 7 | EQUIPOS DE COMPUTO | DELL | ENFERMERÍA | Computo | Soporte técnico | ENFERMERÍA | Baja | Bajo | Baja | | $1.491.274 |
| 8 | Servidor HP Proliant DL160 Gen9 | HPE | Este equipo fue convertido en un Firewall Open Source - Pfsense | Infraestructura | Soporte técnico | Soporte técnico | Alta | Alto | Alta | | $4.260.784 |
| 9 | Servidor HP Proliant DL160 Gen9 | HPE | Este equipo contiene aplicaciones de controlador de red inalámbrica y sistema de | Infraestructura | Soporte técnico | Soporte técnico | Media | Medio | Media | | $2.982.549 |
| 10 | Servidor HP Proliant DL160 Gen9 | HPE | Este equipo contiene el controlador de dominio, al cual está desplegado en una Hyper-v | Infraestructura | Soporte técnico | Soporte técnico | Alta | Alto | Alta | | $4.260.784 |
| 11 | Switch HP 1920-16G | HPE | A este switch están conectados los servidores al igual que el Firewall | Infraestructura | Soporte técnico | Soporte técnico | Alta | Alto | Alta | | $4.260.784 |
| 12 | Planta telefónica UCM6202 | Grandstream | Este equipo está conectado al switch HP 1920 y al Router del ISP, ya que este último provee | Infraestructura | Soporte técnico | Soporte técnico | Media | Medio | Media | | $2.982.549 |
| 13 | Switch SG300-28 (1) | CISCO | Este dispositivo va conectado por fibra óptica con los switch (3) y (5) para alimentar a los | Infraestructura | Soporte técnico | Soporte técnico | Alta | Alto | Alta | | $4.260.784 |
| 14 | Switch SG300-28 (2) | CISCO | Dispositivo que brinda conexión a equipos finales | Infraestructura | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 15 | Switch SG300-28 (3) | CISCO | Dispositivo que brinda conexión a equipos finales | Infraestructura | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 16 | Switch SG300-28 (4) | CISCO | Dispositivo que brinda conexión a equipos finales, al igual que está conectado al switch (2) | Infraestructura | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 17 | Switch SG300-28 (5) | CISCO | Dispositivo que brinda conexión a equipos finales | Infraestructura | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 18 | Switch 1930 24p | ARUBA | Dispositivo que brinda conexión a equipos finales | Infraestructura | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 19 | Switch TL-SG1024D | TP-LINK | Dispositivo que brinda conexión a equipos finales | Infraestructura | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 20 | Switch DGS-1210-28 | D-LINK | Dispositivo que brinda conexión a equipos finales | Infraestructura | Soporte técnico | Soporte técnico | Alta | Medio | Alta | | $3.621.666 |
| 21 | APEX017 | ARUBA | Conectividad inalámbrica | Infraestructura | Soporte técnico | Soporte técnico | Media | Medio | Media | | $2.982.549 |
| 22 | UniFi AP x 3 | UniFi-Ubiquiti | Conectividad inalámbrica | Infraestructura | Soporte técnico | Soporte técnico | Media | Medio | Media | | $2.982.549 |
| 23 | UniFi AP-AC-Pro x 4 | UniFi-Ubiquiti | Conectividad inalámbrica | Infraestructura | Soporte técnico | Soporte técnico | Media | Medio | Media | | $2.982.549 |
| 24 | Servidor HP Proliant DL160 Gen9 | HPE | Este equipo contiene aplicativos de consulta para el área de tesorería y contabilidad | Infraestructura Externa | Proveedores | Tesorería y Contabilidad | Alta | Medio | Alta | | $3.621.666 |
| 25 | CANAL DE INTERNET | CLARO-TIGO | CANALES DE INTERNET DEDICADOS | Infraestructura Externa | Proveedor | Proveedor | Alta | Bajo | Alta | | $2.876.029 |
| 26 | RED INAMABRICA | DELL | RED INAMABRICA | Servicio | Soporte técnico | Soporte técnico | Media | Medio | Media | | $2.982.549 |
| 27 | CONTROL DE ACCESO | BIOSTART | CONTROL DE ACCESO | Software | Soporte técnico | Soporte técnico | Baja | Bajo | Baja | | $1.491.274 |
| 28 | FIREWALL | PFSENSE | SEGURIDAD PERIMETRAL | Software | Soporte técnico | Soporte técnico | Alta | Alto | Alta | | $4.260.784 |
| 29 | ANTIVIRUS | SHOPOS | ANTIVIRUS END POINTS | Software | Soporte técnico | Soporte técnico | Media | Medio | Media | | $2.982.549 |
| 30 | AULA VIRTUAL | TRENDI | AULA VIRTUAL | Software Externo | Proveedor | Proveedor | Alta | Medio | Alta | | $3.621.666 |
| 31 | PAGOS ONLINE | PayU | PAGOS ONLINE | Software Externo | Proveedor | Proveedor | Alta | Medio | Alta | | $3.621.666 |
| 32 | SAP BUSSINESS ONE | SAP | SAP BUSSINESS ONE | Software Externo | Proveedor | Proveedor | Alta | Medio | Alta | | $3.621.666 |

53% Medio-Bajo

| Item | Activos | Servicios | Categoría | Responsable de TI | Responsable Funcional | Nivel de criticidad | Nivel de impacto | Nivel de prioridad | Coste de indisponibilidad X |
|---|---|---|---|---|---|---|---|---|---|
| 1 | EQUIPOS DE COMPUTO | ADMISIONES Y SECRETARIA GENERAL, COMPRAS, DIRECCION, TESORERÍA | Computo | Soporte técnico | ADMISIONES Y SECRETARÍA GENERAL | Alta | Medio | Alta | $3.621.666 |
| 2 | Servidor HP Proliant DL160 Gen9 | Servidores Open Source - Pfsense, Controlador inalambrico, Sistema de ingreso, Controlador | Infraestructura | Soporte técnico | Soporte técnico | Alta | Alto | Alta | $4.260.784 |
| 3 | Switches SG300 | A este switch están conectados los servidores al igual que el Firewall, capa de acceso a | Infraestructura | Soporte técnico | Soporte técnico | Alta | Alto | Alta | $4.260.784 |
| 4 | Planta telefónica UCM6202 | Este equipo está conectado al switch HP 1920 y al Router del ISP, ya que este último provee | Infraestructura | Soporte técnico | Soporte técnico | Media | Medio | Media | $2.982.549 |
| 5 | APEX017, UniFi AP x 3, UniFi AP-AC-Pro x 4 | Conectividad inalámbrica | Infraestructura | Soporte técnico | Soporte técnico | Media | Medio | Media | $2.982.549 |
| 6 | CANAL DE INTERNET | CANALES DE INTERNET DEDICADOS | Infraestructura Externa | Proveedor | Proveedor | Alta | Bajo | Alta | $2.876.029 |
| 7 | RED INAMABRICA | RED INAMABRICA | Servicio | Soporte técnico | Soporte técnico | Media | Medio | Media | $2.982.549 |
| 8 | CONTROL DE ACCESO | CONTROL DE ACCESO | Software | Soporte técnico | Soporte técnico | Baja | Bajo | Baja | $1.491.274 |
| 9 | FIREWALL | SEGURIDAD PERIMETRAL | Software | Soporte técnico | Soporte técnico | Alta | Alto | Alta | $4.260.784 |
| 10 | ANTIVIRUS | ANTIVIRUS END POINTS | Software | Soporte técnico | Soporte técnico | Media | Medio | Media | $2.982.549 |
| 11 | AULA VIRTUAL | AULA VIRTUAL | Software Externo | Proveedor | Proveedor | Alta | Medio | Alta | $3.621.666 |
| 12 | PAGOS ONLINE | PAGOS ONLINE | Software Externo | Proveedor | Proveedor | Alta | Medio | Alta | $3.621.666 |
| 13 | SAP BUSSINESS ONE | SAP BUSSINESS ONE | Software Externo | Proveedor | Proveedor | Alta | Medio | Alta | $3.621.666 |

53% Medio-Bajo

A manera de ejemplo se definen una serie de variables que podrán
ser utilizadas
para realzar la evaluación de los incidentes
- Prioridad
- Criticidad de impacto
- Impacto Actual
- Impacto Futuro

**Nivel de Prioridad:** Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

| Nivel Criticidad | Valor | Definición |
|---|---|---|
| **Inferior** | **0,10** | Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas. |
| **Bajo** | **0,25** | Sistemas que apoyan a una sola dependencia o proceso de una entidad. |
| **Medio** | **0,50** | Sistemas que apoyan más de una dependencias o proceso de la entidad. |
| **Alto** | **0,75** | Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas. |
| **Superior** | **1,00** | Sistemas Críticos. |

*Tabla 1: Niveles de Criticidad de Impacto*

**Impacto Actual:** Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

**Impacto Futuro:** Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

| Nivel Impacto | Valor | Definición |
|---|---|---|
| **Inferior** | **0,10** | Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| **Bajo** | **0,25** | Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| **Medio** | **0,50** | Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo. |
| **Alto** | **0,75** | Impacto moderado en uno o más componentes de más de un sistema de información. |
| **Superior** | **1,00** | Impacto alto en uno o más componentes de más de un sistema de información. |

*Tabal 2: Niveles de Impacto Actual y Futuro*

Luego de tener definidas las variables se obtiene la *prioridad* mediante la siguiente formula:

***Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)***

Y los resultados obtenidos se deben compara con la siguiente tabla para determinar la prioridad de atención:

| Nivel Prioridad | Valor |
|---|---|
| **Inferior** | **00,00 – 02,49** |
| **Bajo** | **02,50 – 03,74** |
| **Medio** | **03,75 – 04,99** |

| | |
|---|---|
| **Alto** | **05,00 – 07,49** |
| **Superior** | **07,50 – 10,00** |

