

NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Código: SI-DG-02

Versión: 11



CONTENIDO

1.	OBJETIVO	3
2.	ALCANCE	3
3.	CUMPLIMIENTO	3
4.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	4
4.1.	Seguridad de la Información y Ciberseguridad	4
4.2.	<i>Propiedad intelectual</i>	4
4.3.	Responsables de <i>activos de información</i>	5
4.4.	Cumplimiento de regulaciones	5
4.5.	Administración del riesgo en Seguridad de la Información y Ciberseguridad	6
4.6.	Capacitación y creación de cultura en Seguridad de la Información y de Ciberseguridad	7
4.7.	Seguridad del personal	7
4.8.	Terceros que acceden información de PISA local o remotamente	8
4.9.	Identificación y autenticación individual en la infraestructura local y en el ciberespacio	9
4.10.	Control y administración del acceso de usuarios a la información	12
4.11.	Clasificación de la información	14
4.12.	Continuidad del negocio	15
4.13.	Seguridad física	17
4.14.	No repudio.....	18
4.15.	Administración de alertas.....	18
4.16.	Auditabilidad de los eventos de Seguridad de la Información	19
4.17.	Conectividad.....	20
4.18.	Uso de los recursos informáticos de PISA, de dispositivos móviles y de trabajo móvil	21
4.19.	Seguridad de Información y Ciberseguridad en los procesos de administración de sistemas	23
5.	DOCUMENTO DE APROBACIÓN	25
6.	DOCUMENTOS RELACIONADOS	25
7.	RELACIÓN DE FORMATOS Y/O REGISTROS	25
8.	CONTROL DE CAMBIOS	26

ESTE DOCUMENTO ES PROPIEDAD DE PISA. LAS PERSONAS QUE TENGAN ACCESO A ÉL SON RESPONSABLES DE SU CUSTODIA Y CONSERVACIÓN. NO PODRÁ SER REPRODUCIDO TOTAL NI PARCIALMENTE, NI ENTREGADO A TERCEROS, SIN LA AUTORIZACIÓN DEL RESPONSABLE DE PROCESOS. CUALQUIER COPIA IMPRESA DE ESTE DOCUMENTO SE CONSIDERA COPIA NO CONTROLADA.

* * *

Este documento fue aprobado por la Junta Directiva el 18 de febrero de 2025, por medio del acta N° 410 y fue emitido el 25 de marzo de 2025.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

La Junta Directiva de Proyectos de Infraestructura S.A.S. (PISA) tiene la competencia de diseñar, evaluar y revisar de manera permanente las directrices, así como aprobar y actualizar los lineamientos corporativos que establecen las pautas que rigen la actuación de PISA.

En ejercicio de estas responsabilidades, y consciente de que la creación de valor sostenible se fundamenta en nuestro propósito superior de interconectar a las comunidades y regiones para el progreso y bienestar del país y en los valores de PISA, la Junta Directiva aprueba esta Norma de Seguridad de la información y Ciberseguridad.

1. OBJETIVO

Desarrollar la Política de Seguridad de la Información y *Ciberseguridad*¹, documentando formalmente las normas para la protección de la información de Proyectos de Infraestructura S.A.S (en adelante PISA), la cual es procesada, transportada o almacenada por medios informáticos como software, hardware, redes o cualquier otro medio o formato en que se encuentre.

2. ALCANCE²

Las Normas de Seguridad de la Información y Ciberseguridad responden y desarrollan las directrices establecidas por la Política de Seguridad de la Información y Ciberseguridad y son requeridas para implantar un *Modelo de Seguridad de la Información y Ciberseguridad*³ confiable y flexible.

Estas normas hacen parte del Modelo de Seguridad de la Información y Ciberseguridad y aplican para todos los niveles jerárquicos de PISA. Usuarios (que incluye colaboradores y accionistas), Clientes, Terceros con los cuales se intercambia información (incluye proveedores y contratistas), Entes de Control y demás Entidades Relacionadas, que acceden, ya sea interna o externamente, a cualquier activo de información, independiente que éste se encuentre de manera física o almacenada en medios informáticos locales como los implementados en el *ciberespacio*⁴.

Para la adecuada interpretación y aplicación de las normas de seguridad de la información que se desarrollen en el presente documento, se debe tener como parámetro lo estipulado en el documento POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD y aplicará al presente documento las definiciones contenidas en el mismo, las que se reproducen en este documento sin perjuicio que al mismo se adicione los términos que sean producto del presente documento.

3. CUMPLIMIENTO

Las normas definidas en este documento deben ser cumplidas por todos los usuarios que tengan acceso o hagan uso de la información de PISA a través de software, hardware, redes o cualquier otro medio ya sea que se encuentre localmente y/o ciberespacio; independiente del formato en que ésta se encuentre.

El cumplimiento de las normas es de carácter obligatorio y cualquier excepción debe ser documentada como un *riesgo*⁵ en el que incurre PISA y debe ser formalmente aceptado por el *Responsable de la Información*⁶. Todos los niveles jerárquicos de PISA deben entender las implicaciones de las normas y las responsabilidades en su estricto cumplimiento.

¹ Ciberseguridad: Es el conjunto de políticas, conceptos de seguridad, recursos, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para prevenir el acceso, obstaculización, interceptación, daño, violación de datos, uso de software malicioso, hurto de medios y la transferencia no consentida de activos informáticos y los activos de PISA en el ciberespacio.



² Alcance: De acuerdo con lo establecido en el otrosí No. 5 del contrato de prestación de servicios suscrito entre PISA y CCFC, y a las instrucciones dadas por las Juntas Directivas de cada compañía, el presente documento es aplicable a Concesiones CCFC S.A.S. en lo que le aplique o le llegare a aplicar de conformidad con la estructura y naturaleza de los procesos y/o actividades desarrolladas por CCFC.

³ Modelo de Seguridad de la Información y Ciberseguridad: Se refiere al conjunto de políticas, procedimientos, estándares, normas de seguridad, elementos de seguridad y topologías que garantizan la protección de la información del negocio.

⁴ Ciberespacio: Corresponde a un ambiente complejo resultante de la interacción de personas, software y servicios en Internet, soportado en dispositivos tecnológicos y redes conectadas a la red mundial, propiedad de múltiples dueños con diferentes requisitos operativos y regulatorios.

⁵ Riesgo: La probabilidad de que ocurra un evento en seguridad de la información, que cause pérdida a PISA.

⁶ Responsable de la información: Cada área y/o proceso donde ejerce 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 Presidencia o a quienes éstos deleguen.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

El incumplimiento de las normas aquí establecidas puede resultar en acciones disciplinarias para los colaboradores de PISA. En el caso de proveedores, contratistas o terceros podría llegar incluso a la terminación de la relación contractual y/o acciones judiciales. **El desconocimiento de las Políticas y normas no exime su aplicación.**

Para los nuevos desarrollos o nuevas adquisiciones de Recursos informáticos ya sean locales o en el ciberespacio, las normas rigen a partir del período de vigencia de estas.

4. NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

4.1. Seguridad de la Información y Ciberseguridad

a. Protección Homogénea de la información

La información de PISA ya sea se encuentre localmente y/o en el ciberespacio debe tener un nivel de protección definido de acuerdo con su clasificación y ésta debe mantenerse dentro del nivel de protección sin importar el medio o formato en que ésta se encuentre. Ver el numeral 4.1.11 en donde se amplía las normas relacionadas con "Clasificación de la Información".

b. Asignación de responsabilidades en seguridad de la información y ciberseguridad

Todos los colaboradores de PISA deben tener asignado un rol en el Modelo de Seguridad de la Información y Ciberseguridad de acuerdo con las funciones y responsabilidades que desempeñan en PISA y estas deben ser comunicadas a aquellos que las desarrollen. Las responsabilidades de los roles del Modelo de Seguridad de la Información se encuentran consignadas en el documento ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

c. Desarrollo de tareas de Administración de la Seguridad y Ciberseguridad

Se deben establecer procedimientos para el desarrollo de las actividades de administración de la seguridad que obedezcan a estándares de proceso y no al desarrollo de actividades informales.

d. Propiedad de la Administración de Seguridad de la Información y Ciberseguridad

La administración de la seguridad de la información y ciberseguridad es responsabilidad de PISA y no debe ser ejecutada por personal ajeno a la misma o terceras personas, sin las definiciones y directrices de seguridad de la información y ciberseguridad, las cuales deben estar alineadas al cumplimiento de todos los elementos del Modelo de Seguridad de la Información de PISA y Ciberseguridad.

e. Administración de Seguridad de la Información y Ciberseguridad

PISA debe propender porque las funciones relacionadas con la administración de los recursos informáticos tanto locales como en el ciberespacio, la administración de datos y de seguridad y/o ciberseguridad estén segregadas.

f. Seguridad de la Información y/o en Ciberespacio en Gestión de Proyectos



En todos los proyectos de PISA se debe incluir un componente de seguridad de la información y ciberseguridad, donde se identifiquen los requerimientos de confidencialidad, integridad, disponibilidad, privacidad y auditabilidad.

4.2. Propiedad intelectual⁷

a. Asignación de derechos de propiedad intelectual a PISA

Los descubrimientos o invenciones y las mejoras en los procedimientos, lo mismo que todos los trabajos y consiguientes resultados de las actividades de los colaboradores en PISA o cuando por la naturaleza de sus funciones haya tenido acceso a secretos o investigaciones confidenciales, quedarán de propiedad exclusiva de PISA.

