POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Código: SI-DG-01

Versión: 12

Interconectamos a las comunidades y regiones para el progreso y bienestar del País.

CONTENIDO

* * *

Esta Política fue aprobada inicialmente por la Junta Directiva mediante el acta N° 389 del 19 de septiembre del 2023 y emitida el 27 de septiembre de 2023.

Las *amenazas*[1] que vulneran la Seguridad de la Información y Ciberseguridad pueden afectar considerablemente la reputación de Proyectos de Infraestructura S.A.S (en adelante PISA), así como sus activos de información más importantes. Conscientes de las consecuencias, y como respuesta a su compromiso en la preservación de los *pilares de Seguridad de la Información*[2] y Ciberseguridad, PISA desarrolla la presente política para proteger y garantizar la *disponibilidad*[3], *confidencialidad*[4], *Integridad*[5] y *privacidad*[6] de la información y el establecimiento, implementación, mantenimiento y mejora continua de su sistema de gestión de *Seguridad de la Información*[7] y *Ciberseguridad*[8].

Por lo tanto, los *colaboradores*[9] de PISA deben actuar teniendo en cuenta los lineamientos consignados en esta Política y en las normas, estándares y procedimientos que la desarrollen.

1 Finalidad

1.1 Objetivo general

Proteger los activos de información estratégicos de PISA, gestionando y cumpliendo los principios generales que preservan la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información, mediante la definición de políticas, identificación de *riesgos*[10] y *controles*[11], que fijan roles y responsabilidades de los actores clave, que intervienen en el *Sistema de Gestión de Seguridad de la Información*[12] (SGSI).

1.2 Objetivos específicos

- Establecer los lineamientos para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información y ciberseguridad en PISA.
- Definir de qué manera la información debe ser protegida de forma homogénea con base en la valoración de los activos críticos de información de PISA.
- Garantizar la gestión de riesgos de Seguridad de la Información y Ciberseguridad en PISA.
- Establecer e implementar los controles que preserven la confidencialidad, integridad, disponibilidad y privacidad de la información en PISA.
- Fijar roles y responsabilidades de autoridades de control en materia de los pilares de Seguridad de la Información y Ciberseguridad de PISA.
- Garantizar la aplicación de los requisitos de Seguridad de la Información y Ciberseguridad en la continuidad del negocio y la recuperación ante desastres en PISA.
- Definir el marco general para gestionar el Sistema de Gestión de Seguridad de la Información (SGSI) que se adapte a los requerimientos del negocio y que esté acorde a los lineamientos establecidos en esta política.

2 Ámbito de aplicación

La presente política de Seguridad de la Información y Ciberseguridad aplica a todos los colaboradores y terceros que en el ejercicio de sus funciones utilicen información y servicios tecnológicos de PISA.

[1] **Amenaza:** causa potencial de un incidente no deseado, el cual puede causar daños a un sistema o a la organización.
[2] **Pilares de Seguridad de la Información**: principios o características de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad).
[3] **Disponibilidad**: la información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.
[4] **Confidencialidad**: hace referencia a la protección de información cuya divulgación no está autorizada.
[5] **Integridad**: la información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
[6] **Privacidad**: propiedad de la información que garantiza el uso adecuado de la misma, así esté legítimamente autorizado a manejarla.
[7] **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. También denominada el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para preservar los pilares de la información, que se almacene, reproduzca o procese en los sistemas informáticos de PISA.
[8] **Ciberseguridad:** Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de PISA.
[9] **Colaboradores**: trabajadores incluyendo Alta Gerencia, practicantes y aprendices de PISA.
[10] **Riesgo**: la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.
[11] **Control**: medida que tome la entidad y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.
[12] **Sistema de gestión de Seguridad de la Información y Ciberseguridad**: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

3 Principios básicos de actuación

PISA ha establecido como fundamentales los siguientes principios que soportan la Política de Seguridad de la Información y Ciberseguridad:

- La información es uno de los activos más importantes de PISA y por lo tanto debe utilizarse acorde con los requerimientos del negocio y conservando criterios de calidad (Efectividad, Eficiencia y Confiabilidad).
- La confidencialidad de la información de PISA, así como aquella perteneciente a terceros, debe mantenerse, independientemente del medio o formato donde se encuentre.
- La información de PISA debe preservarse en su integridad, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.
- La información de PISA debe estar disponible cuando sea requerida y por quienes tengan autorización de utilizarla. Así mismo debe presentarse de forma oportuna cuando por requisitos legales y reglamentarios así se requiera.
- La privacidad de la información de PISA debe preservarse.
- Los eventos que ocurren al tener acceso a la información de PISA deben dejar rastro y permitir la reconstrucción, revisión y análisis de la secuencia de estos.

4 Declaración de compromiso

PISA está comprometida con la Política de Seguridad de la Información y Ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los principios establecidos por el sistema de gestión de Seguridad de la Información y Ciberseguridad; por lo anterior se compromete a:

- Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la política de Seguridad de la Información y Ciberseguridad.
- Promover continuamente una cultura de Seguridad de la Información y Ciberseguridad.
- Gestionar de manera estructurada y estratégica los riesgos de Seguridad de la Información y Ciberseguridad asociados al negocio y su relacionamiento con terceros.

Por otro lado, cada colaborador y proveedor, es responsable por aplicar los criterios definidos en esta Política y por ajustar sus actuaciones de acuerdo con los valores de PISA y los lineamientos establecidos en Seguridad de la Información y Ciberseguridad; de igual forma es responsable de reportar los incidentes de los que pudiera llegar a tener conocimiento.

5 Marcos de referencia

Como mejores prácticas del mercado, son utilizados los siguientes marcos de referencia (no es un listado taxativo):

NTC-ISO-IEC 27001:2013: Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de Seguridad de la Información, dentro del contexto de la organización. La presente norma también incluye los requisitos para la valoración y el tratamiento de riesgos de Seguridad de la Información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para aplicarse a todas las organizaciones independientemente de su tipo, tamaño o naturaleza.

ISO/IEC 27000: Es un grupo de estándares internacionales titulados: Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Visión de conjunto y vocabulario. Tiene como fin ayudar a las compañías de todo tipo y tamaño a implementar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27701: Estándar que especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de privacidad de la información.

Framework de Ciberseguridad NIST: Marco de trabajo basado en estándares, directrices y prácticas existentes para que las compañías gestionen el riesgo de Ciberseguridad.