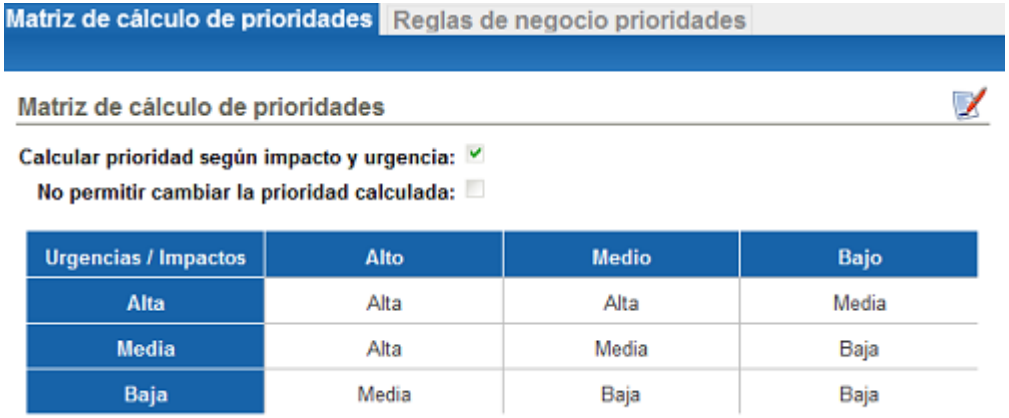
*Tabla 3: Niveles de Prioridad del Incidente*

Calculo para valorar las perdidas

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Perdida por hora | $4.260.784 | ########## | $170.431.360 | $681.725.440 | $7.498.979.840 | 1760 | $4.260.784 |

| Criticidad | | Impacto | | | | | |
|---|---|---|---|---|---|---|---|
| Alto | 100% | Alto | 100% | 100% | Alto-Alto | 85% | Alto-Medio |
| Medio | 70% | Medio | 70% | 70% | Medio-Medio | 68% | Alto-Bajo |
| Bajo | 35% | Bajo | 35% | 35% | Bajo-Bajo | | |

Nivel de prioridad




| Urgencias / Impactos | Alto | Medio | Bajo |
|---|---|---|---|
| **Alta** | Alta | Alta | Media |
| **Media** | Alta | Media | Baja |
| **Baja** | Media | Baja | Baja |

**(Institución Educativa)**

# PLAN DE SEGURIDAD DE LA INFORMACIÓN

**2022**

**TABLA DE**

**CONTENIDO**

# Documento aprobación

| Nombre | Cargo | Fecha |
|---|---|---|
| | | |
| | | |
| | | |

# Historial Revisión

| Fecha | Versión | Descripción Revisión | Autor |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |

# 1. INTRODUCCION

Los requerimientos de seguridad que actualmente la globalización demanda frente a las nuevas tecnologías de información y comunicaciones (TIC), hace necesario que las instituciones tanto privadas como públicas, se vean inmersas en el desarrollo e implementación de políticas que contrarresten la aparición de nuevas amenazas en los sistemas computarizados, tales como las transgresiones e intrusiones cibernéticas, que atentan contra la estabilidad y el normal funcionamiento de los servicios que presta la Oficina de Tecnologías de la Información y las Comunicaciones. De igual manera y para resguardar la información desde todos los ángulos, es crucial desarrollar conciencia en todos los funcionarios de la organización, de la responsabilidad que tienen frente a los activos de información que cada uno tiene a cargo.

La institución educativa (CNG) consolidada como una institución líder del sector, para garantizar su competencia tiene la responsabilidad de contar con un direccionamiento estratégico en materia de seguridad de los activos de información propios de su ambiente institucional.

Las políticas generales y específicas de seguridad y privacidad de la información se fundamentan en los dominios y objetivos de control de

la norma ISO/IEC 27001:2013 y en el código de buenas prácticas para la gestión de la seguridad de la información ISO/IEC 27002:2013.

## 2. OBJETIVOS

### 2.1 OBJETIVO GENERAL

Definir los lineamientos, políticas generales y específicas que deben cumplir todos los funcionarios, contratistas y terceros del CNG, frente a amenazas internas o externas, deliberadas o accidentales, para garantizar y preservar la confidencialidad, integridad y disponibilidad de los activos de la información.

### 2.2 OBJETIVOS ESPECÍFICOS

- Establecer los roles y responsabilidades para la implementación, seguimiento y mejora del plan de seguridad de la información.

- Sensibilizar sobre los requerimientos técnicos del estándar ISO/IEC 27001:2013 de Seguridad de la Información, la cual establece los requerimientos para el establecimiento, implementación y mejoramiento continuo del sistema de gestión de seguridad de la información necesarios para la implementación, seguimiento y mejora del sistema de gestión de seguridad de la información.

- Orientar la implementación del Plan de Seguridad de la Información al interior del Colegio Nuevo Gimnasio.

## 3. ALCANCE

Este documento aplica a todos los funcionarios, directivos, terceros tales como proveedores y contratistas, entes de control, usuarios internos y externos que accedan o hacen uso de cualquier activo de información, independientemente de su ubicación, medio o formato. Las políticas aplican a toda la información creada, procesada y/o utilizada en el soporte y desarrollo de las funciones y competencias del CNG, sin importar el medio, formato, presentación o lugar en el cual se encuentre. Toda información debe contar con mecanismos y disposiciones que garanticen su confidencialidad, integridad y disponibilidad.

## 4. MEDIDAS DE SEGURIDAD

Los sistemas de información, los recursos tecnológicos, las bases de datos son accesibles únicamente por las personas designadas por la institución educativa. Los responsables de los datos de la institución educativa, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución con el objetivo que prevalezca la confidencialidad, integridad, disponibilidad y almacenamiento durante su vigencia, así como la periodicidad con la que se cambian.

## 5. RESPONSABILIDADES:

**5.1. Rector:** Es responsable por generar las condiciones adecuadas para la comunicación de la presente política, así como de establecer el alcance para su aplicación. También es responsable de aprobar los planes de respuesta.

**5.2. Directores:** Son responsables por la identificación de los procesos críticos y los activos de información, deben participar en la creación del plan de continuidad de negocio. También son responsables de realizar el análisis de impacto en negocio (BIA).

**5.3. Responsable de tecnología:** Debe participar en la planeación técnica del plan de contingencia y recuperación ante desastres, se sugiere que exista un área de Seguridad de la Información que vele por el cumplimiento de la política, esta área será responsable de la definición y gestión del plan de continuidad y recuperación ante desastres.

**5.4. Funcionarios de la Institución Educativa:** Deben cumplir con lo establecido en la política y participar activamente de las pruebas que se realicen en el plan de continuidad y recuperación ante desastres.

**5.5. Responsable de seguridad de la información:** debe velar por el cumplimiento de la presente política y realizar las revisiones oportunas de la misma.

## 6. DEFINICIONES

**Aceptación del riesgo:** decisión de asumir un riesgo.

**Activo:** Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

**Activo crítico:** Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectaran el cumplimiento de los objetivos misionales del CNG.

**Amenaza:** causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización, la amenaza es una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se ocasione una violación de la seguridad.

**Análisis de vulnerabilidad:** Proceso sistemático para identificar vulnerabilidades presentes en los activos informáticos (también llamados CI).

**Buenas prácticas**: El concepto de buena práctica, involucra procesos, estructuras e instrumentos de participación, que siempre van en función

de lograr y alcanzar una mejora continua empresarial, donde es necesario sumar contenido con levantamiento de información de TI propio de cada empresa (procesamiento, almacenamiento, networking, seguridad, nubes híbridas, DevOps***, aplicaciones, base de datos, etc.). Para ello existen los siguientes marcos de referencia que se pueden consultar para TI: gestión de servicios (las más populares son ITIL y la ISO 20000), gestión de gobierno, gestión de riesgos, gestión de la seguridad de la información (ISO 27000), análisis del negocio, arquitectura empresarial (TOGAF), gestión de proyectos, entre otros.

**CI:** Elementos de configuración pueden ser hardware, las aplicaciones de software instaladas, documentos, servicios empresariales y también las personas que forman parte de su sistema de TI.

**CNG:** Institución Educativa Colegio Nuevo Gimnasio.

**Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, la información es accesible solamente por quienes están autorizados para ello.

**Control:** medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, acciones, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de

gestión o legal. NOTA. Control es también utilizado como sinónimo de salvaguarda.

**Control Compensatorio:** Es una medida de mitigación alterna implementada en casos en los que no es posible (por razones técnicas, económicas o de negocio) cerrar la vulnerabilidad encontrada.

**Disponibilidad:** propiedad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

**Evento:** Los eventos son aquellos sucesos o cambios significativos en el estado del hardware o el software de un sistema.

**Hardening**: El hardening o endurecimiento de los sistemas se refiere a las herramientas, los métodos y las buenas prácticas utilizadas para reducir la superficie de ataque en la infraestructura tecnológica, incluyendo el software, los sistemas de datos y el hardware.

**Incidente:** Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información.

**Información:** toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en

cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

**Integridad:** propiedad de salvaguardar la exactitud de la información y sus métodos de proceso y el estado completo de los activos.

**Líder de Seguridad de la Información:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los funcionarios de la institución que así lo requieran.

**Medio removible:** Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.

**Mesa de ayuda**: La función de la Mesa de Ayuda es proveer a los usuarios un punto único de contacto mediante el cual se resuelvan y/o canalicen sus necesidades relativas al uso de recursos y servicios de plataformas tecnológicas, siempre de acuerdo con un estándar adoptado por la empresa.