⁷ Propiedad intelectual: Reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

Además, este último tendrá derecho a hacer patentar a su nombre o a nombre de terceros esos inventos o mejoras, para lo cual el colaborador accederá a facilitar el conocimiento oportuno de las correspondientes formalidades y a dar su firma y extender los poderes y documentos necesarios para tal fin, según y cuando se lo solicite PISA, sin que ésta quede obligada al pago de compensación alguna. Todo ello de conformidad con lo establecido en el contrato de trabajo.

b. Avisos de Propiedad intelectual

Se deben incluir avisos de derechos de propiedad intelectual en todo el software que se encuentre localmente como en el ciberespacio y que sea de propiedad de PISA y en su correspondiente documentación a excepción del software libre que maneje PISA. Estos avisos deben ser incorporados, aunque no se requiera que sea explícito, para que los derechos de propiedad intelectual sean exigibles. La existencia de un aviso tiene un efecto disuasivo.

c. Publicación de Información de PISA en medios masivos

Para que exista un manejo transparente y responsable de las comunicaciones, que evite cualquier tipo de confusión frente al público en general, se debe tener en cuenta que: a) La opinión de PISA será expresada a terceros y medios masivos exclusivamente por su Representante Legal o aquellas personas que éste de manera explícita autorice para ello.

En todo caso, en ninguna circunstancia se podrá utilizar el nombre de PISA para emitir declaraciones sobre temas distintos a los propios del objeto social de la empresa o relacionados con el mismo.

d. Transferencia de software con partes externas

La transferencia de software de propiedad o adquirido por PISA debe cumplir con la normatividad de protección de Derechos de Autor⁸ a los que haya lugar.

e. Almacenamiento de información audiovisual

No está permitida la descarga, uso, intercambio y/o instalación de archivos de audio y video en equipos y servidores de PISA ya sea que se encuentren de manera local o en el ciberespacio que no estén relacionados directamente a las actividades de PISA y/o incumpla con la propiedad intelectual de sus autores.

4.3. Responsables de activos de información⁹

a. Asignación de Responsables de la Información

Cada área y/o proceso actúa como Responsable de la Información (física y digital), ejerciendo así la facultad de aprobar o revocar el acceso a la información a su cargo ya sea que se encuentre de forma local o en el ciberespacio. Se debe divulgar a toda PISA quienes actúan como Responsables de la Información.

b. Actividades que deben desarrollar los Responsables de la Información

Los responsables de la Información deben contar con un inventario de estos para las áreas o procesos que lideran ya sea que se encuentren de forma local, garantizando su continua actualización, validez de los usuarios y accesos autorizados de la información a su cargo.



4.4. Cumplimiento de regulaciones

a. Cumplimiento de normas legales y disposiciones externas

Toda reglamentación, regulación o requerimiento contractual para cada recurso de información y ciberseguridad que se encuentre de forma local o en el ciberespacio debe estar definida explícitamente y documentada formalmente. Deben existir documentos que

⁸ Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

⁹ Activos de Información: Son todos los recursos que utiliza un sistema de gestión de seguridad de la información para que PISA funcione, soporta uno o más procesos CORE de PISA y, en consecuencia, debe ser protegida. Estos recursos pueden ser: información física y digital, software, hardware, servicios de información, servicios de comunicaciones, servicios de almacenamiento, reputación e Imagen.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

establezcan la forma en que los recursos informáticos de PISA cumplen con toda reglamentación, regulación o requerimiento contractual interno o externo.

b. Cumplimiento de los Derechos de Autor

La instalación de software en los recursos informáticos debe ser previamente autorizada por la Dirección de Sistemas y debe cumplir con los requerimientos legales que facultan su utilización. Deben implantarse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

c. Calidad de la información

El procesamiento, almacenamiento y suministro de la información de PISA ya sea que se encuentre de forma local o en el ciberespacio debe estar adecuadamente soportado (técnica y procedimentalmente) de modo que permita conservar criterios de calidad, de tal forma que la información sea la apropiada para la toma de decisiones y el cumplimiento de sus obligaciones (confiabilidad), generada haciendo el mejor uso de los recursos (eficiencia), y su suministro en forma oportuna, correcta y consistente (efectividad).

d. Instalación de Software Autorizado

El software que reside en los recursos informáticos de PISA o en el ciberespacio sólo podrá ser el autorizado por la Dirección de Sistemas. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos en el contrato para la prestación del servicio.

e. Cifrado¹⁰ de información restringida¹¹ enviada a correos externos

Toda información considerada restringida que deba ser enviada a través de correo electrónico para destinatarios externos deberá ir cifrada.

f. Custodia de Medios magnéticos, Manuales y Licencias de Uso

La Dirección de Sistemas debe conservar en un lugar seguro y específico para este fin, los originales de los medios, manuales y licencias de uso de los recursos informáticos adquiridos.

g. Ley de Protección de Datos Personales

Los Responsables de Información que procesan datos personales de colaboradores y/o usuarios deben obtener la debida autorización para su tratamiento (recolección, transmisión, almacenamiento, uso circulación, supresión o actualización), de acuerdo con las actividades ejecutadas en PISA. De igual manera, los Responsables de la Información deberán asegurar que solo personal autorizado pueda tener acceso a dichos datos.

4.5. Administración del riesgo en Seguridad de la Información y Ciberseguridad

a. Análisis de riesgo

Debe realizarse anualmente un análisis de riesgos que permita identificar los recursos de informáticos de mayor criticidad y orientar los esfuerzos para proteger dichos recursos.

b. Seguros con cobertura para los Recursos Informáticos

Se deben contratar seguros que cubran los recursos informáticos. (hardware, medios de almacenamiento (Datos), Software y documentación) que cubran dichos recursos ante la posible materialización de un riesgo externo o interno, de acuerdo con el impacto en la continuidad de las operaciones de PISA.

¹⁰ Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

¹¹ Información Restringida: Información crítica al interior de la organización y es para uso exclusivo de un grupo específico de funcionarios, Área o División. Dicha información puede ser conocida únicamente por los colaboradores de PISA relacionados con las tareas asignadas y terceros relacionados estrictamente según la operación del negocio y que al ser revelada a personas no autorizadas puede poner en riesgo la continuidad de la operación del negocio y/o puede tener un fuerte impacto en los estados financieros, en los asuntos legales y/o en la imagen de PISA.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

c. **Para la Gestión de la Seguridad de la Información y la Ciberseguridad la entidad debe considerar las siguientes etapas:**

Prevención: Desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la gestión de la ciberseguridad. La función de prevención admite la capacidad de limitar o contener el impacto de un posible *incidente*¹² de ciberseguridad. En tal sentido, en la entidad se debe propender por la identificación y medición de los riesgos cibernéticos emergentes que puedan llegar a afectar a la entidad y establecer controles para su mitigación.

Protección y detección: Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos.

Respuesta y comunicación: Aún con las medidas de seguridad adoptadas, la entidad debe desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad.

Recuperación y aprendizaje: Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad

4.6. Capacitación y creación de cultura en Seguridad de la Información y de Ciberseguridad

a. Programa de Concientización

El Oficial de Seguridad de la Información debe desarrollar un programa de concientización que enfatice la importancia del cumplimiento del Modelo de Seguridad de la Información y Ciberseguridad y su contribución al logro de los objetivos del negocio. Este programa debe ser realizado desde el mismo momento del ingreso de un colaborador o cuando se inician relaciones con terceros con los cuales se intercambie información.

b. Difusión De La Organización de Seguridad de la Información y Ciberseguridad

Se debe difundir periódicamente, a través del Programa de Concientización, la estructura de la Organización de Seguridad de la Información, sus objetivos y las responsabilidades de sus miembros.

c. Divulgación del Modelo de Seguridad de la Información y Ciberseguridad y sus modificaciones

El Oficial de Seguridad de la Información debe implementar el plan de divulgación del Modelo de Seguridad y Ciberseguridad y de sus respectivas modificaciones cuando se presenten.

d. Certificación de los usuarios en Seguridad de la Información

PISA debe realizar procesos mediante los cuales todos los usuarios de los Recursos informáticos se certifiquen periódicamente según el programa de concientización de seguridad y ciberseguridad.

e. Medición de la efectividad del programa de Concientización y Certificación



Se deben realizar evaluaciones periódicas de los resultados del programa de concientización y certificación a fin de establecer su efectividad y obtener información que permita establecer ajustes y correctivos en su diseño y ejecución.

4.7. Seguridad del personal

a. Cumplimiento del Modelo de Seguridad de PISA

Es obligación de todos los niveles jerárquicos, sin excepción alguna, conocer, respetar, cumplir y hacer cumplir el Modelo de Seguridad de la Información de PISA. El compromiso se encuentra en el documento COMPROMISO DE CONFIDENCIALIDAD DE USUARIO DE APLICATIVOS, HERRAMIENTAS O INFORMACIÓN DE LA COMPAÑÍA.

¹² Incidente: Evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, la consecuencia, el número de veces ocurrido o el origen (interno o externo).