6 Políticas generales de seguridad de la información y ciberseguridad entorno al riesgo

PISA reconoce la importancia de proteger adecuadamente la información de amenazas que puedan afectar la continuidad del negocio. Por lo anterior establece el desarrollo de actividades para la protección de los activos de información, gestión y administración de riesgos de Seguridad de la Información y Ciberseguridad, protección de datos personales, cultura de seguridad

y las conductas que deben adoptar todos los colaboradores y terceros que en el ejercicio de sus actividades utilicen información y servicios tecnológicos de PISA, los cuales deben velar por el cumplimiento de los requisitos y pilares de la Seguridad de la Información y Ciberseguridad, protegiendo los activos de información de PISA, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información; por lo anterior, PISA acoge las siguientes políticas sobre las cuales se fundamenta y estructura el Sistema de Gestión de Seguridad de la Información (SGSI). Tales Políticas son expresiones de la gerencia para una presentación y valoración justa y transparente de riesgos de Seguridad de la Información y Ciberseguridad. Lo anterior permite hacer una adecuada identificación de los controles que mitigan razonablemente los riesgos identificados.

En virtud de lo anterior, en caso de que PISA tenga relaciones con terceros que en el ejercicio de sus actividades utilicen información y servicios tecnológicos de PISA, se debe dar cumplimiento a la Instrucción Seguridad de la Información y Ciberseguridad - Modelo Cláusula Certificación de Proveedor Crítico emitida por Grupo Aval, Instrucción que se adapta a las condiciones de PISA.

6.1 Proteger la Confidencialidad, Integridad, Disponibilidad , Privacidad y no repudio de la Información

Todos los colaboradores de PISA deben proteger y asegurar, la confidencialidad, integridad, disponibilidad y privacidad de la información, de tal manera que la información:

- Solo sea accedida por personal autorizado.
- Sea concisa, precisa, incidiéndose en la exactitud.
- Esté disponible en el momento que sea requerida.
- Sea accedida legítimamente y utilizada para lo que se autorizó.

6.2 Adoptar y mantener una sólida cultura de Seguridad de la Información y Ciberseguridad

Las tres líneas deben tomar la iniciativa en el establecimiento de una sólida cultura de Seguridad de la Información y Ciberseguridad donde:

- La primera línea debe ser ejemplo y replicador de una sólida cultura y conciencia en Seguridad de la Información y Ciberseguridad, en el cumplimiento de políticas y procedimientos organizacionales definidos.
- La segunda línea debe definir y ejecutar las actividades de concientización y cultura, que abarquen a todos los colaboradores, sobre las políticas y procedimientos organizacionales de Seguridad de la Información y Ciberseguridad.
- La tercera línea debe monitorear la ejecución y el cumplimiento de la cultura y concientización de Seguridad de la Información y Ciberseguridad.

6.3 Implementar y mantener un sistema de gestión integral de riesgos de Seguridad de la Información y Ciberseguridad.

Todos los colaboradores de PISA deberán utilizar un marco de control interno generalmente aceptado donde defina los elementos que se espera que estén presentes y funcionando en un sistema de control interno efectivo. Para el efecto se deberá alinear con la metodología de Administración de Riesgo Operativo - SARO (evaluación *riesgo inherente*[13], *riesgo residual*[14] y mapa de calor) y con las Metodologías de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad.

6.4 Determinar el Apetito de Riesgo, el nivel de tolerancia y la capacidad de riesgo

La Alta Dirección y la segunda línea de PISA deberán determinar el *Apetito de Riesgo*[15], el nivel de tolerancia y la capacidad máxima al riesgo, considerando el efecto de la naturaleza de sus operaciones, así como los tipos y niveles de riesgo de Seguridad

[13] **Riesgo Inherente (RI)**: nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. En otras palabras, Riesgo Inherente es la probabilidad de que una Entidad pueda incurrir una pérdida material como resultado de su exposición a, y de la incertidumbre que surge de, potenciales eventos adversos. El RI es intrínseco a cada actividad significativa y se evalúa sin tener en consideración el tamaño de esta en relación con la organización y antes de evaluar la calidad de la administración de los riesgos que ésta realiza. Para identificar y evaluar los RI a los que está expuesta una organización es esencial tener un conocimiento profundo tanto de la naturaleza de las actividades que ésta realiza como del entorno en el que opera.

[14] **Riesgo Residual**: también conocido como riesgo neto, es el resultado de la mitigación de los riesgos inherentes por parte de la gestión operativa y las funciones de supervisión. En otras palabras, es el riesgo que permanece tras haberse ejecutado los controles y se hayan tomado las medidas preventivas para dar respuesta a los riesgos identificados.

[15] **Apetito de Riesgo**: es la exposición al nivel de riesgo que una entidad está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su plan de negocios.

de la Información y Ciberseguridad que PISA está dispuesta a asumir en cada uno de estos niveles. La Junta Directiva deben aprobar el Apetito de Riesgo, el nivel de tolerancia y la capacidad máxima al riesgo.

En virtud de lo anterior, y como un mecanismo para limitar la exposición de PISA en casa de materializarse un riesgo de Seguridad de la Información y Ciberseguridad, se debe dar cumplimiento a la Instrucción Seguridad de la Información y Ciberseguridad - Criterios Póliza Ciberseguridad emitida por Grupo Aval, Instrucción que se adopta para todos los efectos.

6.5 Evaluación de riesgos de Seguridad de la Información y Ciberseguridad

PISA debe contar con un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de Seguridad de la Información y Ciberseguridad. Este proceso se hace por lo menos una vez al año o cuando circunstancias especiales ocurran, identificando riesgos y evaluando su probabilidad e impacto, el cual debe estar alineado con las Metodologías Corporativas de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad.

En virtud de lo anterior, se debe dar cumplimiento a las Instrucciones Seguridad de la Información y Ciberseguridad - Actualización Metodología Gestión de Riesgo, Inventario de Riesgos Genéricos y Línea Base de Controles, Instrucciones emitidas por Grupo Aval, las cuales se adoptan junto con los documentos anexos a dichas Instrucciones.

6.6 Supervisar la Administración del Sistema de Gestión de Seguridad de la Información y Ciberseguridad

La Alta Dirección y la segunda línea deben establecer, aprobar y revisar periódicamente el "Sistema de Gestión de Seguridad de la Información y Ciberseguridad". Así mismo, deben supervisar a la *Administración*[16] para asegurarse de que las políticas, procesos y sistemas se aplican eficazmente en todos los niveles de decisión.

6.7 Gestionar el cambio

La Alta Dirección y la segunda línea deben asegurar que haya un proceso de aprobación que evalúe plenamente los riesgos de Seguridad de la Información y Ciberseguridad en todos los nuevos procesos, actividades, productos y sistemas críticos, así como que se identifiquen nuevas amenazas. Por ejemplo, cada vez que se realicen cambios sobre alguna aplicación que impacte el negocio, se lleva a un comité de cambios donde se evalúan los posibles riesgos que traería la implementación de dicho cambio.