**Mitigación de vulnerabilidad:** Es la consecuencia de la implementación de un control compensatorio, que reduce el riesgo de explotación de la vulnerabilidad.

**No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

**NTC-ISO/IEC 27001:2013:** Norma técnica colombiana que ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

**Plan de Continuidad de Negocio:** Actividades documentadas que guían a la institución en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles pre-definidos después de un incidente que afecte la continuidad de las operaciones.

**Plan de seguridad de la Información - PSI - :** Son medidas que se toman con el fin de proteger los recursos de la organización y minimizar los riesgos y comprenden todas aquellas actividades que contribuyen a garantizar la confidencialidad, integridad y disponibilidad de la información.

**Proceso:** Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

**Retest:** Procedimiento que se ejecuta a un componente que ya fue analizado previamente, es decir, una segunda revisión.

**Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

**Sistema de gestión de la seguridad de la información – SGSI - :** Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información (ciclo PHVA).

**Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso dentro del CNG.

**Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en un

computador o una red para dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

**Soporte Técnico:** es un servicio que proporciona un único punto de contacto para todos los usuarios de servicios relacionados con tecnologías de información del Ministerio, respondiendo y dando solución a las preguntas y problemas. De igual manera, brinda un apoyo inmediato en línea acerca de los problemas relacionados con el software y hardware de las estaciones de trabajo y equipos portátiles. El Soporte Técnico resuelve requerimientos e indica los pasos a seguir para solicitar los servicios proporcionados por el Grupo de Soporte Técnico y orienta dichas solicitudes al personal apropiado.

**Vulnerabilidad:** Es un fallo informático que pone en peligro al sistema. Es decir, que se trata de un bug que puede usar un atacante con fines maliciosos.

**VPN:** Una red privada virtual de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Es una directriz global que establece qué y por qué se quiere proteger. Su definición está ceñida a las normas internacionales ISO 27001:2013

para gestionar la seguridad de la información y deberá estar alineada igualmente con el plan estratégico de la Institución Educativa.

La institución Educativa en cumplimiento de requisitos legales y regulatorios define criterios, directrices, controles físicos y digitales, asignación de responsabilidades y lineamientos específicos dentro de su plan de su plan de seguridad de la información que le permitan cumplir con una cultura de seguridad de la información, previniendo incidentes a través de la gestión de riesgos de seguridad y privacidad de la información y seguridad digital, frente a amenazas internas o externas, deliberadas o accidentales, que garanticen y preserven la confidencialidad, integridad y disponibilidad de la información, de todos los funcionarios, contratistas y grupos de interés de la Institución Educativa con el fin de tener un recurso humano comprometido garantizando un servicio de calidad a toda la comunidad.

## 7. MARCO NORMATIVO

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001:2013 y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a la institución. Sus normas establecen los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse

siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- Alcance estratégico: La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- Seguridad integral: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información
- Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- Mejora continua: Las medidas de seguridad se revaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal calificado.

- Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. Las buenas prácticas considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal. Puesto que la Seguridad de la Información incumbe a todo el personal, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.

## 8. CONTROL DE ACCESO

El control de acceso está enmarcado en la política que define como debe manejarse en todos los sistemas de información con los que cuenta la institución, en cualquier ámbito y bajo las condiciones sobre las cuales opere, un acceso que garantice y/o asegure la entrada de los usuarios

autorizados, previniendo el acceso no autorizado, logrando de esta manera obtener una confiabilidad en la operación.

Existen tres aspectos sobre las cuales el control de acceso debe operar:

**8.1. La autenticidad:** Los usuarios deberán ser únicos y no compartidos, asignando los privilegios mediante el principio del mínimo privilegio. Se prohibirá la creación de usuarios genéricos, acudiendo siempre a cuentas de usuario asociadas a la identidad nominal del empleado.

**8.2. Derechos de acceso:** Está orientado a solo garantizar que a los usuarios se les otorgue privilegios y derechos necesarios para poder realizar sus tareas en el día a día. Se debe basar en roles donde se le asigne los permisos a la aplicación, en la función de aplicación del mínimo privilegio, al recurso únicamente si lo requiere para realizar sus labores, junto a una segregación de funciones según sea el caso. Su función es de la operar bajo una restricción y un control adecuado.

**8.3. Definición de los recursos:** Deberán ser asignados solamente a los recursos físicos, dispositivos, acceso lógico, a los que se necesite para el desarrollo de sus actividades.

Estos aspectos deberán ser revisados periódicamente y más cuando el empleado, se ha movido de manera temporal o definitiva a otra área.

Deberán entrar en operación conjunta, tanto con el de tecnología como del área de recursos humanos, con el fin de poder ser activado o desactivado.

## 9. USUARIOS Y CONTRASEÑAS

Para este rubro la institución debe contar con normas que cubran los siguientes aspectos:

1. Activación y desactivación de usuarios.
2. Activación y desactivación de privilegios de accesos.

Los usuarios y contraseñas a recursos de la institución deben ser tratados como personales, confidenciales e intransferibles y cada empleado que tenga una cuenta de usuario asignada, debe ser responsable por el uso y manejo de esta, la cual no deben en ninguna circunstancia ser compartida.

La utilización de usuarios genéricos representa un riesgo de seguridad muy alto y debe no utilizarse, salvo en excepciones que deben ser analizadas, justificadas y documentadas por el responsable de seguridad de la información.

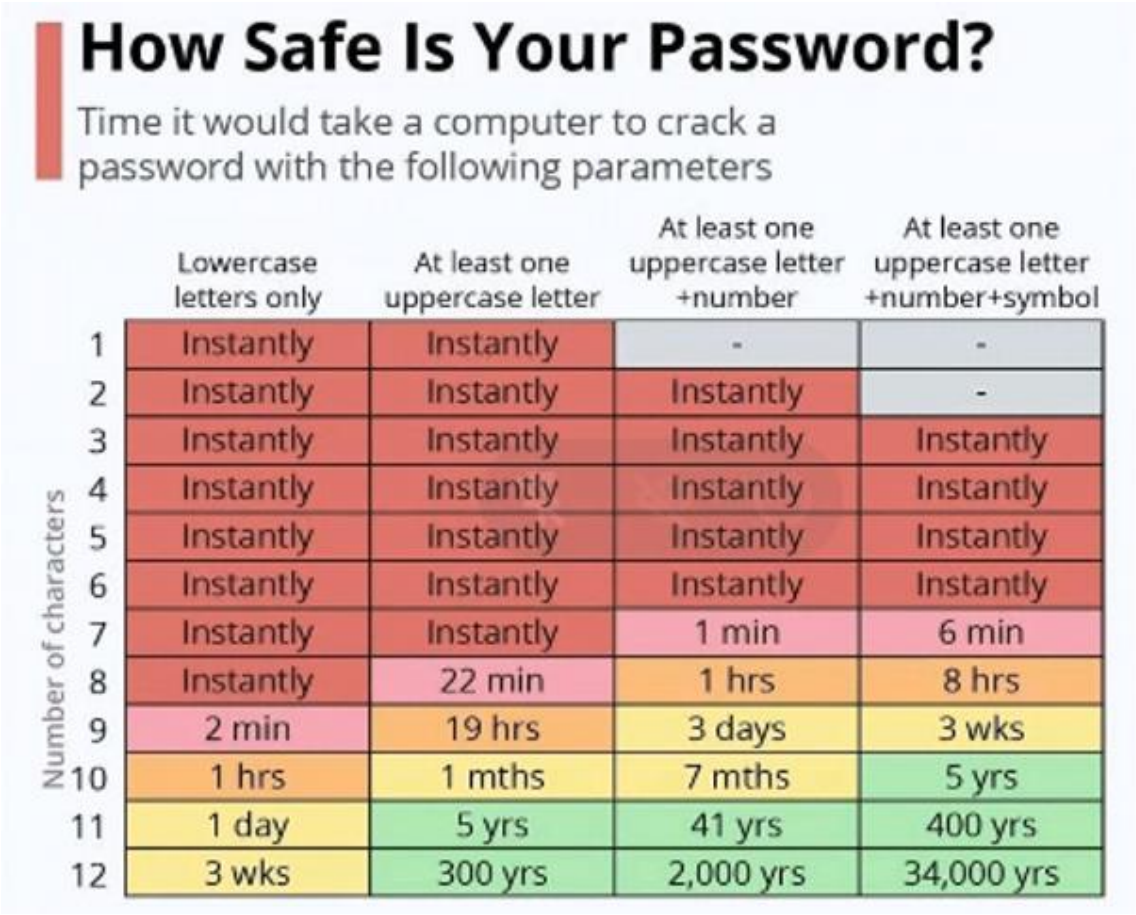
Toda cuenta de usuario debe tener asignada una contraseña, con la opción de que sea cambiada una vez se logré el acceso.

Con respecto a la asignación de contraseñas deben requerir cierto nivel de complejidad mínimo y no pueden estar asociadas a datos personales que permitan su deducción.

Las contraseñas deben cumplir, al menos, con los siguientes requerimientos:

- Longitud mínima de 12 caracteres.
- Estar conformada por al menos 4 características que se enumeran a continuación:
- Caracteres alfabéticos mayúsculas
- Caracteres alfabéticos minúsculas
- Caracteres numéricos
- Caracteres especiales o extendidos

Bajo el ámbito de seguridad una contraseña con esa longitud va a tardar más en que pueda ser descifrada, según las fuentes tardaría más de 2000 años aproximadamente.