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

b. Manejo Confidencial de la Información con los empleados

Todos los colaboradores, sin importar el tipo de contrato de trabajo, ya sea a término fijo o indefinido, deben acatar lo concerniente al manejo confidencial de la información de PISA. Lo anterior, según lo establecido tanto en el contrato laboral como en el Código de Conducta, lo cual será de obligatorio cumplimiento y el no aplicarlo tendrá implicaciones disciplinarias. Dependiendo de la gravedad, PISA emprenderá las acciones legales que estime convenientes.

c. Definición de roles de Seguridad y Ciberseguridad

Debe existir una descripción de las actividades para cada rol dentro de la Organización de Seguridad de la Información de PISA y ésta debe ser comunicada a los colaboradores que las desarrollen. En PISA las responsabilidades de los roles del Modelo de Seguridad de la Información se definen en el documento ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

d. Actualización de conocimientos en Seguridad de la Información

El personal que forma parte de la ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD debe estar permanentemente informado y actualizado sobre los avances relativos a la seguridad de la información y Ciberseguridad y las nuevas *vulnerabilidades*¹³.

e. Confidencialidad de la información personal (Datos personales)

Todos los empleados a término indefinido y fijo deben tratar como restringida la información personal de los demás empleados. La confidencialidad de la información personal sea que se encuentre de forma local o en el ciberespacio de cualquier empleado debe respetarse y el no cumplimiento deberá tratarse de acuerdo con el tipo de sanción administrativa definida en PISA.

f. Participación de PISA en redes sociales

El acceso, uso y participación de los colaboradores, proveedores y contratistas de PISA, en las redes sociales debe realizarse aplicando principios de legalidad, ética y moral, garantizando el cumplimiento de los valores corporativos y de las distintas obligaciones laborales, contractuales y/o cláusulas de confidencialidad suscritas con PISA.

g. Confidencialidad de la información en la desvinculación de colaboradores

Todos los colaboradores a término indefinido y fijo deben guardar la confidencialidad de la información de PISA después de su desvinculación. Los empleados a término indefinido y fijo deben comprometerse a no revelar a terceros por ningún medio escrito, digital, tecnológico o verbal.

4.8. Terceros que acceden información de PISA local o remotamente

a. Acuerdos de Niveles de Servicio¹⁴ para la Información con entes externos

Se deben establecer Acuerdos de Niveles de Servicios con respecto a la seguridad de la información y ciberseguridad que rijan los compromisos entre PISA y entes externos.

b. Inclusión de cláusulas de seguridad de la información y ciberseguridad en contratos con entes externos



La Gerencia Jurídica debe incluir cláusulas de seguridad de información en los contratos firmados con entes externos relacionados con los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información ya sea que este se encuentre de forma local o en el ciberespacio.

Los acuerdos o cláusulas de confidencialidad podrán incluir alguno de estos puntos (según aplique):

- La obligación de proteger la privacidad de la información verbal, escrita, o en cualquier otro medio que se encuentre, restringiendo su uso exclusivamente al personal que tenga absoluta necesidad de conocerla y para los efectos que se determinen en el contrato. De igual forma, se deberá garantizar que las personas que tengan acceso a la información

¹³ Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

¹⁴ Acuerdos de Niveles de Servicios: Pactos realizados entre áreas o con terceros con el fin de establecer aspectos a tener en cuenta para el intercambio de información; tales como: medios de transmisión, periodicidad, canalizador y como es este caso, las seguridades implementadas (certificación digital, cifrado, reserva, etc.).

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

conozcan su carácter confidencial y de reserva; y que la información será utilizada única y exclusivamente para los fines estipulados en el contrato.

- De acuerdo con el objeto del contrato, se deben definir los niveles de servicio en cuanto a seguridad de la información, que debe cumplir el tercero.
- La titularidad de la información que sea entregada, procesada o resultante de la ejecución del contrato, pertenece a PISA.
- Restricciones sobre el software empleado durante la ejecución del contrato, garantizando que dicho software cumple con los requisitos de Derechos de Autor.
- Restricciones sobre el software desarrollado que indiquen los controles a implementar con el fin de prevenir el uso de código malicioso¹⁵.
- Cláusulas contractuales que especifican la propiedad de la información que se transmite por redes públicas.

c. Control de Acceso a Terceros

El acceso de entes externos a los Activos de Información de PISA ya sea que se encuentre de forma local o en el ciberespacio debe ser otorgado de acuerdo con las políticas establecidas para acceso a la información y debe contemplar las siguientes condiciones:

- Estar fundamentado en los requerimientos específicos del Responsable de la Información.
- Haber observado y cumplido los requisitos internos y legales previos a la realización de cualquier autorización de acceso al tercero.
- Tener asignados identificadores únicos y claramente reconocibles para el acceso a los recursos informáticos.
- Los perfiles son asignados siguiendo un proceso específico de autorización de acceso a los recursos requeridos y están sustentados en una necesidad legítima del negocio.
- Disponer de una lista de individuos autorizados para la utilización de los servicios con los respectivos privilegios y derechos con respecto a cada uso.
- Se ha establecido el acceso a información estrictamente necesaria para el cumplimiento del servicio por parte del tercero.
- Están implementados los procedimientos de supervisión y control de las actividades del tercero.
- Los recursos informáticos empleados por el tercero en el suministro del servicio han sido homologados y aprobados por PISA.

d. Revisión periódica de niveles de acceso de usuarios de entes externos

El Oficial de Seguridad de la Información en coordinación con el Responsable de la Información, deben realizar periódicamente una revisión formal de los derechos de acceso de los usuarios de entes externos que acceden a la información de PISA.

e. Verificación de la Seguridad de la Información de Terceros



Se debe evaluar regularmente el cumplimiento de los compromisos de seguridad de la información de PISA por parte de terceros y contratistas.

4.9. Identificación y autenticación individual en la infraestructura local y en el ciberespacio

a. Código de usuario Único

Cada colaborador debe tener asignado un único código de usuario para obtener acceso a cada una de las plataformas y aplicaciones que utilice ya sea que estos se encuentren de forma local y/o en el ciberespacio.

¹⁵ Código Malicioso: Software que es creado con el propósito de hacer daño. Los virus informáticos están catalogados como código o software malicioso.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

b. Uso Personalizado del Código de Usuario

Los usuarios de los recursos informáticos de PISA ya sean que se encuentren en la infraestructura o el ciberespacio no deben compartir su código de usuario/contraseña o cualquier mecanismo otorgado para su identificación y autenticación. La responsabilidad que un usuario de PISA adquiere al recibir su código de usuario/contraseña o cualquier mecanismo de identificación y autenticación se extiende a todo tipo de interacción que ese código de usuario tenga en el sistema.

c. Identificación y Autenticación de Usuarios y Programas

Para el acceso a cualquier *recurso informático*¹⁶ de PISA ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio mediante la red, pública o privada, se requiere un proceso de identificación y autenticación del colaborador ante el programa al que se accede; este proceso será parte del sistema de identificación y autenticación.

d. Mecanismos de Identificación y Autenticación

Todos los recursos informáticos de PISA ya sea se encuentre en la infraestructura tecnológica local o en el ciberespacio deben disponer de los mecanismos que soliciten la identificación y autenticación del usuario de los programas que pretendan acceder.

e. Creación y eliminación de códigos de Usuario

PISA debe contar con procedimientos documentados para la creación y eliminación de códigos de Usuario, ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio. Igualmente debe disponer de las herramientas que permiten la creación y eliminación de los códigos de usuarios, manteniendo la información histórica de los mismos (*Logs*¹⁷). La eliminación de un código de usuario debe realizarse de manera inmediata una vez ha finalizado la vinculación laboral entre PISA y el colaborador o cuando este ha cambiado de responsabilidades o cargo y no se requiera que acceda a esos Recursos informáticos.

f. Inactivación de Usuarios

PISA debe disponer de mecanismos para deshabilitar el acceso de aquellos usuarios que se ausenten o no hayan accedido a los Recursos informáticos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, por un período prolongado de tiempo, aquellos que hayan presentado un número determinado de intentos fallidos durante el ingreso de la contraseña, aquellos a los que el Responsable de la Información explícitamente indique y a los que por razones de seguridad los entes de control señalen.

g. Bloqueo por Inactividad de Sesiones

Con el fin de proteger la información de PISA, el usuario deberá bloquear la sesión de trabajo cuando se ausente de su puesto de trabajo y requiera dejar su computador en posición de encendido.

h. Creación de Contraseñas

Todas las contraseñas de los aplicativos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio deben ser creadas de acuerdo con el estándar establecido por PISA para tal fin. Se puede tener el apoyo de herramientas automáticas que aseguren el cumplimiento del estándar de creación de contraseñas.


i. Asignación de Contraseñas

La asignación de contraseñas debe ser controlada por un proceso de administración formal que permita:

- Obtener el compromiso escrito de los usuarios de mantener la confidencialidad de las contraseñas.
- Asegurar que los usuarios acaten los estándares y recomendaciones para la elección y el cambio de contraseñas.
- Notificar de manera segura las contraseñas temporales/iniciales a los usuarios.
- Confirmar la recepción de las contraseñas por parte de los usuarios.

¹⁶ Recurso informático: Un recurso informático es cualquier aplicación, herramienta, componente o dispositivo que se puede agregar a una computadora o sistema; por lo tanto, puede ser tanto un recurso de hardware (dispositivos) como de software (programas).

¹⁷ Log: Archivo donde se registran las diversas actividades realizadas por los usuarios en el sistema (rastros).

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

j. Vigencia de Contraseñas

Las contraseñas usadas para acceder a los recursos informáticos de PISA ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, deberán ser cambiadas periódicamente. La contraseña debe tener una vigencia mínima de tiempo luego del cual el usuario puede realizar un cambio de contraseña, la cual vencerá automáticamente después de transcurrida la vigencia máxima establecida. Un usuario con contraseña vencida requiere ingresar una nueva contraseña para acceder a los Recursos informáticos. El usuario debe ser informado previamente al vencimiento de su contraseña. Se debe llevar un registro histórico de las últimas contraseñas para evitar que las mismas sean repetidas después de un cierto número de cambios.

k. Cambio de Contraseñas

PISA debe disponer de un procedimiento documentado para el cambio de contraseña de los usuarios. El procedimiento de cambio de contraseña debe ser ejecutado en forma automática cuando un usuario acceda a los recursos informáticos por primera vez, cuando la vigencia de la contraseña haya expirado o cuando la contraseña haya sido reinicializada, ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio. Este procedimiento también estará disponible para que pueda ser realizado manualmente por el usuario cuando lo estime conveniente.

l. Confidencialidad de la contraseña

Las contraseñas o cualquier otro método de autenticación de los aplicativos o servicios ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio deben mantener el nivel de información restringida. Las contraseñas o cualquier otro mecanismo de autenticación deben ser entregadas a los usuarios de forma personal y a través de un medio que asegure su confidencialidad.

m. Cifrado de Contraseñas

Las contraseñas de acceso deben ser almacenadas por medio de un algoritmo de cifrado reconocido por la industria y no deben ser susceptibles de ser descifradas. Las contraseñas nunca pueden ser almacenadas en formato texto. Para esto se debe considerar la incorporación de un algoritmo de cifrado reconocido por la industria el cual no debe permitir el descifrado de la contraseña.

n. Bloqueo de Contraseñas

La identificación del usuario debe ser deshabilitada de los aplicativos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio si el usuario falla durante un número limitado de intentos al ingresar la correspondiente contraseña.

o. Acceso a Recursos Informáticos mediante el uso de una sesión desatendida.