6.8 Realizar Seguimiento y Presentar Informes

La segunda línea debe implementar un proceso para monitorear regularmente los perfiles de riesgo de Seguridad de la Información y las exposiciones a pérdidas importantes. Adicionalmente debe realizar un diagnóstico de Seguridad de la Información basados en normas, estándares y marcos de referencia que respalden la gestión de Seguridad de la Información y Ciberseguridad ISO 27000 y Framework de Ciberseguridad NIST con el fin de calcular el nivel de seguridad y madurez en el que ese encuentra PISA, establecer Indicadores para el monitoreo del sistema, monitorear la evolución de riesgos y de controles. De manera específica deberán trabajarse en este mismo sentido los riesgos de Ciberseguridad.

En virtud de lo anterior, se debe dar cumplimiento a la Instrucción Seguridad de la Información y Ciberseguridad - Tablero Control Seguridad de la Información emitida por Grupo Aval, Instrucción que se adopta junto con el documento anexo a dicha Instrucción.

6.9 Controlar y mitigar

La primera y segunda línea de PISA deben tener un fuerte "ambiente de control", estructurado mediante políticas, procedimientos, estándares, sistemas, controles internos adecuados y la ponderada mitigación o compensación de riesgos.

Con lo anterior, la primera línea debe contar con controles generales de accesos, privilegios, actualizaciones en los siguientes aspectos mínimos:

- Supervisión de controles de accesos físicos.
- Supervisión de controles de accesos lógicos.
- Supervisión y protección de contraseñas.
- Supervisión protección de los puertos de configuración y acceso remoto.
- Restricción de la instalación de aplicaciones por parte del usuario final.

[16] **Administración**: Gerente General y Gerentes de áreas.

- Asegurar que los sistemas operativos estén "parchados" con las actualizaciones o en su defecto que los controles implementados mitiguen la posibilidad de materialización de un incidente.
- Asegurar que las aplicaciones de software se actualicen regularmente.
- Restricción de los privilegios administrativos (es decir la capacidad de instalar software o cambiar los ajustes de configuración de una computadora).

6.10 Asegurar que el sistema de Gestión de Seguridad de Información y Ciberseguridad opera en situaciones de contingencia

La segunda línea debe velar porque en los planes de continuidad del negocio se incluyan y se implementen los controles necesarios sobre los pilares de la Seguridad de la Información y Ciberseguridad.

6.11 Garantizar el cumplimiento de la Ley vigente aplicable

Es obligación de las tres líneas de PISA dar cumplimiento a todas las normas de los reguladores vigentes que le aplique a PISA, relacionadas con seguridad de la información y ciberseguridad.

7 Políticas individuales (adaptadas de la política corporativa de Corficolombiana)

7.1 Seguridad de la Información y Ciberseguridad

La información del negocio es un activo vital de la Compañía y por lo tanto debe ser protegida

La información de PISA sin importar su presentación, medio o formato en el que sea creada o utilizada para el soporte de las operaciones de PISA, se califica como activo de información y por lo tanto debe ser protegida.

La Seguridad de la Información y la Ciberseguridad de PISA es el conjunto de medidas de protección que toma PISA contra la divulgación, modificación, hurto o destrucción accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en que se pueda ver comprometida.

Los Responsables de la Información deben asegurar que la información de PISA cuenta con la protección apropiada para así preservar la confidencialidad, integridad, disponibilidad y privacidad de esta.

PISA debe disponer de los medios necesarios para asegurarse que cada colaborador preserve y proteja los *activos de información*[17] de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer, o sobrepasar cualquier control de seguridad será sujeto de las acciones disciplinarias correspondientes.

PISA debe contar con una estructura organizacional de Seguridad de la Información y Ciberseguridad que permita gestionar y controlar lo dispuesto en el Modelo de Seguridad de la Información y Ciberseguridad.

7.2 Propiedad intelectual

La propiedad de la información se debe mantener

La propiedad intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de PISA.

Todo el material que es desarrollado mientras se trabaja para PISA, se considera que es de su propiedad intelectual y de uso exclusivo de PISA. Por lo tanto, debe ser protegido contra un develado, descubrimiento o uso que menoscabe la competitividad de PISA.

7.3 Responsables de la información

Cada activo de información de la Compañía debe tener un responsable que debe velar por su seguridad con base en los riesgos a los que está expuesta

PISA utiliza información para realizar sus actividades. Esta se crea y se entrega a cada colaborador para que pueda desarrollar y cumplir sus respectivas metas dentro de las funciones desarrolladas.

[17] **Activos de Información:** conocimiento o datos que tienen valor para la entidad o el individuo.

La información que PISA utilice para el desarrollo de sus objetivos debe tener asignado un responsable. Cada área y/o proceso debe actuar como Responsable de la Información, ejerciendo así la facultad de aprobar o revocar el acceso a la información a su cargo, tomando las decisiones que sean requeridas para la protección de la información y determinando quiénes son los usuarios autorizados y sus privilegios de uso. En PISA actuarán como Responsables de la Información, los Gerentes, Directores, Coordinadores y demás titulares de las dependencias que reporten directamente a la Gerencia General o a quienes éstos deleguen.

7.4 Cumplimiento de regulaciones

La Compañía debe cumplir con las regulaciones locales e internacionales de privacidad y seguridad de la información y Ciberseguridad

La Política de Seguridad de la Información y Ciberseguridad está acorde y apoya el cumplimiento de las leyes y regulaciones locales e internacionales relativas a la seguridad de la información y ciberseguridad. Por lo tanto, tales requerimientos deben ser incluidos en el desarrollo del Modelo de Seguridad de la Información y Ciberseguridad y se deben establecer acciones específicas para mantener alineada permanentemente la Política de Seguridad de la Información y Ciberseguridad de PISA con tales disposiciones.

Así mismo y con el fin de mantener un buen nivel de seguridad, esta Política se debe apoyar en las mejores prácticas de seguridad de la información y ciberseguridad.

7.5 Administración del riesgo en Seguridad de la Información y Ciberseguridad

Los riesgos de Seguridad de la Información y Ciberseguridad a los que está expuesta la información de la Compañía deben ser identificados, evaluados y mitigados acorde con su valor, probabilidad de ocurrencia e impacto en el negocio

La información de PISA se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, a través del Comité de Seguridad de la Información y Ciberseguridad, se debe realizar periódicamente un análisis del estado del negocio frente a la seguridad de la información y ciberseguridad, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo Responsable de la Información.

Establecidos el nivel de riesgo y el valor de la información, cada Responsable de la Información debe realizar una evaluación formal de riesgos, para que estos sean identificados y evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos y definidos en la Matriz de Riesgos control de Seguridad de la Información y ciberseguridad de PISA.