## How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

| Number of characters | Lowercase letters only | At least one uppercase letter | At least one uppercase letter +number | At least one uppercase letter +number+symbol |
|---|---|---|---|---|
| 1 | Instantly | Instantly | - | - |
| 2 | Instantly | Instantly | Instantly | - |
| 3 | Instantly | Instantly | Instantly | Instantly |
| 4 | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 1 min | 6 min |
| 8 | Instantly | 22 min | 1 hrs | 8 hrs |
| 9 | 2 min | 19 hrs | 3 days | 3 wks |
| 10 | 1 hrs | 1 mths | 7 mths | 5 yrs |
| 11 | 1 day | 5 yrs | 41 yrs | 400 yrs |
| 12 | 3 wks | 300 yrs | 2,000 yrs | 34,000 yrs |

Dentro de las propiedades a nivel de contraseñas deben mantener las siguientes reglas:

- Periodo de validez de 60 días.
- Debe no permitir repetir la contraseña al menos en las últimas 10 utilizadas.
- Debe forzar a cambiarla en su primer uso o cuando sea cambiada por alguna razón.
- Debe ser bloqueada cuando se presenten más de 3 intentos fallidos de inicio de sesión.

- Debe garantizar que el almacenamiento y el tránsito de la palabra clave del usuario viaje de manera segura no en texto plano o claro.
- La contraseña una vez le llegue al usuario debe ser cambiada de inmediato, evitando y minimizando riesgos de posible intervención para que pueda ser robada por algunos de los entes amenazantes que existen en la red o inclusive en el mundo digital.
- Cuando una cuenta de usuario no ha sido utilizada en un periodo mayor a 3 meses, deberá ser automática bloqueada.
- Evite guardar la contraseña en post-its o papel en cualquier lugar de su oficina.
- Evite guardar la contraseña en archivos en su computadora o dispositivos móviles (teléfonos, tablets) sin cifrado.
- Evite utilizar la función "Recordar Contraseña" de aplicaciones (por ejemplo, navegadores web).
- Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe reportar el incidente inmediatamente a la mesa de ayuda o soporte y cambiar la contraseña a la brevedad posible.

## 9.1 USUARIOS CON ACCESO PRIVILEGIADO

Con respecto al acceso privilegiado, la solicitud de una cuenta de usuario debe ser realizada por el jefe autorizado para aprobar su creación y/o desactivación del mismo, con la debida justificación que permitirá cubrir la necesidad de uso y dirigida al responsable de su creación, quien

cumplirá con la solicitud de acuerdo a lo establecido en el procedimiento definido.

Las cuentas de usuario privilegiado deben ser otorgadas a los empleados dependiendo de su rol que desempeña, pero lo más importante que le permita desarrollar sus actividades correspondientes a sus funciones para lo cual fue contratado.

Por buena práctica, las contraseñas de administrador deben ser eliminadas o deshabilitadas, además modificadas sus contraseñas por seguridad.

## 10. REQUISITOS PARA LOS EQUIPOS DE COMPUTO

Los requisitos que exige esta política están protegidos por la norma ISO 27001:2013, que da unas pautas para aplicar en los equipos de cómputo y que deben ser aplicados a todos los equipos de cómputo de la institución, con el propósito que garantice y/o asegure su acceso a la red LAN de la institución.

Estos requisitos, están enmarcados bajos cuatro aspectos fundamentales, a saber:

1. Actualización del firmware del equipo.
2. Actualización a nivel de sistema operativo como parches.
3. Verificación del software instalado.

4. Configuraciones de acceso.

Para precisar esos 4 aspectos, desglosaremos cada uno de ellos.

1. **Actualización del firmware**: Con este requisito lo que se persigue es que se tenga siempre actualizado el bios y/o firmware del equipo, que permite proteger frente a posibles vulnerabilidades descubiertas y que pueden estar latentes en el equipo. Con esta aplicación se logra disminuir las amenazas y riesgos que representen un impacto ante la red.

2. **Actualización a nivel de sistema operativo**: Con este requisito lo que se persigue es que el equipo cuente con las actualizaciones que libere el fabricante en donde puedan mitigarse y eliminarse las vulnerabilidades descubiertas, asegurando una operación confiable ante la red e institución.

3. **Verificación del software instalado**: Con este requisito lo que se persigue es que:

- El software instalado tenga una licencia oficial.
- Que no se permita la instalación de cualquier software.
- Que se tenga una antivirus instalado y manejado desde una consola, que permita realizar su actualización y que permita reportar cualquier alertamiento de virus, como la aplicación de su actualización para resolverlo.

4. **Configuraciones de acceso**: Lo que se persigue con este requisito es:

- Que se apliquen la lista de comprobación del hardening para el sistema operativo.
- Que el acceso debe estar sujeto a un usuario nombrado y con permisos de usuario normal no administrador.
- Se debe crear una carpeta temporal compartida para almacenar de manera temporal los archivos de trabajo, pero condicionada a que se depurará mediante un Job programado cada 8 días. En el caso que requiera guardar en algún dispositivo externo (USB), se tienen dos opciones o que el dueño del archivo lo envíe vía correo a su buzón de correo personal o que el soporte técnico de mesa de ayuda lo pueda bajar al dispositivo externo, no sian antes pasar por la revisión correspondientes antes de ser usado para almacenar la información. De esta manera lo que se quiere perseguir es minimizar posibles riesgos como son los virus o malware (PROGRAMAS MALIGNOS) que quieran colarse a la red y comprometer de esta manera la seguridad de la INFRAESTRUCTURA.

NOTA: LA INSTITUCION NO SE HARA RESPONSABLE POR LA INFORMACION ALMACENADA FUERA DE LA CARPETA COMPARTIDA QUE SE DEFINA COMO PUNTO UNICO DE ACCESO A LOS ARCHIVOS DE

TRABAJO QUE SE GENEREN PRODUCTO DE LAS ACTIVIDADES ACADEMICAS QUE SE GENEREN EN LA INSTITUCION.

## 11. GESTIÓN DE INCIDENTES DE SEGURIDAD

En un evento que afecte la integridad, confidencialidad y disponibilidad de los activos de información de la Institución Educativa se debe atender con actividades de preparación, detección, contención, erradicación, recuperación, documentación, lecciones aprendidas y cierre del evento.

Los siguientes eventos son los indicadores que nos señalan que posiblemente ha ocurrido un incidente:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Reportes de usuarios
- Software antivirus dando informes
- Otros funcionamientos fuera de lo normal del sistema

Ante un incidente, el funcionario, estudiante o tercero deberá realizar las siguientes actividades:

**Identificar el incidente:** Implica notificar a través del correo electrónico o a la línea de soporte técnico.

Posteriormente el equipo de soporte técnico deberá:

**Registrar del incidente:** Se debe describir de la forma más completa posible, indicando modo, lugar y tiempo del evento. La información que se recoge en este punto es clave para toda la gestión del evento.

**Categorizar el incidente:** Con la información recibida, el ingeniero soporte técnico deberá categorizar el incidente de acuerdo con su nivel de riesgo y criticidad, clasificarlo, medir el impacto y definir el nivel de prioridad, para que posteriormente se determine el tiempo de respuesta de atención.

**Clasificación:** Se clasifican dependiendo su infraestructura, riesgo, y criticidad de los activos; las categorías son:

- **Acceso no autorizado:** Involucra a una persona o sistema que obtiene acceso lógico o físico sin autorización del dueño a una aplicación, sistema, información o activo de información.
- **Modificación no autorizada de un recurso:** Involucra a una persona o sistema que afecte la integridad de la información o de un sistema.
- **Uso inadecuado de recursos:** Involucra a una persona que viola la política de uso de recursos.
- **Indisponibilidad de los servicios:** Involucra a una persona o sistema que impide el uso de un activo de información.
- **Suplantación:** Involucra
- **Otros:** El incidente no puede categorizarse en alguna de las categorías anteriores. El incidente de debe monitorear y de

acuerdo con su comportamiento y necesidad se deben crear nuevas categorías.

Es posible que un incidente se encuentre en más de dos categorías.

## 11.1 Impacto del activo de información

Se determina basado en el análisis de riesgos y clasificación de los activos:

| Nivel de Impacto | Valor | Definición |
|---|---|---|
| **Impacto alto** | 0.35 | Afecta activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos estratégicos de la Institución Educativa, aquí se incluyen aquellos incidentes que afectan la reputación y el buen nombre o involucren aspectos legales y se deben atender de forma inmediata. |
| **Impacto medio** | 0.7 | Afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado. |

| | | |
|---|---|---|
| **Impacto bajo** | 1.0 | Afecta a activos de información considerados de impacto menor e insignificante, que no influyen con ningún objetivo y deben ser monitoreados para evitar un impacto mayor. |

Tabla 1: Niveles de Impacto

## 11.2. Prioridad

Depende del valor o importancia dentro de la institución educativa con base en la siguiente tabla:

| Nivel de criticidad | Valor | Definición |
|---|---|---|
| Bajo | 0.35 | Sistemas que apoyan un área o proceso de la Institución. |
| Medio | 0.7 | Sistemas que apoyan más de una área o proceso de la Institución. |
| Alto | 1.0 | Sistemas críticos que apoyan la Infraestructura Tecnológica y estaciones de trabajo de usuarios con funciones críticas. |

Tabla 2: Niveles de Prioridad de Impacto (criticidad del sistema)

## 11.3 Impacto actual y futuro

**Impacto actual:** se evalúa el daño causado en el momento que se presenta el incidente.

**Impacto actual:** se evalúa el daño causado en que pueda causar el incidente si no es contenido ni erradicado.

| Nivel de impacto | Valor | Definición |
|---|---|---|
| Bajo | 0.35 | Impacto leve en uno de los componentes de la infraestructura tecnológica o estación de trabajo. |
| Medio | 0.7 | Impacto moderado en uno o más componentes de la infraestructura tecnológica o estación de trabajo. |
| Alto | 1.0 | Impacto alto en uno o más componentes de la infraestructura tecnológica o estación de trabajo. |

Tabla 3: Niveles de Impacto Actual y Futuro

Con la información anterior, se utiliza la siguiente formula para obtener la prioridad

**Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)**

Con el resultado se determina la prioridad de atención:

| Nivel de prioridad | Valor |
|---|---|
| Bajo | 0 - 35 |
| Medio | 36 - 70 |

| | |
|---|---|
| Alto | 71 – 10 |

Tabla 4: Niveles de Prioridad del Incidente

**11.4. Tiempo de respuesta:** Se estiman unos tiempos de respuesta máximos para la atención de un incidente de acuerdo con su criticidad e impacto. Los tiempos de solución pueden variar dependiendo el caso.

| Nivel de prioridad | Tiempo de Respuesta |
|---|---|
| Bajo | 3 horas |
| Medio | 30 minutos |
| Alto | 5 minutos |

Tabla 5: Tiempos Máximos de Atención de Incidentes

**11.5. Contención del incidente:** Se deben tomar acciones de respuesta inmediata aplicando controles de emergencia y/o controles permanentes, lo que se busca es evitar la propagación del incidente y la reducción de los daños a los sistemas de información.