Los usuarios deben acceder a los recursos informáticos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, mediante una sesión iniciada utilizando su propio código de usuario y contraseña. Un usuario no debe usar una sesión de trabajo iniciada por otro usuario.

p. Usuarios por Defecto

A todos los códigos de usuario que vienen por defecto con los sistemas operativos, bases de datos y productos de las diferentes plataformas de PISA se les debe restringir el acceso.



q. Usuarios Privilegiados¹⁸

La asignación de privilegios de acceso a la información de PISA debe ser controlada mediante un proceso formal de autorización del Responsable de la Información. En general los usuarios con privilegios especiales deben usar métodos de acceso y comunicación seguros y sus acciones deben ser monitoreadas de manera periódica.

r. Prohibición a la suplantación de usuarios

Está prohibida la suplantación, el enmascaramiento o la firma por otros usuarios de correos electrónicos o de acceso a cualquier recurso informático de PISA. Los usuarios deben usar siempre su código de usuario para acceder a los Recursos informáticos de PISA, incluso si deben hacerlo desde una estación diferente a la asignada.

¹⁸ Usuarios privilegiados: Individuos que tiene autoridad por el Responsable de la información para ver, modificar, adicionar, divulgar, eliminar o acceder a dicha información.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

4.10. Control y administración del acceso de usuarios a la información

a. Acceso a la información

Los accesos a la información de PISA por parte de los usuarios ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, deben ser definidos y autorizados por el Responsable de la Información (Jefes/Gerentes/Directores del área a la que pertenece el usuario) y deben estar basados en requerimientos específicos del negocio.

b. Controles de acceso lógico

Con el objeto de prevenir el acceso no autorizado a la información contenida en los recursos informáticos de PISA, ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, se deben establecer controles de acceso lógico que permitan el acceso únicamente a los usuarios autorizados. Los recursos informáticos deben:

- Controlar los accesos de usuarios a los datos y funciones de PISA conforme a las políticas de control de acceso definidas. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.
- Proveer la protección del acceso no autorizado a cualquiera de los *utilitarios*¹⁹ del software operativo o de soporte de los aplicativos que sea capaz de modificar los parámetros del sistema o de la aplicación.
- Evitar comprometer la seguridad de otros recursos de informáticos que sean compartidos con otras aplicaciones.

c. Definición de Perfiles acordes al rol

Se deben crear perfiles de acceso asociados a roles que tengan responsabilidades y cumplan con actividades comunes; estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios de los aplicativos y servicios ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio.

d. Definición de Perfiles de Usuario

Los permisos de acceso a los aplicativos de PISA ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, deben ser garantizados a grupos de usuarios y no a individuos. Se deben otorgar permisos de acceso a los Recursos informáticos en función de grupos. Estos grupos deben ser conformados por individuos cuyo rol, responsabilidad y actividades sean equivalentes. Cada grupo debe ser asociado a un perfil de acceso autorizado por el Responsable de la Información y los usuarios a quienes sea asignado un mismo perfil contarán con los mismos privilegios.



Un usuario que pertenezca a más de un grupo debe tener la suma de todos los privilegios asociados con cada uno de los grupos a los que pertenece.

e. Asignación de accesos basados en los perfiles de usuario aprobados

La Dirección de Sistemas de PISA debe asignar a los usuarios los privilegios de acceso a la información ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio con base en los perfiles de usuario aprobados por PISA y no basados en requerimientos individuales. Estos privilegios deben estar autorizados por el Responsable de la Información.

¹⁹ Utilitarios: Son herramientas o programas diseñados para realizar una función determinada, por ejemplo, un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro o aquellos que resuelven problemas relacionados con la administración del sistema de los equipos de cómputo como:

- Tareas de Mantenimiento,
- Revisión de software,
- Recuperación de datos perdidos,
- Eliminación de software maliciosos,
- Cifrado de archivos,
- Compresión de archivos,
- Desfragmentadores de disco,
- Editores de texto,
- Respaldo

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

f. Perfiles de Auditoría

Se debe contar con perfiles especiales para ser usados por la función de Auditoría. Los Auditores deben tener privilegios para ver la información del negocio acorde con su clasificación ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio y no pueden realizar ningún tipo de modificación.

g. Actualización de los privilegios de acceso a la información

Se deben deshabilitar o actualizar los privilegios de acceso a los recursos informáticos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio cuando se presente la novedad correspondiente o cuando se genere un cambio de privilegios en un rol o perfil. Cuando un colaborador o un usuario externo deje PISA o cambie de rol/cargo, se deben eliminar o reasignar sus privilegios de acceso a los Recursos informáticos de PISA.

h. Manejo centralizado de privilegios

Los privilegios de los usuarios de los Recursos informáticos deben ser manejados y controlados centralizadamente, de acuerdo con los lineamientos del Modelo de Seguridad de la Información.

i. Verificación del nivel de acceso real de los usuarios

El Oficial de Seguridad de la Información ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, debe realizar una comparación periódica entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que realmente cuentan y verificar que los usuarios que efectivamente acceden la información corresponden a los autorizados por el Responsable de la Información.

j. Restricciones de acceso a la información

El acceso a los recursos informáticos de PISA y sus datos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, debe ser otorgado de acuerdo con las POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD para acceso a la información, estar basado en los requerimientos individuales de cada aplicación y otorgando los menores privilegios posibles. La aplicación de los siguientes controles debe ser considerada para soportar los requerimientos de acceso:

- Proporcionar menús para controlar el acceso de los usuarios a las funciones de los aplicativos.
- Restringir la divulgación de datos o funciones de los recursos informáticos que los usuarios no están autorizadas a acceder.
- Controlar las capacidades de acceso de los usuarios mediante el uso de perfiles y grupos de perfiles.
- Asegurar que las salidas de los aplicativos que manejan datos sensibles contengan únicamente los datos que son relevantes para el uso de la salida y se envíen exclusivamente a los usuarios y/o terminales autorizadas.
- Incluir revisiones periódicas de las salidas de aplicativos asegurando que se eliminen los datos redundantes.

k. Restricción de accesos del personal a los diferentes ambientes informáticos o en el ciberespacio

El personal que realiza funciones asociadas a un ambiente específico (desarrollo, pruebas y producción) ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio debe contar con perfiles de acceso que limiten sus actividades exclusivamente al ambiente en el que trabajan. En caso de que por razones propias del negocio se requiera que el personal deba acceder a ambientes diferentes al que tienen asignado para la realización de su trabajo, se deberá documentar y justificar plenamente esta situación y dejar la trazabilidad necesaria que permita establecer las acciones realizadas en el sistema.

l. Acceso a los datos de producción sólo a través de aplicativos

El vehículo normal de acceso a los datos de producción de PISA son los aplicativos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio. Cualquier otro modo de acceso a los datos, deberá ser plenamente justificado y documentado.

m. Usuarios Administradores

Los usuarios privilegiados de los recursos informáticos ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio, deben ser los autorizados por el Responsable de la Información y deben disponer de dos códigos de usuario. Los usuarios privilegiados como administradores del sistema o de bases de datos de PISA, deben ser los que el Responsable de la Información ha dispuesto para tal fin y deben disponer de dos códigos de usuario, uno para la ejecución de actividades privilegiadas

y otro para la ejecución de las actividades habituales de usuario, con el fin de reducir el riesgo de incurrir en errores no intencionales o en utilizar privilegios sin autorización ni justificación.

n. Usuarios de Emergencia y Usuarios Backups

Se debe establecer un programa de administración de usuarios de emergencia y backups para ser utilizado en caso de ausencia de los titulares de los roles, ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio. Se deben establecer medidas de protección y respaldo para las claves de usuarios de emergencia con el fin de garantizar la confidencialidad y disponibilidad en caso de requerirse. Los usuarios de emergencia deben estar limitados a usuarios privilegiados, las claves deben ser cambiadas cada vez que se usen y se debe documentar la situación que requirió el uso de estos usuarios y las acciones que realizaron.

o. Restricción en el uso de Utilitarios

El conocimiento y utilización de utilitarios sensitivos debe ser restringido a usuarios privilegiados que por su rol requieran su aplicación. Los eventos asociados a su uso deben ser incluidos en el Log del sistema para que puedan ser verificados y controlados en forma periódica, ya sea que se encuentre en la infraestructura tecnológica local o en el ciberespacio. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se registrará bajo los términos definidos en el contrato para la prestación del servicio.

p. Bloqueo de puertos en Equipos de Cómputo

La utilización de los puertos en los equipos de cómputo de PISA debe ser restringida a usuarios que por su rol lo requieran y su uso debe ser autorizado por la Gerencias y validado periódicamente.