Cada colaborador de PISA debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información de PISA y deben reportar inmediatamente cualquier sospecha u observación de un incidente que afecte la seguridad de la información y la ciberseguridad.

7.6 Capacitación y creación de cultura en Seguridad de la Información y Ciberseguridad

La Compañía debe establecer un programa permanente de creación de cultura en Seguridad de la Información y Ciberseguridad para los colaboradores y terceros.

PISA debe contar con un programa permanente que permita asegurar que los colaboradores y terceros están informados acerca de sus responsabilidades en seguridad de la información y ciberseguridad y de las continuas amenazas que ponen en riesgo la información que maneja.

Los colaboradores y terceros deben estar enterados de los procedimientos de seguridad de la información y ciberseguridad que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo. Como parte de su programa de capacitación, el nuevo personal debe asistir durante el periodo de inducción a una charla sobre los requerimientos de seguridad de la información y ciberseguridad de PISA.

7.7 Seguridad en el personal

La Compañía debe proveer los mecanismos necesarios para asegurar que sus colaboradores cumplan con sus responsabilidades en seguridad de la información y ciberseguridad desde su ingreso hasta su retiro

La Política de Seguridad de la Información y Ciberseguridad debe estar disponible para ser consultada por parte de los colaboradores de PISA. Igualmente, todo colaborador de PISA debe certificar el conocimiento y entendimiento de la Política de Seguridad de la Información y Ciberseguridad de PISA.

La carpeta del colaborador debe incluir el compromiso de confidencialidad de usuarios de aplicativos, herramientas o información de PISA donde indican las responsabilidades correspondientes para con la seguridad de la información y ciberseguridad.

7.8 Terceros que acceden a la información de la Compañía de forma local o remota

Los terceros que utilizan local o remotamente información de la Compañía deben cumplir con la política de Seguridad de la Información y Ciberseguridad

El uso de la información de PISA por terceros ya sea que se encuentre en los aplicativos locales o en el *ciberespacio*[18] y se acceda de forma local o remota, debe ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política. En los contratos se debe incluir la obligación de proteger la información de PISA, los requisitos de seguridad para mitigar los riesgos sobre la información y Ciberseguridad y las consecuencias a que estarían sujetos en caso de incumplirla.

En virtud de lo anterior, se debe dar cumplimiento a la Instrucción Seguridad de la Información y Ciberseguridad - Actualización Cláusula Ciberseguridad emitida por Grupo Aval, Instrucción que se adopta para todos los efectos.

7.9 Identificación y autenticación individual

Todos los colaboradores y terceros que acceden a la información de la Compañía deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal

Todo colaborador o tercero es responsable por sus acciones mientras usa cualquier recurso de información de PISA. Por lo tanto, la identidad de cada usuario de los recursos informáticos deberá ser establecida y autenticada de una manera única y no podrá ser compartida.

Los usuarios, una vez creados y asignadas sus autorizaciones en los sistemas de información, podrán acceder a la información mediante su usuario y clave de autenticación. Dependiendo del valor de la información y del nivel de riesgo, PISA definirá medios de autenticación apropiados. Dichos medios de autenticación contienen información confidencial que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

7.10 Control y administración del acceso a la información local o en el ciberespacio

El uso de la información de la Compañía debe ser controlado para prevenir accesos no autorizados. Los privilegios sobre la información deben ser mantenidos en concordancia con las necesidades del negocio, limitando el acceso solamente a lo que es requerido

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información se mantengan protegidos localmente y en el ciberespacio de una manera consistente con su valor para PISA y con los riesgos de pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información.

Los derechos de acceso no deben comprometer la segregación de tareas y responsabilidades. El acceso realizado localmente y/o por el ciberespacio a la información de PISA deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de PISA debe ser restringido en todos los casos, y se debe dar específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.

7.11 Clasificación de la información

Los responsables de la información deben clasificar la información basados en su valor, sensibilidad, riesgo de pérdida o compromiso, y/o requerimientos legales de retención

Al igual que otros activos, no toda la información tiene el mismo uso o valor, y por consiguiente requiere diferentes niveles de protección. Toda la información de PISA será clasificada por el Responsable de la Información con base en un análisis de alto nivel del impacto al negocio en seguridad de la información, que determine su valor relativo y nivel de riesgo a que está expuesta.

Según los riesgos que se detecten, el Responsable de la Información y el Oficial de Seguridad de la Información, determinarán los controles que sean necesarios para proveer un nivel de protección de la información apropiado y consistente en toda PISA, sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

[18] **Ciberespacio**: entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

Por lo tanto, es deber de todos los colaboradores de PISA tomar las medidas necesarias para proteger la información utilizada en sus procesos de negocios y no se debe asumir que otros protegen la información, ya que es deber de los colaboradores de PISA tomar las medidas necesarias para proteger la información.

Cuando el tipo de la clasificación de la información corresponde a Confidencial/Restringido o los riesgos a los que está expuesta es de criticidad alta, se deben implementar controles de cifrado durante los procesos de transmisión y almacenamiento de esta.

7.12 Continuidad del negocio

Todos los recursos de información y los procesos asociados al Core del negocio ya sean locales o en el ciberespacio, deben contar con un plan de continuidad del negocio y estar preparados para ataques a la Seguridad de la Información y Ciberseguridad, garantizando que la continuidad de la gestión de la Seguridad de la Información y Ciberseguridad se mantenga durante situaciones de contingencia

La información debe estar disponible para su uso autorizado cuando un colaborador la requiera en la ejecución de sus tareas regulares. Por lo tanto, se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de PISA, tanto localmente como en el ciberespacio, sin disminuir los niveles de seguridad establecidos. Esto debe ser independiente tanto del medio tecnológico que se utilice, como de la posibilidad de que la información se dañe, se destruya o no esté disponible por un lapso.

PISA establecerá medidas de reacción que permitan detectar y mitigar los efectos de ataques en Seguridad de la información y Ciberseguridad como son los denegados de servicio y el ingreso de código no autorizado. Estas medidas estarán documentadas en procedimientos y elementos que permitan mantener informado a los responsables de la seguridad de la información de la existencia de estas amenazas, detectar los ataques y ejecutar las acciones requeridas para mitigar dichos ataques.

7.13 Seguridad física

Todas las áreas físicas de la Compañía deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas. La información restringida o confidencial debe mantenerse en lugares seguros cuando no es utilizada. Todos los colaboradores deben cumplir con las directrices para la protección física de la información restringida o confidencial que usen.