Algunas acciones concretas son:

Desconectar

Apagar

Bloquear

Activar contingencia

Copiar / Clonar

Notificar a los interesados

Estas acciones dependerán del tipo de incidente, sistema comprometido y comportamiento del incidente de seguridad, por ejemplo:

Incidente: Acceso no autorizado

Descripción: Varios intentos fallidos de login

Estrategia: Bloquear la cuenta

Se recomienda siempre mantener la evidencia de las acciones correctivas y documentar completamente los procedimientos.

**11.6. Erradicación y recuperación:** Se realiza la eliminación de cualquier rastro dejado por el incidente y de ser necesario la restauración de los sistemas afectados. Así mismo se debe recuperar el servicio para devolver el nivel de operación a su estado normal.

En algunos casos será necesario aplicar el Plan de Recuperación ante Desastres en caso de que el incidente haya afectado gravemente la Infraestructura Tecnológica, para lo cual aplicará la política definida para tal fin.

**11.7. Documentación y lecciones aprendidas:** Documentar el incidente con un informe detallado que contenga información relevante para la construcción de las lecciones aprendidas. En este informe se debe especificar aspectos como; modo, tiempo y lugar del evento, tiempos de respuesta en la atención y solución del incidente, las acciones tomadas y la causa raíz del incidente.

Dentro de los procesos del área de Tecnología se debe incorporar la mejora continua para evitar futuros eventos que afecten la integridad, confidencialidad y disponibilidad de los activos de información. El equipo debe evolucionar para reflejar nuevas amenazas y mejorar constantemente la tecnología en función del negocio.

**11.8. Cierre del incidente:** Realizar un cierre documental del incidente, validando con los usuarios el estado del servicio.

## 12. GESTION DE VULNERABILIDADES

La gestión de vulnerabilidades es el tratamiento que se realiza sobre la infraestructura tecnológica, con la finalidad de mitigar la materialización de riesgos ante posibles ataques a esta. Dicha gestión, se centra, en

llevar a cabo actividades de identificación, clasificación, mitigación o cierre de las brechas de seguridad presentes en la infraestructura tecnológica.

Los análisis de vulnerabilidades a la infraestructura tecnológica del Banco son realizados mediante una herramienta especializada en identificar brechas de seguridad. Se recomienda que este análisis se realice al menos 1 (una) vez al año, cuando se realicen cambios importantes sobre la infraestructura tecnológica de la Institución Educativa y cuando se ingresen nuevos componentes.

El informe del análisis de vulnerabilidades deberá tener como mínimo, el inventario de equipos escaneados, vulnerabilidades identificadas y acciones de mitigación sugeridas, este debe ser socializado a la Dirección de la Institución y al equipo de soporte técnico.

## 12.1. Ejecución del análisis de vulnerabilidades:

Este proceso deberá ser realizado por el equipo de soporte técnico de la Institución mediante un software especializado.

Se recomienda realizar el escaneo de vulnerabilidades en un horario no hábil para la Institución con el fin de minimizar los riesgos de indisponibilidad de servicios. Así mismo se debe informar a la Dirección sobre el proceso ejecutado indicando el tipo de escaneo (de

descubrimiento o a activos definidos), servicios y componentes analizados y fecha y hora estimada para la ejecución.

## 12.2. Revisión del informe de análisis de vulnerabilidades:

Una vez realizado el escaneo a los componentes de la infraestructura tecnológica se genera un informe de los hallazgos, esta información deberá ser filtrada y organizada para que sea de fácil lectura para los interesados.

El informe deberá tener información relevante como; nombre del componente, dirección IP, vulnerabilidad encontrada, criticidad, remediación y links de referencia.

## 12.3. Plan de remediación

Con el informe final del análisis de vulnerabilidades se deberá establecer un plan de remediación en el corto, mediano y largo plazo de acuerdo con la criticidad de cada componente.

El responsable de cada CI deberá evaluar el impacto, la solución técnica y la pertinencia de remediar el componente sin afectar la operación del negocio.

Con la información anterior se debe elaborar un cronograma detallado de actividades de remediación, este cronograma deberá ser aprobado por la Dirección de la Institución.

Una vez aprobado el cronograma de actividades se deberán establecer compromisos en tiempo y responsabilidades y se deberá hacer control y seguimiento al menos 1 (una) vez por semana para asegurar que se ejecuten todas las actividades.

Para vulnerabilidades que no puedan remediarse, por limitantes técnicas sobre el activo, se evalúa la posibilidad de implementar controles compensatorios, los cuales se documentan en el Acta de aceptación de riesgo.

Cada vez que se remedie una vulnerabilidad, se deberá correr un análisis de vulnerabilidades especifico para el CI intervenido (retest) con el fin de garantizar que la remediación fue exitosa.

El proceso de remediación de vulnerabilidades de soluciones tecnológicas (aplicaciones, hardware, dispositivos de comunicaciones, entre otros) en los que la Institución Educativa no tiene administración directa, al ser provistos por terceros, deben ser ejecutados y remediados por estos, para dar cumplimiento tanto a requisitos regulatorios, lineamientos de seguridad de la información, así como buenas prácticas.

## 12.4. Consideraciones sobre las acciones de remediación

- Los controles o configuraciones a implementar sobre los componentes de infraestructura tecnológica para remediar las vulnerabilidades no deben afectar la operación normal de los servicios del Banco.

- Antes de la puesta en producción de las remediaciones, se requiere ejecutar sobre ambientes de prueba y/o dentro de ventanas de mantenimiento autorizadas, contemplando estrategias de roll back.

- Los controles deben ser validados previamente frente a los aspectos de seguridad de la información, compatibilidad tecnológica, factibilidad técnica y funcional.

## 12.5. Tiempos de atención

Tiempos de atención para las vulnerabilidades en la Institución Educativa: Se establecen unos tiempos de respuesta de acuerdo con la criticidad definida en el informe de análisis de vulnerabilidades.

A continuación se relacionan los tiempos en los que se atenderán las vulnerabilidades encontradas en la institución educativa en función de su clasificación: **niveles de acuerdo a servicio**

| Clasificación de la vulnerabilidad | Tiempo de atención |
|---|---|
| Crítica | 30 días hábiles |
| Alta | 30 días hábiles |
| Media | 60 días hábiles |
| Baja | 90 días hábiles |

## 13. PLAN DE CONTINUIDAD

### 13.1. Prevención:

Etapa donde se ejecutan actividades preventivas que tienen como objetivo medir y mantener actualizado el plan de continuidad del negocio y recuperación ante desastres.

- El análisis de impacto del negocio debe actualizarse cada un (1) año o cada vez que se presenten cambios en los procesos, nuevos productos o servicios.

- El monitoreo a los riesgos de continuidad se efectuará de manera anual en conjunto con la Autoevaluación de Riesgos y Controles de acuerdo con el programa de la Oficina de Riesgo Operativo,

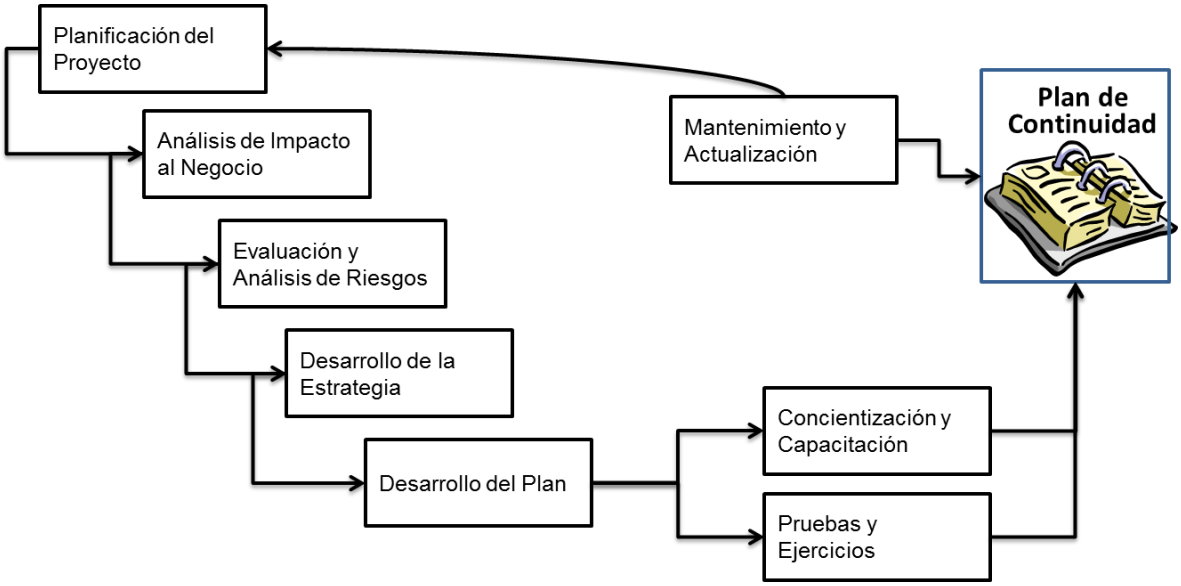
- Pruebas anuales deben realizarse a todas las estrategias de contingencia definidas.