4.11. Clasificación de la información

a. Categorías de clasificación

Toda la información, independientemente del medio en el que se encuentre, debe estar clasificada en una de las siguientes categorías de acuerdo con el estándar de clasificación de información establecido por PISA:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Restringida	Alta	Misión Crítica
Uso Interno	Media	Crítica
Pública	Baja	No Crítica

Los Responsables de la Información deberán realizar a partir del *Cuadro de Clasificación Documental*, la clasificación o reclasificación de acuerdo con las tres (3) categorías definidas por PISA.

b. Rotulado de medios de Información

Toda información clasificada como restringida y almacenada en cualquier medio (físico, magnético, portable o impreso), ya sea que se encuentre en la infraestructura local o en el ciberespacio debe ser rotulada. En caso de que la información contenga piezas de distinto tipo, ésta debe rotularse con la clasificación más alta de cualquier elemento de información contenida.

c. Recursos Informáticos con información de diferentes categorías de clasificación



Si un recurso informático contiene información con varias categorías de clasificación, ya sea que se encuentre en la infraestructura local o en el ciberespacio, los controles usados para su protección deben reflejar la mayor de las categorías que contenga.

d. Divulgación de la clasificación de la Información

Todos los colaboradores deben conocer la clasificación de la información que utilizan para el desarrollo de sus actividades.

e. Protección de información de los Usuarios de la Vía y de los Datos Personales

La clasificación de la información de los Usuarios de la Vía es restringida en PISA, al igual que los Datos Personales cuyo tratamiento realice PISA según lo establecido en la POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES, ya sea que se encuentre en la infraestructura local o en el ciberespacio.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

f. Información restringida en estaciones de trabajo o PC's

La información restringida que se encuentre en las PC's debe ser adecuadamente protegida. Además de la contraseña de acceso a la red deberá contar con protector de pantalla y contraseña.

g. Intercambio de Información con entes externos, entes de control, entidades y filiales

El intercambio con entes externos de información Restringida o de Uso Interno de PISA, ya sea que se encuentre en la infraestructura local o en el ciberespacio, debe hacerse únicamente con la autorización del Responsable de la Información y aplicando los controles necesarios tales como la existencia de un acuerdo previo de términos contractuales garantizando la Confidencialidad, Autenticidad e Integridad y controles de cifrado y certificados digitales durante el intercambio de esta. El intercambio de información con Terceros, Entes de Control, Entidad o Filial se debe realizar sólo si es requerido por razones de negocio.

h. Información Restringida almacenada electrónicamente

La información Restringida almacenada electrónicamente ya sea que se encuentre en la infraestructura local o en el ciberespacio, debe ser adecuadamente protegida. Se debe evaluar respecto al riesgo al que está expuesta, la implementación de controles tales como ser cifrada y firmada electrónicamente cuando se vaya a respaldar, guardar y transmitir si es requerido.

i. Confidencialidad de las llaves de cifrado

Las llaves de cifrado son clasificadas como información restringida. El control de las llaves de cifrado de la información debe ser estricto. Las llaves de cifrado deben ser consideradas como un activo de información altamente crítico y restringido.

j. Mecanismos para incrementar la seguridad de las llaves de cifrado

Para las llaves de cifrado deben considerarse controles adicionales para incrementar su Confidencialidad, Integridad y Disponibilidad. Entre los mecanismos que incrementan la seguridad de las llaves de cifrado pueden citarse la clave dual, tiempo definido de expiración, mecanismos de emergencia, manejo del intercambio, seguridad de almacenamiento, entre otros.

k. Destrucción de Información Restringida

Cuando la información restringida o de uso interno de PISA, por razones de negocio, deba ser desechada se debe destruir de manera segura, independiente del medio en que ésta se encuentre. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se registrará bajo los términos definidos en el contrato para la prestación del servicio.

l. Destrucción de información contenida en recursos que se entregan a terceros

Cuando un recurso informático va a ser dado a cambio, enviado a servicio o desechado, la información almacenada en él debe ser destruida de manera segura conforme a los métodos aprobados por PISA.



m. Validación de integridad de la información

La información de PISA ya sea que se encuentre en la infraestructura local o en el ciberespacio, que de acuerdo con el principio de integridad se encuentra clasificada como "Alta", debe contar con mecanismos que permitan validar su integridad y autenticidad durante el almacenamiento y/o transmisión a través de los recursos informáticos. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se registrará bajo los términos definidos en el contrato para la prestación del servicio.

4.12. Continuidad del negocio

a. Seguridad del Plan de Continuidad del negocio

Los planes de continuidad del negocio deben mantener los niveles de seguridad establecidos en el Modelo de Seguridad de la Información y Ciberseguridad de PISA, para los servicios habilitados durante el evento de contingencia. Se debe definir una estrategia permanente de recuperación para la operatividad de los Recursos informáticos, así como desarrollar, documentar, probar y mantener los planes de recuperación que conduzcan a su restauración, teniendo en cuenta la seguridad definida en las políticas y normas de seguridad de la información PISA. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se registrará bajo los términos definidos en el contrato para la prestación del servicio.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

b. Respaldo de Información Crítica, Software y datos de Seguridad

Las copias de respaldo de la información crítica de PISA ya sea que se encuentre en la infraestructura local o en el ciberespacio, deben ser realizadas en forma periódica de modo que se garantice su disponibilidad. Se deberá definir la periodicidad de la ejecución de los procesos de respaldo de la información crítica PISA. Esta periodicidad debe considerar los requerimientos del Responsable de la Información.

Las copias de respaldo del Software de seguridad deben tener mayores medidas de control que el resto del Software. Se deben considerar medidas como acceso único por personal de seguridad, almacenamiento en sitios diferentes, la identificación de medios en forma inteligible y generación de mayor número de copias; adicionalmente y de acuerdo con la criticidad de los aplicativos y datos de seguridad, en la medida que lo permita la plataforma, deben realizarse copias de respaldo completas (Sistema Operativo y Aplicativo) que faciliten la recuperación mediante comandos de restauración. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

c. Usuarios de contingencia y continuidad

Se deben definir usuarios de contingencia y un programa de administración de estos, para ser utilizados en el momento en que se presente la contingencia en la infraestructura local o en el ciberespacio. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

d. Custodia de los medios de respaldo de la Información de misión crítica

Los medios de respaldo de la información de misión crítica de PISA se deben almacenar en localidades alternas y seguras.

e. Pruebas de restauración de Información crítica

Se deben realizar pruebas periódicas de los medios que contienen copias de respaldo de información crítica que incluyan la restauración y verificación de la información. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

f. Programa para el control de Código Malicioso

Debe existir un programa completo a nivel institucional de protección contra código malicioso en los equipos de PISA, ya sea que se encuentre en la infraestructura local o en el ciberespacio. Este programa debe contemplar:

- El manejo adecuado de copias de respaldo de la información, por medio de la educación al usuario ante el peligro del código malicioso y sus consecuencias.
- El acceso y uso de repositorios de software y recursos informáticos de producción que limite el acceso a los sistemas y programas y el uso de las funciones en los sistemas para disminuir el riesgo de las infecciones por virus.
- La detección de infecciones por virus con el empleo regular de software apropiado que mantenga un registro lleve estadísticas, verifique cambios a objetos ejecutables, permanezca activo y en alerta ante sucesos inesperados.
- La actualización permanente del software antivirus.



En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

g. Erradicación de código malicioso por expertos

Los usuarios no deben intentar erradicar el código malicioso de los Recursos informáticos por sus propios medios, ya sea que se encuentre en la infraestructura local o en el ciberespacio. Si un usuario sospecha que un recurso informático está bajo los efectos de un código malicioso, debe suspender el uso de este inmediatamente y solicitar asistencia al Oficial de Seguridad de la Información.

h. Planes de Contingencia y Continuidad en los Contratos con Terceros

Con el fin de apoyar la continuidad del negocio y continuar con las actividades y procesos críticos, los terceros con quien PISA contrata, cuya falla afecte directamente la prestación del servicio a sus Clientes y Usuarios, ya sea que se encuentre en la infraestructura local o en el ciberespacio, deben disponer de planes de contingencia y continuidad del servicio.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

4.13. Seguridad física

a. Clasificación de áreas, análisis de riesgo y plan de seguridad física para áreas críticas

Las áreas físicas de PISA deben ser clasificadas considerando entre los principios necesarios, la criticidad de la información que resguarden, con el fin de establecer los controles de seguridad necesarios.

Seguridad Física de áreas de acceso restringido

Deben existir controles estrictos para la autorización y el registro del personal que ingresa a las áreas donde se encuentren los Recursos informáticos que contienen activos críticos de información y a las áreas que trabajan con información clasificada como Restringida. El acceso a las áreas donde residen los componentes de la red de comunicación y de Recursos informáticos que soportan actividades críticas de PISA, debe ser estrictamente controlado y restringido. El acceso debe estar permitido únicamente a personal formalmente autorizado.

b. Restricciones de acceso al centro de cómputo

Los únicos usuarios autorizados para acceder en forma permanente al centro de cómputo de PISA son aquellos que, en virtud de sus actividades y responsabilidades, deban hacerlo. Las demás personas deberán ser previamente autorizadas y registrar tanto su ingreso como su salida.

c. Seguridad física para información restringida

La información clasificada como restringida de PISA debe preservar las características de seguridad cuando es almacenada físicamente y por ningún motivo debe ser desatendida. La persona que genera información, con este tipo de clasificación, en un medio de almacenamiento portable es responsable por el buen uso que se haga de la misma y por el cumplimiento de las directrices que se emitan para la protección de la información.

d. Protección de medios de almacenamiento

Los medios de almacenamiento de PISA que contienen copias de respaldo de información deben protegerse en concordancia con la clasificación de la información que almacenan.

e. Equipos de seguridad ambiental en áreas de almacenamiento de activos críticos de información

Las áreas donde se encuentran Recursos informáticos que contienen activos de información crítica de PISA deben contar con equipos de seguridad ambiental, procedimientos formales para su uso y controles periódicos de verificación de su estado.