Las áreas físicas construidas para soportar toda la operación de PISA deberán estar provistas de los controles adecuados (por ejemplo: puertas, cerraduras, lectores de tarjetas, biométricos, entre otros) según el valor de la información que contienen.

Los recursos informáticos de PISA deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de PISA.

La información clasificada como confidencial o restringida no se dejará desatendida o sin control. Por lo tanto, PISA desarrollará un programa que permita prevenir que la información crítica del negocio sea accedida sin autorización, dentro de lo cual está comprendido la implantación y cumplimiento de las directrices de Escritorio Limpio y Pantalla Limpia.

7.14 No repudio

La autenticidad de un negocio o transacción electrónica que realice la Compañía debe ser asegurada

Al realizar transacciones electrónicas se debe asegurar la autenticidad de cada parte que interviene y evitar que alguna de ellas niegue su participación (no repudio). Para ello se deben generar rastros que le permitan a PISA resolver conflictos cuando alguna de las partes niegue su participación. Estos se deben generar, guardar y ser accedidos acorde con las Políticas y Normas que regulen estos aspectos en PISA.

7.15 Administración de alertas

La Compañía debe ser alertada en el mismo instante en que existan violaciones a la política de Seguridad de la Información y Ciberseguridad

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas e informadas al Oficial de Seguridad de la Información de manera inmediata (alertas). Se deben desarrollar mecanismos para el reporte de eventos e incidentes que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información.

7.16 Auditabilidad de los eventos de Seguridad de la información y Ciberseguridad

Los registros de Seguridad de la Información y Ciberseguridad de la Compañía deben ser revisados permanentemente para asegurar el cumplimiento del Modelo de Seguridad de la Información y Ciberseguridad

El Oficial de Seguridad de la Información debe realizar monitoreo de los eventos críticos (por ejemplo: intentos de acceso fallidos al sistema de información, borrado o alteración de información, entre otros) y generar los respectivos registros de dicho evento.

Los registros de seguridad deben ser activados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera oportuna a los Responsables de la Información. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las pruebas.

7.17 Conectividad

Todas las conexiones a redes públicas deben ser autenticadas para prevenir que la información sea develada o alterada

Las conexiones a la red privada de PISA deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida al ciberespacio y a otras empresas deben realizarse sobre redes aprobadas por PISA. Esto aplica igualmente a cualquier conexión actual o futura en la red, que utilice medios públicos para integrar lugares que estén geográficamente dispersos.

Se requiere la aprobación del Oficial de Seguridad de la Información para poder acceder remotamente a la información de PISA y dichos accesos deben cumplir con la política de identificación y autenticación.

En virtud de lo anterior, se debe dar cumplimiento a la Instrucción Seguridad de la Información y Ciberseguridad - Medidas de Prevención Conexiones Remotas emitida por Grupo Aval, Instrucción que se adopta junto con la lista de controles mínimos a implementar.

7.18 Uso de los recursos informáticos de la Compañía (local y en el ciberespacio), de dispositivos móviles y de trabajo móvil

Los recursos informáticos son provistos a los colaboradores localmente y en el ciberespacio son para uso exclusivo de las actividades de la Compañía

Los recursos informáticos de PISA tanto locales como en el ciberespacio son exclusivamente para propósitos del negocio y deben tratarse como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Los colaboradores de PISA y terceros que intenten acceder a información para la que no tienen un requerimiento autorizado por PISA están violando la presente Política.

En el uso de la información de PISA, no se debe presumir privacidad, por lo que cuando ésta sea utilizada se podrán crear registros de la actividad realizada, que pueden ser revisados por PISA, de acuerdo con lo dispuesto en las Normas de Seguridad de la Información y Ciberseguridad, que deben ser conocidas y aceptadas por todos los colaboradores de PISA. En caso de requerirse, se ejecutarán los procedimientos de revisión correspondientes acorde con lo establecido en las NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DE PISA.

PISA se *reserva*[19] el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Personal seleccionado y autorizado por PISA podrá utilizar tecnología de uso restringido como la de monitoreo de red y de aplicaciones, datos operacionales, almacenamiento virtual, dispositivos extraíbles. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa autorización formal del Director de Sistemas, del jefe inmediato y del Oficial de Seguridad de la Información, según aplique.

Para acceder a la información de PISA a través de medios tales como los dispositivos o trabajo móviles, se deben implementar los controles necesarios para reducir los riesgos introducidos por estas prácticas.

7.19 Seguridad de información y ciberseguridad en los de administración de sistemas

Cada proceso de administración de sistemas de la Compañía debe cumplir con la presente política de Seguridad de la Información y Ciberseguridad

[19] **Reserva**: hace referencia a que la información sólo pueda ser utilizada para los propósitos con que fue obtenida del titular y única y exclusivamente para fines del negocio. Conlleva la obligación de no utilizar, revelar o distribuir la información adquirida para fines diferentes para los cuales fue obtenida del titular y única y exclusivamente para fines del negocio.

Actividades, normas y responsabilidades en seguridad de la información y ciberseguridad deben ser incluidas dentro de cada uno de los procesos de administración de sistemas de PISA, para lograr el cumplimiento de la presente Política y de las Normas de Seguridad de la Información y Ciberseguridad.

La Dirección de Sistemas debe crear y mantener una metodología que garantice una operación segura de los sistemas tecnológicos y su infraestructura.

Los requerimientos de seguridad de la información y ciberseguridad deben ser identificados previos al diseño y desarrollo de los sistemas de tecnología de la información y ciberseguridad. Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas, y si una modificación es requerida, ésta debe cumplir estrictamente con los requerimientos de desarrollo seguro y seguridad de la información y ciberseguridad que han sido previamente establecidos. El nivel de seguridad de la información de un sistema no puede verse disminuido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.

La implantación de un sistema nuevo o cambio significativo a los existentes debe ser revisada por medio de una evaluación de riesgos, que permita la detección de riesgos, la ubicación de controles apropiados que los mitiguen o eliminen y la operación segura.

La realización de un cambio tecnológico que no considere los requerimientos de seguridad de la información y ciberseguridad hace que PISA esté expuesta a riesgos. Por lo tanto, un cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad y sus respectivas Normas, y en caso de exponer a PISA a un riesgo en seguridad de la información y ciberseguridad, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo Responsable de la Información y presentado y aprobado por el Comité de Seguridad de la Información y Ciberseguridad.

En la gestión de incidentes de seguridad de la información, se registra, asigna, hace seguimiento y resuelve situaciones (problemas) que comprometen la disponibilidad de los servicios que provee la Dirección de Sistemas a PISA. Las fuentes de este proceso son los problemas derivados de situaciones que rompen o comprometen la Política de Seguridad de la Información y Ciberseguridad. Por lo tanto, todos los problemas de seguridad de la información de PISA deben ser canalizados hacia el Oficial de Seguridad de la Información, quien con base en un análisis posterior determinará si corresponden a violaciones, problemas vulnerabilidades en seguridad de la información, dando paso a los procedimientos establecidos para cada caso.