- Las estrategias se revisarán cada vez que el Líder del Proceso lo considere o como resultado del análisis de riesgos se determine el ajuste o implementación de estrategias de contingencia.

## 13.2. Desarrollo

Para el desarrollo y mantenimiento del plan, se recomienda atender las definiciones, prácticas profesionales y metodología sugeridas por el Disaster Recovery Institute Internacional DRII de Estados Unidos y del Business Continuity Institute BCI del Reino Unido.

La siguiente gráfica ilustra el Plan de continuidad de negocio sugerido



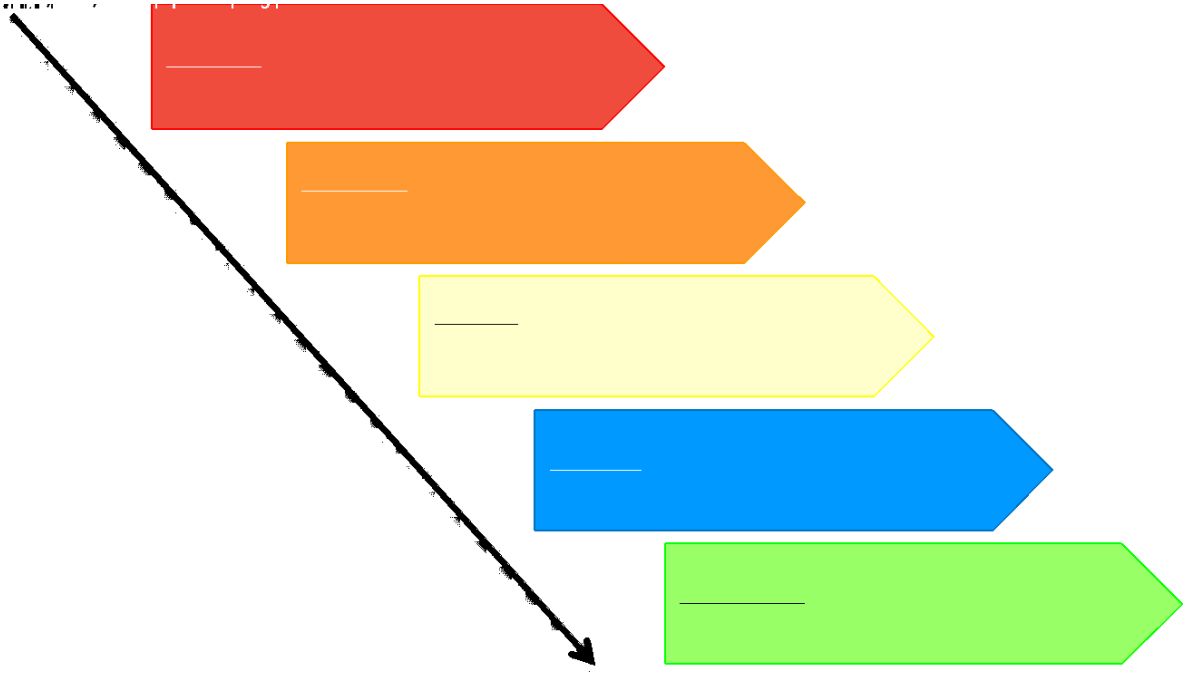

## 13.2.1. Planificación del proyecto:

Se definen las necesidades, el alcance y los objetivos del Plan de Continuidad de Negocio, la definición de responsabilidades, requerimientos para la capacitación del personal y los estándares internacionales que se alineará el PCN.

## 13.2.2. Análisis de Impacto del Negocio – BIA:

Este análisis permite determinar los productos y servicios críticos de la organización y el impacto relacionado con su interrupción, así como le identificación de la prioridad a los procesos y actividades claves y críticas para el negocio, así mismo permite establecer los tiempos de recuperación que deben ser establecidos por la organización: RTO (Recovery Time Objetive y RPO (Recovery Point Objetive) y la priorización de los procesos.

Los criterios de priorización recomendados son:



Considerando el Anexo 1 "Matriz de riesgos" de la presente política, los procesos prioritarios son aquellos que su nivel de criticidad y nivel de impacto son alto - medio, estos son:

- Procesos de la Dirección
- Procesos de Tesorería, Contabilidad y Administración Financiera
- Coordinación Académica y Salones de Clase
- Soporte técnico

### 13.2.3. Recursos:

Se definen los recursos de infraestructura, personal, software y hardware mínimos para para continuar operando, así mismo se identifican las aplicaciones y/o conexiones tecnológicas requeridas para la operación de los productos y servicios.

Considerando el Anexo 1 "Matriz de riesgos" de la presente política, los recursos prioritarios son aquellos que su nivel de criticidad y nivel de impacto son altos, estos son:

- Firewall Perimetral
- Controlador de Dominio
- Switch de servidores
- Switches de usuarios
- Servicio de internet
- Ingeniero de soporte técnico

### 13.2.4. Tiempos:

Se identifican los tiempos de inactividad que puede tolerar la Institución Educativa antes de colapsar, los tiempos críticos son los siguientes:

- **Punto Objetivo de Recuperación de Información (**Recovery Point Objective **RPO):** es la cantidad máxima de información que se puede perder cuando el servicio es restaurado tras una interrupción y que se está en la capacidad de reconstruir a través de otros medios, como las copias de respaldo. El RPO está

generalmente relacionado con la frecuencia con la cual se respalda la información.

- **Tiempo Objetivo de Recuperación (**Recovery Time Objective **RTO):** Período de tiempo después de un incidente en el que el producto o servicio debe ser reanudado con un nivel mínimo de servicio requerido.

- **Nivel mínimo de servicio (**Minimum Business Continuity Objective **MBCO):** es el nivel mínimo de servicio ofrecido sobre los productos y/o servicios durante un incidente de interrupción. Se expresa en términos de porcentaje, cantidad, cobertura, entre otros, dependiendo del tipo de producto.

- **Tiempo Máximo de interrupción aceptable (**Maximum Acceptable Outage **MAO):** es el tiempo que le tomaría a los impactos adversos que se materialicen frente a una interrupción de un proceso o producto, en alcanzar un nivel de impacto inaceptable para el negocio. Se conoce también como MTPD (Maximun Tolerable Period of Disruption).

Considerando el Anexo 1 "Matriz de riesgos" de la presente política, se calcula un valor por cada hora de indisponibilidad de un servicio lo que indica que para servicios críticos se deberían considerar los siguientes tiempos:

| **Tiempos Críticos** | | |
|---|---|---|
| **Tipo de tiempo** | **Tiempo** | **Justificación (Describa las razones por las cuales consideró que el tiempo estimado es el seleccionado)** |
| Tiempo Máximo de Interrupción Tolerable (MAO - Maximum Acceptable Outage) | 1 día | Se debe dar prioridad a las personas que se encuentran dentro de la institución, posteriormente se iniciará el plan de contingencia. |
| Nivel Mínimo de servicio (Minimum Business Continuity Objective - MBCO) | 20 % | La Institución Educativa puede operar con el personal Directivo, Contable y de Tecnología. |
| Tiempo de recuperación (Recovery time objective - RTO) | 1 día | La Institución Educativa no cuenta con un centro alterno por lo que la recuperación de los servicios puede tardar hasta 24 horas. |

## 13.2.5. Evaluación y análisis de riesgos:

La fase de gestión de riesgos tiene como objetivo principal identificar el daño potencial sobre el negocio, producido por una amenaza, la probabilidad realista de que esa amenaza se concrete y la identificación de medidas tendientes a mitigar los riesgos detectados.

En esta etapa se identifican y analizan las posibles amenazas y/o vulnerabilidades de personas, sistemas, infraestructura y procesos que podrían ocasionar riesgos de continuidad para la Institución, con el fin de medir el nivel del riesgo.

Esta información se encuentra en el documento análisis de riesgo que se realizó a la Institución Educativa.

Condiciones de emergencia bajo las cuales no se activarán los Planes de Continuidad

- Pérdida significativa de vidas del personal operativo durante un evento de desastre.

- Daño o compromiso estructural de las instalaciones que albergan los equipos tecnológicos u operativos, tanto principales como alternos, que pongan en riesgo la vida del personal.

- Imposibilidad de transitar en las vías públicas debido a eventos fortuitos (caída de puentes, caída de pasos elevados, capa asfáltica agrietada, derrumbes, aglomeraciones de personas en la vía, entre otras situaciones), durante o después de un desastre, que impidan el traslado del personal crítico a los sitios de trabajo primario o secundario previamente designados.

### 13.2.6. Desarrollo de la estrategia y desarrollo del plan:

Se identifican las alternativas de recuperación de las actividades criticas de la Institución Educativa en los tiempos definidos.