f. Uso de equipos de seguridad ambiental

Los operadores deben recibir capacitación en el uso de los equipos de seguridad ambiental para control de situaciones de emergencia y este conocimiento debe ser reforzado periódicamente.

g. Circuitos alternos y equipos de respaldo para el suministro de energía

Las áreas de procesamiento de información crítica, y las indispensables para la operación del negocio, deben contar con circuitos alternos y equipo de respaldo para suministro de energía con los procedimientos y la capacitación del personal para su correcto uso.

h. Manejo de llaves físicas

Se deben establecer mecanismos y responsabilidades frente a la administración centralizada de las llaves físicas que permiten el ingreso a las áreas de acceso restringido, a los muebles donde se guardan componentes críticos de red y las áreas que almacenan Activos Críticos de Información.

i. Ingreso de visitantes a áreas de acceso restringido

Deben existir controles específicos y de obligatorio cumplimiento para el acceso de visitantes a áreas de acceso restringido de PISA. Únicamente el personal de PISA, formalmente autorizado, puede acceder a las áreas restringidas en función de las actividades que desarrolla. En el caso que colaboradores de otras áreas y/o de entes externos requieran ingresar a estas áreas, deben obtener autorización del Responsable del Área Crítica y seguir los procedimientos establecidos.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

j. Verificación de registros y alertas de acceso a áreas críticas

Los registros de acceso y alertas de intento de violación a las áreas protegidas deben ser revisados periódicamente por el responsable del área. Las bitácoras de visitas y los reportes de alertas de intento de acceso no autorizado a las áreas de acceso restringido deben ser revisados de manera exhaustiva por el Responsable del área y los permisos registrados deben ser validados.

k. Plan de mantenimiento preventivo de equipos

Se debe establecer y ejecutar un plan de mantenimiento periódico que cubra todos los Recursos informáticos de PISA.

l. Obras civiles en áreas de acceso restringido

Todos los cambios estructurales dentro de los lugares destinados al procesamiento de datos y/o almacenamiento de Recursos informáticos críticos deben ser programados y desarrollados de acuerdo con un plan, observando las medidas de seguridad necesarias para la protección de los equipos.

m. Consumo de alimentos en áreas que contienen Recursos Informáticos

Está prohibido consumir alimentos en las áreas de acceso restringido que contienen recursos informáticos críticos para PISA.

n. Escritorios Limpios y Pantallas Limpias

Toda la información de PISA clasificada como "Restringida" debe conservarse en lugares seguros cuando no se esté utilizando (cajas fuertes, archivadores, etc.). En los escritorios de los PC's y servidores no debe permanecer información "Restringida" para evitar su acceso no autorizado.

4.14. No repudio

a. Certificación de transacciones

Con el fin de garantizar la aceptación en la realización de transacciones efectuadas entre PISA, los clientes y entes externos, ya sea que se encuentre en la infraestructura local o en el ciberespacio, se deben establecer mecanismos de certificación para las transacciones que así se consideren.

b. Trazabilidad de la transacción

Por cada transacción ya sea que esta se realice a través de la infraestructura local o en el ciberespacio se debe registrar la información necesaria que permita establecer como mínimo: usuario ejecutor, fecha, hora y el estado de realización de la transacción.

c. Responsabilidad del emisor con la custodia del certificado digital

Es absoluta responsabilidad del emisor de una transacción la custodia y uso que se dé al certificado digital suministrado para la realización de transacciones electrónicas. El emisor de la transacción electrónica debe conocer y asumir la responsabilidad que implica el uso del certificado digital y los cuidados que debe tener para mantener su confidencialidad.

d. Administración y uso de tokens

PISA deberá contar con un procedimiento de administración de tokens, en el cual se establezcan las condiciones de manejo de estos, así como las normas de seguridad que los colaboradores hagan uso responsable de los mismos.



4.15. Administración de alertas

a. Generación automática de alertas

Se deben implementar herramientas automáticas de generación de alertas. Se debe implantar, en los distintos recursos informáticos en función de la criticidad de la información que manejen, la funcionalidad de generar automáticamente alertas hacia las distintas funciones de negocio involucradas.

b. Generación de alertas en tiempo real

Los recursos informáticos críticos deben disponer de mecanismos que alerten sobre eventos que comprometan su integridad, confidencialidad y/o disponibilidad. Deben existir herramientas de generación de alertas en tiempo real a nivel de hardware, sistema

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

operativo, software de administración y/o software de seguridad, las cuales deben ser habilitadas en concordancia con la clasificación y criticidad del recurso informático.

c. Información estándar en la generación de alertas

Se debe establecer información estándar en la generación y registro de alertas que permita documentar en forma completa el evento y provea a PISA el nivel de detalle suficiente que facilite su detección, entendimiento, priorización, seguimiento y resolución.

d. Monitoreo centralizado de alertas

Se deben implantar mecanismos para el monitoreo centralizado de alertas que faciliten su detección, notificación y seguimiento. Los mecanismos de monitoreo centralizado deben detectar tempranamente posibles eventos o incidentes de seguridad, independiente de la aplicación o plataforma que los genere.

e. Análisis de registros de Alertas en Logs de Auditoría

Se deben utilizar herramientas que permitan la extracción y el análisis de los registros de alertas para el desarrollo de una gestión eficiente de verificación, control y seguimiento. Se debe contar con herramientas que faciliten la extracción, análisis y consolidación de alertas en Logs de auditoría y que permitan generar informes estadísticos que faciliten la identificación y seguimiento a posibles violaciones de seguridad de PISA.

f. Responsabilidad de reporte de desviaciones o vulnerabilidades

Todo integrante de PISA es responsable por reportar en forma inmediata cualquier condición anormal o vulnerabilidad que detecte en el uso los recursos informáticos de PISA.

g. Reserva de la información sobre vulnerabilidades

La información específica sobre las vulnerabilidades o condiciones anormales de seguridad de la información tiene carácter de restringida y solo debe darse a conocer a personas autorizadas y que tengan una necesidad demostrada de saberlo.

h. Estructura de comunicación de eventos o incidentes

PISA debe establecer y mantener un procedimiento formal de reporte de eventos o incidentes de seguridad de la información que le permita a los usuarios, terceros y entidades, informar acerca de éstos cuando se presenten o se tenga sospecha de su ocurrencia.

Las directrices establecidas deben incluir los mecanismos para responder a un incidente de seguridad, la activación de los planes de continuidad de negocio (en caso de que aplique) y la recolección y preservación de la evidencia.

i. Seguimiento de eventos o incidentes

Todo evento o incidente de seguridad debe ser tratado de principio a fin mediante un procedimiento de tratamiento de incidentes que garanticen el análisis, investigación, documentación, solución completa y seguimiento a cualquier incidente de seguridad.

En PISA se deben evaluar los eventos de seguridad, para determinar si se debe tratar como un incidente.


j. Consistencia de Ambientes Tecnológicos

Todos los sistemas automatizados de PISA deben utilizar los requerimientos normativos definidos en el modelo de seguridad y ciberseguridad, de tal manera que se garantice la consistencia y exactitud de los registros en cualquier parte de la infraestructura tecnológica y/o en el ciberespacio.

4.16. Auditabilidad de los eventos de Seguridad de la Información

a. Registros de auditoría

Los recursos informáticos deben incluir registros de auditoría que involucren cualquier evento susceptible de verificación posterior e incluyan el código de usuario que lo generó.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

b. Periodo de la retención de registros de eventos de seguridad y ciberseguridad

Se deben retener los registros que contienen eventos relevantes de Seguridad de la Información y Ciberseguridad por un periodo mínimo de tiempo. Durante este periodo, deben afianzarse los registros en archivos históricos tal que no puedan modificarse y sólo puedan ser leídos por personas autorizadas.

c. Disponibilidad de información de Auditoría

La información de auditoría de PISA debe estar disponible para su uso por las personas autorizadas para tal fin.

d. Evaluación de la Información de auditoría

La información de auditoría generada por los Recursos informáticos debe ser evaluada periódicamente para verificar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.

e. Programa regular de Auditoría de Seguridad de la Información

El Modelo de Seguridad de la Información y Ciberseguridad debe ser auditado. PISA debe programar y ejecutar auditorías a la seguridad de la información que verifiquen el cumplimiento y efectividad del Modelo de Seguridad de la Información y Ciberseguridad establecido.

f. Monitoreo de usuarios privilegiados

Se deben registrar de manera permanente y revisar continuamente las actividades de usuarios privilegiados como los Administradores de Recursos informáticos, Instaladores de Software, Operadores, Administradores de Control de Acceso Lógico, etc.

g. Sincronización de relojes

La fecha y la hora deberán estar sincronizadas en todos los Recursos informáticos de acuerdo con un estándar, ya sea que se encuentre en la infraestructura local o en el ciberespacio, para asegurar que los registros reflejan el tiempo exacto de ocurrencia. En el caso de que se trate de Recursos informáticos ubicados en el exterior, se deben tener en cuenta las diferencias horarias.

h. Verificación de la Seguridad de la Información y Ciberseguridad por parte de entes externos

Se debe evaluar regularmente el cumplimiento de los compromisos de seguridad de la información y Ciberseguridad de PISA por parte de Terceros y Entidades. El incumplimiento de los requerimientos de seguridad se debe registrar como un incidente a la seguridad de la información que debe ser resuelto de acuerdo con las normas y procedimientos para tratamiento de incidentes de PISA.