8 Seguridad en nuevas tecnologías y riesgos emergentes

Se debe implementar un plan de Seguridad de la Información y Ciberseguridad, con relación a las nuevas tecnologías, para monitorear, desarrollar e implementar estrategias de remediación de los *riesgos emergentes*[20], donde se debe:

- Adoptar procedimientos de clasificación de la información, gestión y administración de usuarios, definición de responsables y propietarios, de la información que se va a procesar en las nuevas tecnologías para determinar y aplicar los controles de Seguridad de la Información y Ciberseguridad.
- Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de terceros que surgen de la implementación de las nuevas tecnologías como lo son los riesgos operacionales, regulatorios, organizacionales y tecnológicos.
- Incluir en el plan de continuidad del negocio los requisitos y controles de seguridad para reanudar las operaciones orientadas en los sistemas automatizados.
- Supervisar el cumplimiento del trabajo que desempeñan los sistemas automatizados, asegurando que estos sistemas se adhieran a los requerimientos regulatorios y a las políticas de PISA, en materia de seguridad.

9 Modelo de evaluación del sistema de gestión de seguridad de la información y ciberseguridad

Para la identificación de riesgos y la aplicación de controles de Seguridad de la Información y Ciberseguridad, PISA debe adoptar y dar a conocer el modelo de evaluación de Seguridad de la Información y Ciberseguridad. Este modelo tiene como propósito evaluar el nivel de madurez del sistema de gestión de Seguridad de la Información e identificar las oportunidades de mejora que permitan fortalecerlo, basados en los dominios y controles propuestos en la norma NTC-ISO 27001:2013 y en el Framework de Ciberseguridad NIST.

[20] **Riesgos Emergentes**: entiéndase por aquellos riesgos nuevos o no identificados que nunca han sido considerados previamente por la entidad, o riesgos conocidos que están evolucionando de manera inesperada, que puedan afectar no solo a una compañía sino a todo un sector o toda la economía.

10 Reportes

Con el fin de facilitar el monitoreo de cumplimiento, se deben efectuar los reportes de gestión que sean solicitados, los cuales constituyan un efectivo apoyo para la administración; éstos deberán ser veraces, comprensibles, completos y oportunos.

Así mismo, se deberán informar a Grupo Aval aquellos *Incidentes*[21] Seguridad de la Información y Ciberseguridad que hayan afectado de manera significativa la confidencialidad, integridad, disponibilidad y privacidad de la información de PISA en el momento en que estos sucedan, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlos. Adicionalmente PISA deberá tener una base de datos consolidada de incidentes de Seguridad de la Información y Ciberseguridad clasificada en tipo de incidente, impacto y plan de remediación, así como, que este reporte se encuentre protegido dada la sensibilidad de esta información.

En virtud de lo anterior, se debe dar cumplimiento a las Instrucciones Seguridad de la Información y Ciberseguridad - Reportes Medio Impacto y Actualización Reporte Incidentes Ciberseguridad, Instrucciones emitidas por Grupo Aval, las cuales se adoptan junto con los documentos anexos a dichas Instrucciones.

11 Capacitación y entrenamiento

Dentro del proceso de inducción de un colaborador nuevo y al menos anualmente para la totalidad de los colaboradores debe realizarse una capacitación y/o actualización sobre Seguridad de la Información y Ciberseguridad. La capacitación y entrenamiento se puede brindar en forma continua, virtual o presencial a los colaboradores de PISA, con el propósito de fortalecer los conceptos y asegurar la continuidad y sostenibilidad de Sistema de Gestión de Seguridad de la Información.

12 Sistema y responsables de la gestión de la política

Para dar cumplimiento a los objetivos de la política de Seguridad de la Información y Ciberseguridad, se han definido los siguientes actores clave en la Gestión de Seguridad de la Información:

12.1 Junta Directiva

Las responsabilidades de la Junta Directiva serán:

- Aprobar la política Seguridad de la Información y Ciberseguridad.
- Estudiar y aprobar el Apetito de Riesgo de PISA.
- Velar porque se cuente con los recursos técnicos y humanos suficientes para gestionar adecuadamente la Seguridad de la Información y Ciberseguridad.
- Exigir el cumplimiento de las normas y regulaciones gubernamentales de Seguridad de la Información y Ciberseguridad.
- Participar en programas de concientización y capacitación en temas de Seguridad de la Información y Ciberseguridad.
- Supervisar la Seguridad de la Información y Ciberseguridad de PISA, comprendiendo los riesgos y asegurando que estos sean gestionados.

12.2 Alta Dirección

Las responsabilidades de la *Alta Dirección*[22] serán:

- Evaluar el seguimiento del nivel de madurez y monitoreo de las políticas propuestas del Sistema de gestión de Seguridad de la Información.
- Evaluar los informes que le presente el Oficial de Seguridad de la Información sobre los resultados de la evaluación de efectividad del programa de Seguridad de la Información y Ciberseguridad, propuestas de mejora en materias de Ciberseguridad y resumen de los incidentes que afectaron a PISA.

[21] **Incidentes**: un Incidente de Ciberseguridad es la ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio. Un Incidente de Seguridad de la Información es un evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de amenazar la seguridad de la información.
[22] **Alta Dirección**: son las personas responsables de dirigir, ejecutar y supervisar las operaciones de la entidad bajo la dirección de la Junta Directiva.

- Promover la aplicación y apropiación de *buenas prácticas de Seguridad de la Información*[23] y Ciberseguridad.
- Garantizar, sin excepción, la evaluación de Seguridad de la Información y Ciberseguridad de todos los activos de información.
- Fortalecer la cultura de Seguridad de la Información de los colaboradores y terceros que administren activos de información. Se debe evaluar la necesidad de sensibilizar en temas de seguridad de la información a terceros críticos que acceden a los activos de información de PISA.
- Supervisar la Seguridad de la Información y Ciberseguridad de PISA, comprendiendo los riesgos y asegurando que estos sean gestionados.

12.3 Comité de Seguridad de la Información y Ciberseguridad

Las responsabilidades del Comité de Seguridad de la Información y Ciberseguridad serán:

- Revisar y aprobar la Política de Seguridad de la Información y Ciberseguridad, previa a la presentación a la Junta Directiva de PISA.
- Monitorear cambios significativos que afectan a las políticas y normas de seguridad de la información de PISA.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la Seguridad de la Información que se produzcan en el ámbito de PISA.
- Revisar el estado general de la Seguridad de la Información cada que se requiera.
- Revisar y aprobar proyectos de Seguridad de la Información.
- Realizar otras actividades de alto nivel relacionadas con la Seguridad de la Información.
- Promover la difusión y apoyo a la Seguridad de la Información dentro de PISA.
- Conocer los Incidentes de Seguridad de la Información presentados en PISA y los planes de acción llevados a cabo para la mitigación de estos.