Estas alternativas se definen de acuerdo con los siguientes criterios:

- Criticidad del proceso a proteger
- Costo de la estrategia

- Tiempo de recuperación Objetivo (RTO)

Las diferentes situaciones para las cuales se deben definir estrategias de recuperación deben atender los riesgos identificados en el análisis de riesgos, para ello las estrategias sugeridas para la Institución Educativa son:

- Contingencia o estrategia de personas
  - Se debe establecer una personal directiva principal y suplente que pueda tomar decisiones del negocio.
- Contingencia o estrategia de centro alterno
  - Se recomienda tener un espacio alterno al edificio principal donde se pueda seguir operando.
- Contingencia o estrategia tecnológica
  - Se recomienda tener alta disponibilidad en la infraestructura tecnológica en lo posible en dos ubicaciones físicamente aisladas.
- Contingencia o estrategia operativa
  - Se debe establecer una persona operativa principal y suplente que conozca todos los procesos operativos de la Institución, así mismo acatar las recomendaciones de la política de respaldo de la información.
- Contingencia o estrategia de terceros

- Se deben tener contratos vigentes con los proveedores con acuerdos de prestación y niveles de servicio.

### 13.2.7. Concientización y capacitación:

Se deben ejecutar actividades de sensibilización y comunicación a través de las herramientas educativas con las que cuenta la Institución con el objetivo de que los funcionarios conozcan el plan de continuidad del negocio y recuperación ante desastres.

Por otro lado, se busca crear una cultura adecuada de la gestión del riesgo a lo largo de toda la Institución con el fin de que se pueda reaccionar a tiempo ante ciertas amenazas y que esta reacción sea lo más organizada y efectiva en la medida de lo posible y cumplan con los objetivos y tiempos de recuperación.

La sensibilización crea en los funcionarios, las habilidades para la detección oportuna de amenazas y vulnerabilidades asociados a los procesos y les ayuda a reconocer la necesidad de proteger los datos, las personas, la información, los medios utilizados para su procesamiento y demás herramientas empleadas en las labores diarias.

### 13.2.8. Pruebas y ejercicios:

Esta etapa consiste en probar la efectividad de las estrategias diseñadas y permitir el continuo mejoramiento del PCN de la Entidad (ver

Procedimiento Pruebas de Continuidad GR-GIR-D-052). Esta etapa le da a la Organización la oportunidad de identificar y prevenir problemas y fallas en el plan de continuidad de manera que puedan ser atendidas, preparando el negocio para la emergencia real.

La efectividad del Plan en situaciones de desastre se puede comprobar mediante la ejecución de una prueba que permita revisar dicha efectividad antes de enfrentarse a una situación real. La fase de pruebas debe considerar las actividades dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera teniendo en cuenta no poner en riesgo la operación real como consecuencia de esta prueba. Es también importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una crisis según su rol.

Por lo menos una vez en el año se debe realizar las pruebas del PCN. Cada una de las pruebas realizadas se deben dejar documentadas, con el fin de evidenciar la planeación y ejecución de la prueba, incluyendo las observaciones respectivas para definir las acciones de mejora.

A continuación, se presentan dos modelos de pruebas que permiten determinar hasta que punto funciona el plan:

- Restauración de una carpeta o archivo de un equipo de computo
- Alta disponibilidad del canal de internet

Para ejecutarlas puede seleccionarse la simulación de un escenario de prueba:

- No disponibilidad de la sede operativa.
- No disponibilidad del recurso humano crítico para la ejecución de los procesos priorizados.
- No disponibilidad de la plataforma tecnológica que soporta la operación.
- No disponibilidad de energía eléctrica.
- No disponibilidad de proveedores críticos.
- Combinación de los escenarios anteriores.

## 14. CIASIFICACIÓN DE LA INFORMACIÓN

### Descripción

La información en el Colegio Nuevo Gimnasio para efectos del manejo se clasifica de la siguiente manera: información reservada, información clasificada e información pública. El ciclo de vida de dicha información consta de tres etapas: generación, conservación y destrucción, por tanto, cada etapa contiene un procedimiento para garantizar su adecuado uso y confidencialidad. (Ver Manual que debe ser definido si no lo está - Gestión Documental).

## 14.1. Información reservada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

### 14.1.1. Información clasificada

Es considerada como aquella información perteneciente al Colegio Nuevo Gimnasio para el desarrollo propio de sus funciones, del cual su acceso es restringido o podría negarse salvo circunstancias legítimas y necesarias. Por lo tanto, esto obedece a lo establecido en el literal "C" del artículo 6 consagrado en la ley 1712 de 2014.

### 14.1.2. Información pública

Es todo registro, archivo o dato que se recopile, mantenga, procese o se encuentre en poder de entidades públicas y/o privadas, que sea de acceso libre. No tiene el carácter reservada o clasificada.

La Oficina TIC deberá apoyar a cada área los cuales desarrollarán los lineamientos para la clasificación de la información teniendo en cuenta lo siguiente:

- Los propietarios de la información son los encargados de realizar la clasificación de la información.
- El CNG definirá los niveles adecuados para clasificar su información de acuerdo con su sensibilidad donde se valorarán confidencialidad, integridad y disponibilidad de la información. Estos niveles deberán ser oficializados y divulgados a todos los colaboradores.
- Los propietarios y custodios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.
- Los colaboradores y terceras partes, deberán acatar los lineamientos que se definan frente a almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física del CNG.
- La información física y digital del CNG deberá tener un periodo de almacenamiento que puede ser dado por requerimientos legales o misionales; este periodo deberá ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información deberá ser eliminada o transferida adecuadamente.
- El CNG, por medio del área definida, deberá establecer los mecanismos necesarios para proteger la información catalogada como

Información pública reservada, teniendo en cuenta el medio en que se encuentre.

- La información pública clasificada y pública reservada deberá protegerse incluso en los ambientes de pruebas.
- Los funcionarios y contratistas del CNG no deben divulgar información pública clasificada o pública reservada a personas no autorizadas o a entes externos, a menos que se realice por el canal oficialmente establecido y con la aprobación previa del líder de proceso al cual pertenece el activo de información.
- La información del CNG no debe ser divulgada sin contar con los permisos correspondientes, además, ningún funcionario, contratista o proveedor debe copiarla o extraerla en el momento en que se retire del CNG o durante su permanencia.
- Los terceros, proveedores u operadores tecnológicos que accedan a la información del CNG, no deben hacer copias de la información suministrada por el CNG, ni podrán transferirla a otro equipo a través de la red, sin la autorización del dueño de la información.
- Los funcionarios y/o contratistas a los que se haya asignado un equipo de cómputo en el CNG, no debe almacenar información, como música, videos y fotos que no sean de carácter estrictamente institucional.

## 14.2. Responsabilidad por los activos

- El Líder del PSI o a quien este delegue deberá aplicar y mantener actualizada la documentación para el levantamiento y actualización de los activos de información del CNG.

- La identificación, clasificación y valoración de activos del CNG, deberá ser realizada por los Líderes de proceso y/o áreas definidas por el CNG, en el formato de registro de activos de información, de acuerdo con lo definido en la guía para la gestión de activos de información del CNG. Este proceso deberá actualizarse anualmente o previo a los cambios normativos vigentes.

- Los Líderes de los procesos o a quienes estos deleguen con el apoyo de la Oficina TIC deberán mantener un inventario de sus activos de información de forma anual y serán actualizados según el evento en que se requiera.

- Los Líderes de los procesos y/o áreas del CNG, serán los propietarios de los activos de información identificados para sus procesos.

- Los Líderes de los procesos y/o áreas deben establecer los controles de acceso para cada uno de los activos de información.

- El Líder del PSI o a quien este delegue, deberá remitir el consolidado del levantamiento de activos de información, al Profesional que lidera la estrategia o a quien haga sus veces, con el objetivo de ser analizada,

re-alimentada, actualizada y publicada de acuerdo a la normativa vigente.

- Los funcionarios, contratistas y usuarios de los activos de información y de la información del CNG deben:

▪ Aceptar y cumplir las políticas de seguridad de la información establecidas en el CNG.

▪ Proteger contra pérdida, modificaciones y acceso no autorizados a los activos de información del CNG.

▪ Comprender y aceptar sus responsabilidades frente al acceso a los diferentes sistemas de información que se tienen o administran en el CNG.

- Los Líderes de proceso y/o áreas del CNG deberán realizar la respectiva aceptación de los activos de información del proceso a su cargo, con el fin de establecer posteriormente los riesgos de seguridad digital a los que estos se vean expuestos.

- La Oficina TIC, debe establecer lineamientos para el uso y acceso a los recursos de tecnología del CNG "correo electrónico, internet, office 365 entre otros".

- En caso de que un colaborador deba hacer uso de equipos ajenos al CNG, estos deberán cumplir con la legalidad del software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red del CNG una vez esté avalado por la Oficina TIC.

- El único servicio de correo electrónico autorizado para el manejo de la información institucional en el CNG es el que cuenta con el dominio@colegionuevogimnasio.edu.co.

- Las firmas de documentos oficiales que reposan en expedientes, y que se constituyen como activos de información deben reposar en original o su con firma digital que corresponda, en ningún caso se debe utilizar firmas digitalizadas o escaneadas.

- El CNG se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus funcionarios o contratistas, además podrá realizar copias de seguridad en cualquier momento, así como limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información del CNG o de terceros operados en el mismo por solicitud expresa del CNG, Jefes de Procesos y/o áreas, Directores, Subdirectores y Coordinadores de Grupo a la Oficina TIC.

- Con el fin de mitigar la suplantación de la identidad de correos electrónicos, se prohíbe suministrar acceso directo a los buzones de

correo institucional asignado a cada colaborador. En caso de ser necesario realizar la gestión del correo institucional, se debe solicitar a la mesa de servicios listando los colaboradores que tendrán los permisos para escribir correos en nombre del colaborador solicitante.