4.17. Conectividad

a. Segregación de Redes

Se deben definir zonas separadas que agrupen lógicamente los Recursos informáticos de PISA de acuerdo con la criticidad de los activos de información que manejan, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio.

b. Uso de los firewalls de PISA como únicos puntos de acceso a redes externas



El Firewall es el único punto autorizado por PISA para el establecimiento de conexiones de cualquier recurso informático de PISA con redes externas. Otro tipo de conexiones deberán estar debidamente autorizadas y justificadas antes de ser implantadas.

c. Confidencialidad de la información técnica de la red

La información técnica de la red interna de PISA (direcciones internas, configuración y diseño de la red), ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio, debe estar restringida al personal autorizado que tenga necesidad legítima de conocerla y con una autorización explícita del Responsable de la Información. Toda la información mencionada tiene carácter de restringida y debe recibir el tratamiento definido para este nivel de confidencialidad.

d. Controles de enrutamiento

Se debe contar con mecanismos que controlen el enrutamiento en la red. El acceso a los Recursos informáticos de PISA desde redes externas o internas requiere que se verifique y controle que el acceso sea realizado exclusivamente sobre los Recursos

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

informáticos de compañía objeto de la autorización, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio.

e. Control de acceso entre zonas de red

Todas las zonas deben considerar los mecanismos de control de acceso consecuentes con el nivel de confidencialidad de la información que allí reside, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio.

f. Autenticación de conexiones remotas

Los accesos desde puntos remotos o redes específicas externas, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio, deben contar con mecanismos de autenticación de la conexión que prevengan de posibles accesos no autorizados.

g. Integridad de la información en la red

Se deben considerar en la arquitectura de la red los mecanismos apropiados que minimicen la probabilidad de que la información que fluye en la red pueda ser alterada, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio.

h. Restricción de envío de información hacia redes externas

Únicamente con autorización del Responsable de la Información, cuando exista una razón justificada de negocio y cuando se adhiera al procedimiento de uso y manejo de información confidencial, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio, se pueden realizar transferencias de datos y archivos hacia redes externas, incluida Internet.

i. Acceso restringido a servicios de Internet

El acceso de usuarios a los servicios de Internet sólo puede ser autorizado cuando haya sido plenamente justificado y obedezca a propósitos legítimos del negocio y se debe eliminar o restringir cuando el usuario no requiera utilizar dichos servicios para el desarrollo de sus actividades.

Deben existir categorías de navegación en Internet de acuerdo con las actividades y responsabilidades de los usuarios.

4.18. Uso de los recursos informáticos de PISA, de dispositivos móviles y de trabajo móvil

a. Uso de Recursos informáticos de PISA sólo en actividades propias del negocio

Los Recursos informáticos de PISA, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio, deben ser utilizados únicamente para fines de negocio aprobados por PISA. Está prohibido el uso de los Recursos informáticos de PISA en actividades distintas a las del negocio.

b. Ingreso y uso de información ajena para propósitos de negocio en PISA

Sin importar la fuente de donde provenga, la información que ingrese mediante medios electrónicos a PISA y su utilización en la infraestructura tecnológica local y/o en el ciberespacio, está supeditada a propósitos exclusivos del negocio y debe estar explícitamente autorizada por el Responsable de la Información.

c. Uso de Recursos informáticos de Seguridad autorizados



Solamente los Recursos informáticos de seguridad suministrados por PISA y autorizados a través del Oficial de Seguridad de la Información o la Dirección de Sistemas se deben utilizar en la protección de los activos de información.

d. Uso restringido de herramientas propias de la Gestión de Seguridad de la Información y Ciberseguridad

Únicamente el Oficial de Seguridad de la Información y personal autorizado de la Dirección de Sistemas están facultados por PISA para utilizar herramientas propias de la gestión de Seguridad de la Información y Ciberseguridad.

e. Restricción en el uso de privilegios

Está prohibido intentar sobrepasar los controles de seguridad de los Recursos informáticos, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio, buscar vulnerabilidades de seguridad y/o examinar los Recursos informáticos en busca de información, sin la autorización expresa del Oficial de Seguridad de la información. Los usuarios sólo deben ingresar a

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

las funciones u opciones de los aplicativos inherentes a su cargo, así le sean asignados permisos o privilegios adicionales por deficiencias en los sistemas de control de acceso lógico o por error en la definición de su perfil.

f. Seguridad en dispositivos móviles

Todos los dispositivos móviles que contienen datos almacenados de propiedad PISA, deben tener los controles adecuados para proteger la información almacenada en los mismos de acuerdo con los riesgos a los que está expuesta.

Sólo los usuarios que acepten la implementación de los controles de seguridad en los dispositivos móviles (ya sean asignados por PISA o sean de propiedad del colaborador), pueden acceder y almacenar datos de PISA a través de estos dispositivos.

g. Seguridad de la información cuando se accede a través de servicios de tecnología de movilidad (Trabajo Móvil)

Los colaboradores de PISA que por sus responsabilidades tengan la justificación para acceder a la información a través de servicios de tecnología que permitan movilidad (trabajo móvil), deben estar debidamente autorizados. Los accesos y/o servicios deben ser los específicos a cada funcionario, de acuerdo con las tareas a desarrollar.

PISA debe implementar los controles necesarios en cuanto a conectividad, cifrado de la información transferida y almacenada, gestión de permisos de acuerdo con la necesidad de acceso y medidas de concientización.

h. Cumplimiento de las políticas y las normas de seguridad en el uso de los servicios de Internet, Intranet y Mensajería Instantánea

Todo usuario debe ser consciente y cumplir las políticas y las normas de Seguridad de la Información y Ciberseguridad de PISA cuando hace uso de los servicios de Internet, Intranet y Mensajería Instantánea. Los usuarios autorizados explícitamente por PISA para acceder a servicios de Internet, Intranet y Mensajería Instantánea son absolutamente responsables de la utilización que hagan de dichos servicios y por las consecuencias que se deriven de su utilización.

La información que se publique en la Intranet de PISA debe contar con la aprobación del responsable del área encargada de la página y la del Responsable de la información involucrada.

Los colaboradores que accidentalmente se conecten a páginas de Internet que tengan contenidos sexuales, racistas o cualquier otro tipo de material ofensivo deben desconectarse inmediatamente e informar al Oficial de Seguridad de la Información, para que sean bloqueados estos accesos.

El ancho de banda de la red y la capacidad de almacenamiento tienen límites; por lo tanto, los usuarios no deben realizar deliberadamente actos que desperdicien los Recursos informáticos, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio, ni monopolicen los recursos injustamente en detrimento de los demás usuarios. Estos actos incluyen, entre otros: enviar correos masivos o cartas de cadena, pasar períodos prolongados en Internet desarrollando actividades personales, jugar, usar inadecuadamente las charlas en línea, cargar o descargar archivos de gran tamaño, acceder a archivos de audio o vídeo de remisión continua o crear de cualquier otra forma cargas innecesarias en el tráfico de la red asociadas con el uso de Internet que no se relacione con las actividades de negocio.



PISA tiene derecho a supervisar y registrar cualquier y todos los aspectos de su sistema informático incluyendo, entre otros, la supervisión de sitios de Internet visitados por usuarios, la supervisión de charlas y foros de noticias, la supervisión de descargas de archivos y todas las comunicaciones enviadas y recibidas por los mismos utilizando los Recursos informáticos de PISA.

i. Replicación de mensajes de divulgación general y/o advertencias provenientes de fuentes externas a PISA.

Está prohibida la replicación de mensajes de divulgación general o de advertencias públicas relacionadas con Seguridad de la Información y Ciberseguridad hacia otros usuarios sin la autorización explícita del Oficial de Seguridad de la Información. Únicamente el Oficial de Seguridad de la Información y la Dirección de Sistemas o quién ellos deleguen están autorizados para el envío de mensajes de divulgación general o de advertencias públicas provenientes de fuentes externas a PISA y que estén relacionadas con Seguridad de la Información y Ciberseguridad.

j. Prohibición del envío de mensajes en cadenas, bromas y advertencias de virus

Está prohibido el envío de mensajes cadena, bromas y advertencias de virus. El uso de los Recursos informáticos de PISA ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio, para el reenvío de correos con mensajes cadena o advertencias de virus no está permitido. Todo correo recibido con alertas sobre un supuesto virus o la existencia de código dañino dentro de PISA debe ser verificado con el Oficial de Seguridad de la Información.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

Los colaboradores no deben usar una cuenta de correo electrónico que pertenezca a otro colaborador. Si hay necesidad de hacerlo en caso de ausencias y vacaciones se debe recurrir a mecanismos alternos como redirección de mensajes.

Está prohibido utilizar el correo electrónico interno para difundir, visualizar o almacenar anuncios personales o comerciales, ofertas de servicios, promociones, códigos destructivos (por ejemplo: programas conocidos como virus, troyanos, etc.) o ningún otro material no autorizado.

k. **Uso de carpeta compartidas**

El propietario de la información debe definir los controles necesarios para proteger la información que se vaya a publicar en carpetas compartidas; entre otros se debe tener en cuenta:

- Usuarios que deben tener acceso a la carpeta
- Definir los permisos necesarios a cada usuario (control total, lectura, escritura, entre otros)
- Realizar periódicamente depuración de los contenidos de las carpetas compartidas con el fin de que se realice copias de seguridad únicamente a la información necesaria para PISA.

l. **Uso de dispositivos externos (Memorias USB, Discos externos entre otros)**

Solo se podrá conectar los dispositivos comprados y asignados por la Dirección de Sistemas a los equipos de PISA y que previamente cuenten con la autorización del Jefe Inmediato del colaborador que lo requiera y Oficial de Seguridad de la Información.