12.4 Oficial de Seguridad de la Información

Las responsabilidades del Oficial de Seguridad de la Información serán:

- Presentar a la Alta Dirección el informe de Gestión sobre los resultados de la evaluación de efectividad del programa de Seguridad de la Información y Ciberseguridad.
- Participar en el Comité de Seguridad de la Información de PISA.
- Adoptar y socializar las mejores prácticas sugeridas en el Comité y los lineamientos corporativos.
- Propiciar la actualización del inventario de riesgos de Seguridad de la Información y Ciberseguridad.
- Apoyar a la primera línea en el proceso de identificación de riesgos y controles, la determinación de su criticidad y verificación del cumplimiento de los planes de acción establecidos en la gestión de incidentes de Seguridad de la Información y Ciberseguridad.
- Conocer los Incidentes de Seguridad de la Información y las medidas que se han implementado para mitigarlos.
- Monitorear el resultado de evaluación de Riesgos.
- Definir y monitorear indicadores clave de desempeño sobre la gestión de Seguridad de Información y Ciberseguridad.

12.5 Dirección de Sistemas

Las responsabilidades de la Dirección de Sistemas serán:

- Apoyar al Oficial de Seguridad de Información en la preparación del informe de Gestión.

[23] **Buenas Prácticas de Seguridad de la Información**: conjunto de medidas implementadas para asegurar que la información de la entidad y aquella que se encuentre en su poder sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (confidencialidad), que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (integridad), que esté disponible cuando sea requerida (disponibilidad) y que sólo sea utilizada para los propósitos con que fue obtenida (privacidad y reserva) y única y exclusivamente para fines del negocio.

- Participar en el Comité de Seguridad de la Información y Ciberseguridad de PISA.
- Adoptar y socializar las mejores prácticas sugeridas en el Comité.
- Informar al Oficial de Seguridad de Información sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de Ciberseguridad.
- Adoptar los lineamientos establecidos.
- Apoyar a la segunda línea en el proceso de identificación de riesgos y controles, así como en su evaluación.
- Implementar y operar las herramientas de Seguridad TI y Ciberseguridad.
- Analizar los Incidentes de alto impacto de Seguridad de la Información y Ciberseguridad reportados e implementar los planes de remediación.
- Velar porque se adopten medidas para responder a los incidentes presentados y para prevenir futuros incidentes.
- Adoptar las mejores prácticas vigentes en el mercado con respecto a respuestas a incidentes.
- Definir y monitorear indicadores clave de desempeño sobre la gestión de Seguridad TI y Ciberseguridad.

12.6 Responsables de la Información

Los Responsables de la Información deberán:

- Identificar, clasificar y proteger la información bajo su responsabilidad, conocer los riesgos a los que podría estar expuesta y velar porque se provean los mecanismos necesarios para que estos riesgos se mitiguen a niveles aceptables, considerando costo-beneficio para su área de negocio y para PISA.
- Conocer los riesgos de Seguridad de Información que le son aplicables.
- Con el apoyo de la segunda línea, identificar los controles clave para mitigar los riesgos identificados.
- Llevar a cabo la ejecución de los controles para mitigar los riesgos (Autocontrol).
- Definir y ejecutar los planes de acción para mitigar los riesgos de seguridad de la información a su cargo.
- Reportar a la Dirección de Sistemas y al área de GRC, cualquier incidente de seguridad de información y de manera particular cualquier evento material de Ciberseguridad.
- Vigilar y velar que su equipo de trabajo dé cumplimiento a la política de seguridad y Ciberseguridad.

12.7 Auditoría Interna

Las responsabilidades de la Auditoría Interna serán:

- Adelantar las pruebas de auditoría que considere apropiadas de acuerdo con el plan de trabajo anual aprobado por el Comité de Auditoría.
- Evaluar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.

12.8 Colaboradores

Todos los colaboradores de PISA deben ser responsables por la confidencialidad y preservación de la información que se requiera manejar con el objetivo de llevar a cabo sus funciones independientes del tipo de contratación.

12.9 Gobierno para la gestión de seguridad de la información y ciberseguridad

Las funciones y responsabilidades frente al Riesgo de Seguridad de la Información y Ciberseguridad y frente a la gestión en esta materia, deben de estar de acuerdo con la Política para la Gestión Integral de Riesgos que maneje PISA. Este marco de referencia define el esquema de las tres líneas, considerando (i) la gestión por la línea de negocio, (ii) una función de gestión de riesgo de Seguridad de la Información independiente, y (iii) una revisión independiente.

12.9.1 Primera línea

La primera línea la constituyen el área de sistemas y todos los colaboradores de PISA. La política de Seguridad de la Información y Ciberseguridad reconoce al área de sistemas y demás colaboradores como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de Seguridad de la Información y Ciberseguridad inherentes a las actividades, procesos y sistemas de seguridad. Quienes conforman esta línea deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas.

Así mismo deben cumplir con políticas y procedimientos definidos por PISA, contribuyendo a una sólida cultura en Seguridad de la Información y Ciberseguridad.