- No se permite el almacenamiento en los equipos de cómputo y medios de almacenamiento propiedad del CNG, el almacenamiento de archivos de multimedia (Audio, video, Imágenes), programas ejecutables, o cualquier tipo de archivo que no sea de carácter institucional.

- Únicamente se permitirá el acceso a las aplicaciones y sistemas de información autorizados por el CNG, de esta manera evitar la ejecución de software no licenciado el cual atente contra los derechos de autor y propiedad intelectual según como lo regula la ley.

- El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Jefes de área o dependencia.

- Para la consulta de documentos adjuntados en los software de gestión documental, se establecerán privilegios de acceso a los funcionarios y/o contratistas de acuerdo con el desarrollo de sus

funciones y competencias. Dichos privilegios serán establecidos por el Jefe o Director del área, quien comunicará al Grupo encargado de la administración del software el listado con los funcionarios y sus privilegios.

- EL CNG debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo del CNG es responsabilidad de la Oficina TIC, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación del software deben ser los proporcionados por el CNG a través de esta oficina.

- La Oficina TIC debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

- La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una

conexión a la infraestructura tecnológica del CNG, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Oficina TIC.

- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del CNG; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Oficina TIC.

- Los colaboradores y terceras partes deberán devolver todos los activos de información del CNG que se encuentran en su poder a la terminación de su empleo, contrato, convenio o acuerdo.

- Para el traslado de equipos de cómputo al almacén o a otros colaboradores, o baja de los inventarios por cualquier motivo, se deberá realizar un respaldo de la información que en él se encuentre a través de la Oficina TIC. Cuando el dispositivo se vaya a dar de baja la Oficina TIC debe realizar el borrado seguro de la información que contengan medios de almacenamiento con el fin de propender que la información del CNG contenida en estos medios no se pueda recuperar.

- Cuando se realice el traslado de equipos de cómputo a otros colaboradores, se deberá instalar de nuevo el sistema operativo y los programas de la línea base.

- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Oficina TIC, sin embargo, cuando deba realizarse desde y hacia el almacén será el Grupo de Recursos Físicos y/o personal definido por el CNG, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes del CNG.

## 14.3. Manejo de medios

- El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, memorias flash, USBs, Ipods, celulares, y semejantes) sobre la infraestructura para el procesamiento de la información del CNG, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

- La Oficina TIC debe definir un procedimiento para el uso de medios removibles e implementar los controles necesarios para su uso.

- Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información del CNG que este contiene.

- Bajo ninguna circunstancia se dejarán desatendidos los medios de almacenamiento o copias de seguridad de los sistemas de información.

- Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la red del CNG.

- Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.

- Se prohíbe el uso de medios removibles en lugares de acceso al público que contengan
información reservada o clasificada del CNG.

- El Grupo de Recursos Físicos deberá crear un procedimiento para la disposición final de residuos de aparatos electrónicos.

- La Oficina TIC deberá propender por que el procedimiento de almacenamiento de información (backup) cuente con las condiciones para asegurar la confidencialidad, integridad y disponibilidad de la información en custodia.

- Los medios y equipos donde se almacena y procesa información deben mantenerse con las medidas de protección físicas, lógicas y condiciones dadas por los fabricantes, que permitan un adecuado funcionamiento.

- El uso de medios removibles será restringido, en caso de requerir su uso deberá ser solicitado por la parte interesada de manera formal a través de la mesa de servicio y/o mesa de ayuda, posteriormente autorizado por la Oficina TIC teniendo en cuenta lo siguiente:

  - Definir en qué condiciones o casos se permitirá el uso (procedimiento guía o instructivo).

  - La Oficina TIC deberá mantener un registro de los dispositivos y/o medios removibles autorizados.

  - El uso de medios removibles deberá emplear métodos para el cifrado de información, para ello la Oficina TIC deberá indicar los medios de cifrado, esto con el fin de evitar la pérdida y fuga de información institucional de carácter clasificada o reservada.

- Los medios que requieran ser eliminados, dar de baja o ser reasignados deberán sometidos a un proceso de borrado seguro y demás mecanismos que puedan considerarse, con el fin de evitar la

recuperación de la información que alguna vez estuvo contenida en estos medios.

- Los equipos que se regresen al almacén para asignarse a otro colaborador o para dar de baja, se les deberá ejecutar el procedimiento de borrado seguro o en caso de no poder realizar el borrado seguro validar el procedimiento para la disposición final de residuos de aparatos electrónicos RAEE.

- Es requisito realizar el respaldo o copia de la información contenida en el equipo, previa ejecución del procedimiento de borrado seguro.

- Cuando se requiera transferir un medio de almacenamiento de información del CNG a otras entidades se deberán establecer un acuerdo entre las partes. Dichos acuerdos deberán dirigirse a la transferencia segura de información de interés entre el CNG y las partes.

- El transporte para los medios de almacenamiento deberá contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información.
- Toda información propiedad del CNG de tipo clasificada y/o reservada, almacenada en los diferentes medios y que requieran ser transportados a otras locaciones ajenas a la entidad, deberá cumplir con los lineamientos de seguridad establecidos por la Oficina TIC.

# 15. COPIAS DE RESPALDO O BACK-UP

## Descripción

La organización debe contar con un plan y un procedimiento formales para la realización de los respaldos, para garantizar que la información pueda ser reconstruida en caso de pérdida u otra necesidad.

Los propietarios del activo determinarán la frecuencia y tiempo de retención del respaldo, teniendo en cuenta el marco normativo aplicable, así como la valoración del activo a fin de minimizar la pérdida o destrucción total o parcial del mismo, su disponibilidad y confidencialidad. Esta información debe reflejarse en el plan y procedimiento de respaldos.

Los respaldos deben ser probados en intervalos regulares a los efectos de garantizar su confiabilidad ante la necesidad de uso en caso de emergencia. Se debe definir un procedimiento de prueba de respaldos, así como la periodicidad de su ejecución.

Se debe tener en consideración la confidencialidad de la información y en caso que sea requerido, los respaldos deberán estar cifrados de conformidad con la política establecida.

El organismo debe disponer de un lugar adecuado para el almacenamiento seguro de los respaldos que sea consistente con las medidas de protección ambiental del sitio principal.

Se debe contar con respaldos fuera del sitio principal (off-site), conservando las condiciones ambientales consistentemente con las del sitio operativo y con controles de seguridad física adecuados. Debe definirse un procedimiento donde se defina la frecuencia y las actividades necesarias para la transferencia de los respaldos fuera del organismo.

## 15.1. Copias de respaldo

- El CNG debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Oficina TIC y las dependencias responsables de la misma, contenida en la plataforma tecnológica del CNG, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente respaldada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

- La Oficina TIC establecerá procedimientos o un plan de copia de seguridad del CNG donde se establezca esquemas de qué, cuándo, con qué periodicidad, cual es la criticidad explícitos de respaldo, número de copias y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información respaldada.

- La Oficina TIC deberá realizar y mantener copias de seguridad de la información digital solicitadas por el Líder funcional o Líder técnico.

- La Oficina TIC deberá definir la custodia y almacenamiento de las copias.

- La Oficina TIC deberá tener un inventario y bitácora de las copias que se realizan y de las copias que se restauran.

- La Oficina TIC deberá dar los lineamientos para la realización de las copias de seguridad de:

- Bases de datos en producción.
- Software de aplicaciones.
- Sistemas operativos.
- Software base del CNG.
- Cuentas de correo electrónico con valor estratégico para el CNG (Administrativos, Docentes, Asesores, Directores, Administradores de Sistemas, entre otros).

- La Oficina TIC deberá generar mecanismos que mantengan la integridad y confidencialidad de las copias de seguridad.

- La Oficina TIC deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

- Los colaboradores son responsables de la información que resida en el computador asignado y serán los encargados de mantener copia de sus archivos más sensibles entregando al supervisor del contrato o jefe inmediato en custodia al finalizar la vinculación. En caso de que los colaboradores requieran la ejecución de un respaldo de información, lo pueden solicitar a la Oficina TIC a través de la mesa de servicios y/o mesa de ayuda.

- Las copias de seguridad de la información (back-up), deberán ser almacenadas dentro y fuera del CNG, como medida preventiva para asegurar la recuperación total de los datos. En caso de tener una sola copia debe ser llevada fuera de la sede o sitio del procesamiento de datos. El traslado de los medios y/o dispositivos debe ser realizado por personal debidamente autorizado, teniendo en cuentas las medidas de seguridad.

- Los medios magnéticos con al menos una de las copias que contienen la información crítica, deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

## 16. RELACIONES CON LOS PROVEEDORES

### 16.1. Seguridad de la información en las relaciones con los proveedores

- Los contratos deberán establecer lineamientos para el cumplimiento de las obligaciones contractuales del SGSI con terceros o proveedores.

- Los contratos deberán establecer en el momento de suscribirse contratos de apoyo a la gestión que se desarrollen dentro del CNG, los riesgos asociados a la seguridad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información del CNG.

- Los contratos con terceros y proveedores deberán establecer los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.

- La Oficina TIC deberá establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.

- Cada dependencia del CNG que establezca relación con proveedores y su cadena de suministro, solicitará capacitación periódica a la Oficina TIC referente a seguridad de la información con el fin de dar a conocer las políticas que tiene el CNG.

- Todos los proveedores, usuarios externos y funcionarios de entidades externas deben estar autorizados por un funcionario del Ministerio quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales.

## 16.2. Gestión de la prestación de servicios de proveedores

- La Oficina TIC deberá documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica del CNG.

- Las cuentas de proveedores y usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo a la naturaleza del usuario.

- Los proveedores y usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI del CNG.