4.19. **Seguridad de Información y Ciberseguridad en los procesos de administración de sistemas**

a. **Introducción de nuevos Recursos informáticos a PISA**

Se deben configurar los parámetros de seguridad y ciberseguridad a todo nuevo recurso informático que se implante en PISA, de acuerdo con las normas y estándares establecidos que se hayan definido en el procedimiento GESTIÓN DE CONTROL DE CAMBIOS EN LOS APLICATIVOS E INFRAESTRUCTURA. No se pueden implementar nuevos componentes tecnológicos sin que previamente se incluyan todas las medidas de seguridad requeridas. Para ello, se deben implantar las facilidades disponibles en el equipo, en cuanto a seguridad se refiere y adaptarlas en función de las normas y los estándares definidos en el procedimiento GESTIÓN DE CONTROL DE CAMBIOS EN LOS APLICATIVOS E INFRAESTRUCTURA.

b. **Virtualización y Computación en la nube**

El uso de la virtualización y la computación en el ciberespacio en PISA debe llevarse a cabo implementando los controles necesarios para mitigar los riesgos introducidos por estas tecnologías.

c. **Estándares de Plataforma**

Se debe definir un estándar específico de configuración de opciones y parámetros por plataforma que considere los requerimientos de operación segura para los Recursos informáticos de PISA, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

d. **Implantación de estándares de plataforma**

Todo recurso informático de PISA debe ser configurado de acuerdo con el estándar formalmente establecido de la correspondiente plataforma, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

e. **Gestión de las vulnerabilidades técnicas**

PISA debe implementar un proceso de gestión de las vulnerabilidades técnicas de su plataforma tecnológica que incluya los responsables en su gestión, las acciones a implementar y el plazo para la mitigación. Ver GESTIÓN DE CONTROL DE CAMBIOS EN LOS APLICATIVOS E INFRAESTRUCTURA, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

f. Adquisición y mantenimiento de Software aplicativo

Debe existir una metodología estándar para la adquisición y mantenimiento del software aplicativo, ya sea que éstos se encuentren en la infraestructura tecnológica local y/o en el ciberespacio. Dicha Metodología debe incluir los controles de seguridad de la información que garanticen que la adquisición y mantenimiento de las aplicaciones cumplen las Políticas y Normas de seguridad de la información de PISA. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

g. Actividades de desarrollo y mantenimiento de software por personal interno o terceros

Los desarrollos y actividades de mantenimiento de software realizadas por personal interno o por terceros deben cumplir las políticas, normas, procedimientos, y estándares de desarrollo de software (incluyendo las directrices para desarrollo seguro) formalmente establecidos por PISA. El Responsable de la Información, debe asegurarse que todas las actividades de desarrollo de software realizadas por personal interno o terceros cumplen con los requerimientos solicitados, En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

h. Desarrollo de aplicaciones seguras

Los requerimientos de seguridad de la información y ciberseguridad deben ser cumplidos durante todo el ciclo de desarrollo y mantenimiento de software y éstos deben ser integrados desde el principio como parte de la solución y deben ser verificados previos a su puesta en producción. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

i. Liberación de nuevos desarrollos

La puesta en producción ya sea en la infraestructura tecnológica local y/o en el ciberespacio, de nuevos desarrollos o modificación de aplicativos es permitida únicamente si estos cuentan con la seguridad mínima establecida en las políticas, normas y estándares de seguridad para el desarrollo aplicaciones. La implantación de nuevos aplicativos que no contemplen los mecanismos mínimos de seguridad sólo se puede realizar mediante un proceso formal de excepción, a través de la aceptación formal del riesgo por parte del Responsable de la Información. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

j. Documentación del Software

Toda adquisición, desarrollo o modificación de software, ya sea en la infraestructura tecnológica local y/o en el ciberespacio, debe incluir el suministro o actualización de la documentación correspondiente del producto. Es obligación de quien adquiere o solicita un desarrollo o modificación del software de PISA, requerir la documentación del producto o la actualización de los manuales para el caso de cambio.

k. Diccionario de datos

Se debe definir un diccionario de datos que corresponda a la información que contienen las bases de datos de compañía, ya sea en la infraestructura tecnológica local y/o en el ciberespacio. El administrador de la base de datos debe definir y divulgar a las áreas con interés legítimo el diccionario de datos de PISA.

l. Separación de ambientes

Los ambientes de desarrollo, pruebas y producción de los Recursos informáticos de PISA deben encontrarse separados, ya sea en la infraestructura tecnológica local y/o en el ciberespacio. Se deben definir controles físicos y de acceso lógico para garantizar esta separación de ambientes. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se regirá bajo los términos definidos en el contrato para la prestación del servicio.

m. Paso de aplicativos a producción

Los sistemas aplicativos de PISA deben haber pasado por un proceso completo de pruebas y certificación por parte del Responsable de la Información, antes de ser liberados a producción en un ambiente dedicado para tal fin, ya sea en la infraestructura tecnológica local y/o en el ciberespacio. Ver GESTIÓN DE CONTROL DE CAMBIOS EN LOS APLICATIVOS E INFRAESTRUCTURA.

n. Manejo de Información de Producción en otros ambientes

La información de producción sólo debe ser utilizada en ambientes de desarrollo, pruebas, Q.A., entre otros (diferentes al ambiente de producción), ya sea en la infraestructura tecnológica local y/o en el ciberespacio, con los debidos controles para proteger su

 Proyectos de Infraestructura S.A.S.	NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			 Proyectos de Infraestructura S.A.S.
	SEGURIDAD DE LA INFORMACIÓN			
	Código: SI-DG-02	Versión: 11	USO INTERNO	

confidencialidad. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se registrará bajo los términos definidos en el contrato para la prestación del servicio.

o. Control de Procesos

La ejecución de procesos debe ser los autorizados en PISA y realizarse de acuerdo con las instrucciones formalmente documentadas, ya sea en la infraestructura tecnológica local y/o en el ciberespacio. Ver GESTIÓN DE CONTROL DE CAMBIOS EN LOS APLICATIVOS E INFRAESTRUCTURA.

p. Actualización simultánea de registros

Debe existir protección contra la actualización simultánea de un registro buscando que se mantenga la integridad de los datos, ya sea en la infraestructura tecnológica local y/o en el ciberespacio. Durante la actualización de archivos o bases de datos, el registro afectado debe ser protegido para que ningún otro programa lo modifique.

q. Integridad referencial en Bases de Datos

Todos los modelos de datos deben manejar integridad referencial, mediante herramientas de base de datos o implantados en la programación del aplicativo, ya sea en la infraestructura tecnológica local y/o en el ciberespacio. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se registrará bajo los términos definidos en el contrato para la prestación del servicio.

r. Mecanismos para la preservación de la integridad en los aplicativos

Las aplicaciones por sí solas deben asegurar que la información que se procesa mantenga su integridad, ya sea en la infraestructura tecnológica local y/o en el ciberespacio. En el diseño de aplicaciones se debe considerar la existencia de validaciones para el ingreso correcto de la información, mecanismos de verificación que aseguren su correcto procesamiento, especialmente cuando se realizan cálculos y alertas que comuniquen desviaciones críticas o de alto impacto. En el caso que el servicio sea prestado por un tercero en el ciberespacio, se registrará bajo los términos definidos en el contrato para la prestación del servicio.

s. Arquitectura Tecnológica de Seguridad

La infraestructura tecnológica local y/o ciberseguridad debe contemplar los aspectos de seguridad definidos en el Modelo de Seguridad de la Información y Ciberseguridad de PISA.

5. DOCUMENTO DE APROBACIÓN

Junta Directiva N°410 del 18 de febrero 2025.

6. DOCUMENTOS RELACIONADOS

CÓDIGO	NOMBRE DEL DOCUMENTO
SI-DG-01	Política de Seguridad de la Información y Ciberseguridad
SI-DG-03	Organización de Seguridad de la Información y Ciberseguridad
GA-DG-11	Política de Protección de Datos Personales
TIC-PT-03	Gestión de Control de Cambios en los Aplicativos e Infraestructura
N/A	Cuadro de Clasificación Documental

7. RELACIÓN DE FORMATOS Y/O REGISTROS

CÓDIGO	NOMBRE DEL DOCUMENTO
SI-FM-03	Compromiso de Confidencialidad de Usuario de Aplicativos, Herramientas o Información de la Compañía.

8. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
31 de enero de 2019	9	<p>Todo el Documento. Donde adicionalmente se incluyen los siguientes cambios</p> <ul style="list-style-type: none"> • Eliminación de convenciones para cada directriz de la Política de Seguridad de la Información. • Se recodifica el documento asignado código SI, asociado al área de seguridad de la información. • Se separa las Normas de las Políticas
Acta N°352 25 agosto 2020	10	<ul style="list-style-type: none"> • Se actualiza la Norma incluyendo lo relacionado con los temas de ciberseguridad. • Se incluye en el punto 4.18 USO DE LOS RECURSOS INFORMÁTICOS DE LA COMPAÑÍA, DE DISPOSITIVOS MÓVILES Y DE TRABAJO MÓVIL, el ítem I → Uso de Dispositivos extraíbles. • 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. <p>25/07/2022 – Se realizan los siguientes cambios menores:</p> <ul style="list-style-type: none"> • 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". <p>23/05/2024 – Se realiza el siguiente cambio menor:</p> <ul style="list-style-type: none"> • Se actualiza la estructura del documento, de acuerdo con el estándar actualmente establecido por el área de Mejoramiento.
Acta N°410 18/02/2025	11	<ul style="list-style-type: none"> • Se realizan los siguientes ajustes. • Se modifica el alcance del documento incluyendo a concesiones CCFC, De acuerdo con lo establecido en el otrosí No. 5 del contrato de prestación de servicios suscrito entre PISA y CCFC, y a las instrucciones dadas por la Junta Directiva. • Se Actualiza el nombre del responsable de la autorización para el acceso del documento pasando del Área de Mejoramiento y Sostenibilidad al responsable de Procesos • Se incluye la competencia que tiene la junta directiva frente a los lineamientos corporativos de acuerdo con la estructura definida.