12.9.2 Segunda línea

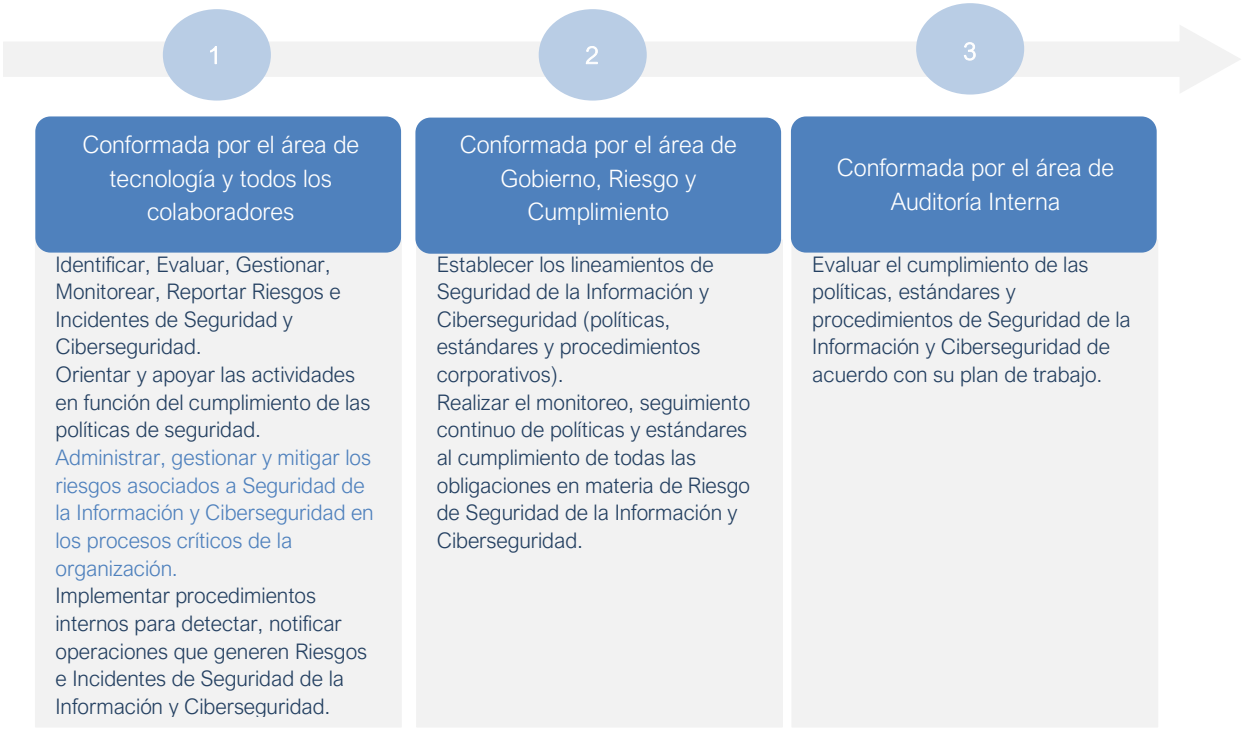
Esta línea está conformada por el área de GRC, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de Riesgo en Seguridad de la Información y Ciberseguridad.

El Oficial de Seguridad de la Información y Ciberseguridad es responsable de presentar los resultados de gestión directamente a la Alta Dirección. Debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Seguridad de la Información. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos de Seguridad de la Información derivados del negocio, incluyendo temas específicos de Ciberseguridad.

12.9.3 Tercera línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la Seguridad de la Información y Ciberseguridad, así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

En resumen, las responsabilidades de cada una de las tres líneas serían las siguientes:



13 Investigaciones y sanciones

PISA reconoce que en el evento de incumplimiento de esta Política y demás actividades que se deriven de ella, los terceros y los colaboradores responsables por su incumplimiento podrán ser objeto de acciones disciplinarias por parte de PISA de acuerdo con las políticas internas de PISA relacionadas con el manejo de Incidentes de Seguridad de la Información. Lo anterior, sin perjuicio de la eventual responsabilidad que pudiera derivarse por el incumplimiento de la normatividad aplicable a Seguridad de la Información.

14 Documentos de referencias

CÓDIGO	NOMBRE DEL DOCUMENTO
SI-DG-02	Normas de Seguridad de la Información y Ciberseguridad.
SI-DG-03	Organización de Seguridad de la Información y Ciberseguridad.
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Modelo Cláusula Certificación de Proveedor Crítico
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Actualización Metodología Gestión de Riesgos
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Inventario de Riesgos Genéricos
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Línea base de controles
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Actualización Cláusula Ciberseguridad
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Conexiones Remotas
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Reportes de Medio Impacto
N/A	Instrucción Seguridad de la Información y Ciberseguridad - Actualización Reporte Incidentes Ciberseguridad

15 Control de cambios

Fecha	Versión	Descripción del Cambio
31 de enero de 2019	09	• Inclusión de la política COMPROMISO DE LA DIRECCIÓN • Eliminación de normas para cada directriz de la Política de Seguridad de la Información. • Separación en diferentes documentos entre las políticas y normas. Para efectos de mayor claridad, ajuste de redacción en las directrices de la Política de Seguridad de la Información.
Acta N° 352 25 de agosto 2020	10	• Se actualiza la Política incluyendo lo relacionado con los temas de Ciberseguridad. • Se adiciona que la información para tener en cuenta como activo de información no solo será la almacenada en la infraestructura local, sino que también se debe proteger la que se almacene en el ciberespacio y sea propiedad de PISA. • Se adiciona para los servicios prestados por un tercero y este almacene la información en el ciberespacio, el tercero debe regirse bajo los términos definidos en el contrato para la prestación del servicio. • Se modifica el nombre del Comité de Seguridad de la Información de PISA a Comité de Seguridad de la Información y Ciberseguridad. • Se incluye como nuevas definiciones Ciberseguridad, Ciberespacio. • Se actualiza el documento de acuerdo con la estructura establecida por el Sistema de Gestión Integral de Calidad.
Acta N° 365 28 de septiembre de 2021	11	• Se alinea la Política de acuerdo con la **Instrucción Seguridad de la Información y Ciberseguridad N°23 - Actualización Política Corporativa Seguridad de la Información y Ciberseguridad,** emitida por Grupo Aval. • Se adicionan Objetivo General y Objetivos Específicos. • Se incluye las Responsabilidades de los diferentes actores frente a la política. • Se adicionan los siguientes capítulos: o Marcos de Referencia o Política de Seguridad de la Información y Ciberseguridad entorno al riesgo o Gobierno para la gestión de Seguridad de la Información y Ciberseguridad o Seguridad en nuevas tecnologías y riesgos emergentes o Modelo de evaluación del sistema de gestión de Seguridad de la Información y Ciberseguridad o Reportes o Capacitación y entrenamiento 22/08/2022 Se realiza el siguiente cambio menor: • Se cambia el tipo de sociedad de las empresas PROYECTOS DE INFRAESTRUCTURA S.A., ahora PROYECTOS DE INFRAESTRUCTURA S.A.S, debido a que se transformó en una sociedad por acciones simplificadas. • Se reemplaza el término “la Compañía” por “PISA”.
Acta N° 389 19 de septiembre de 2023	12	• Se alinea la Política de acuerdo con la Instrucción Seguridad de la Información y Ciberseguridad N°29 - Actualización Política Corporativa Seguridad de la Información y Ciberseguridad, emitida por Grupo Aval. • Se modifica el ámbito de aplicación de la política para alinearlo a la Política Corporativa de Grupo Aval. • Se incluye referencia a las Instrucciones Corporativas de Grupo Aval, las cuales se adoptan o adaptan para su aplicación al interior de PISA. • Se incluye tabla con las responsabilidades de las tres líneas (antes tres líneas de defensa). • Se incluyen nuevas definiciones y se efectúan cambios menores de redacción.