PLAN DE SEGURIDAD DE LA INFORMACIÓN

Aprobado de Sesión de Directorio de fecha 27.12.2019

Contenido

1. Introducción

BLANCO SAFI (en adelante la SAFI) es una Sociedad de Fondos de Inversion es consciente del valor de su información y de la necesidad que tiene la misma de ser protegida de los riesgos a los que está expuesta. Para tal fin ha creído conveniente implementar un Sistema de Gestión de Seguridad de la Información, basada en los estándares internacionales ISO 27001.

2. Objetivo

El presente plan tiene como objetivo establecer políticas, procedimientos, y controles, así como una estructura organizacional para garantizar la integridad, confidencialidad y disponibilidad de los activos de información de BLANCO SAFI.

3. Alcance

El presente plan tiene como alcance los siguientes procesos críticos de BLANCO SAFI:

Nro.	Proceso	Áreas involucradas
1	Estructuración e inscripción de un Fondo	Área Comercial, Legal, Contabilidad y Operaciones
2	Colocación del Fondo (Captura de partícipes)	Área de Comercial y Operaciones.
3	Inversiones y comité de inversiones	Área Inversiones, Legal, Tesorería y Operaciones
4	Pago a Partícipes	Área Tesorería y Operaciones
5	Valorización de las cuotas	Área Operaciones

4. Base Legal

El presente documento está basado en la Resolución SMV N° 037-2015 Reglamento de la Gestión Integral de Riesgos y su modificatoria 027-2016 y en el estándar internacional ISO/IEC 27001:2013.

5. Definiciones de Términos

a) **Activo de Información**: cualquier información o recurso informático que tiene valor para la organización, por lo tanto debe ser protegido.

b) **Código malicioso:** programa que oculta funciones que buscan dañar u obtener información de manera no autorizada.

c) **Contingencia:** interrupción que afecta directa o indirectamente la capacidad de la organización para ofrecer niveles de servicio adecuados a nuestros clientes, proveedores, organizaciones externas o cualquier unidad organizacional.

d) **Control dual:** Se refiere a que el trabajo de una persona sea verificado por otra asegurando que ha seguido el plan de autorización en las operaciones y que éstas han sido correctamente registradas y ultimadas.

e) **Identificador de usuario o grupo:** un identificador de usuario se asigna a una persona para facilitarle el acceso a un sistema de información. Hay casos en que un identificador es utilizado por un grupo de usuarios de manera autorizada, identificando qué persona es la que usa el identificador en un momento determinado.

f) **Incidente de Seguridad de información:** Evento asociado a una posible falta en la política de seguridad, una falla de los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

g) **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

h) **Objetivo de Control:** Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de una tecnología de información particular.

i) **Proceso crítico:** Proceso considerado indispensable para la continuidad de las operaciones y servicios de BLANCO SAFI, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la Compañía.

j) **Propietario:** es la persona que organizativamente tiene la responsabilidad de mantener operativos sus activos de información, determinar su criticidad y clasificación, establecer los requerimientos de protección y validar los derechos de acceso a los usuarios.

k) **Recurso Informático:** hardware, software y comunicaciones, destinado al tratamiento de la información

l) **RIT:** Reglamento Interno de Trabajo, tiene como objeto establecer el marco normativo sobre el cual se desarrollarán las actividades laborales orientadas a mantener y desarrollar las relaciones armoniosas entre la BLANCO SAFI y sus trabajadores dependientes.

m) **Seguridad de la Información:** Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura

organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios siguientes:

- Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
- Integridad: La información debe ser completa, exacta y válida.
- Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

n) **Sistema de Gestión de la Seguridad de la Información (SGSI):** tiene como propósito garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

o) **SMV:** Superintendencia de Mercado de Valores.

6. Entorno de TI

6.1 Organización de TI

BLANCO SAFI cuenta con un área de sistemas propiamente dicha, compuesta por un Jefe de TI y un asistente de sistemas, quien tiene por función dar el soporte al sistema actualmente usado por la SAFI para sus operaciones financieras. Las funciones de Administración de la red, infraestructura y equipos de cómputo están a cargo de una empresa de terceros, Digital Dynamics SAC.

Para el establecimiento y cumplimiento de las políticas de seguridad, la SAFI ha establecido un Oficial de Seguridad de Información cargo que recae en Violeta Rivera.

A la fecha las personas designadas para las funciones antes mencionadas son:

- Oficial de Seguridad – Violeta Rivera
- Jefe de sistemas - Jose Florindez,
- Asistente de sistemas - Percy Tomairo

6.2 Centro de Cómputo e Infraestructura Tecnológica

El centro de cómputo de BLANCO SAFI que contiene los activos de la compañía se ubica en el piso 8 de la Torre El Pilar del Centro Comercial Camino Real en San Isidro. El acceso a dicho centro de datos, se encuentra protegido con una cerradura física.

La infraestructura tecnológica de BLANCO SAFI está compuesta por:

- Un servidor de dominio
- Un firewall

- Un servidor de aplicación (Spectrum)

6.3 Sistemas de Información

La Compañía cuenta con los siguientes sistemas de información:

- Spectrum Fondos, sistema que soporta el proceso de administración de los Fondos, Este sistema fue comprado a un tercero con códigos fuentes lo que le permite al analista programador de la SAFI llevar a cabo el soporte y mantenimiento del mismo.
- Sistema Siscont adquirido a la empresa Siscont S.A., únicamente en códigos compilados, por lo que el soporte de este se encuentra en manos de su proveedor.

7. Evaluación de Riesgos

El plan de seguridad de la información se desarrolló con base al resultado obtenido en la evaluacion de riesgos, cuyo alcance y metodología se describen en el Manual de Gestion de Riesgos. Mediante esta evaluación se identificaron los recursos críticos involucrados en cada proceso así como las amenazas, a los que estaban expuestos dichos activos. La determinación del riesgo se calculó en base a la probabilidad de ocurrencia de cada riesgo y el impacto que tendría de materializarse en el proceso al que perteneciá el impacto. Los controles necesarios para reducir el impacto de los riesgos identificados son tratados en el plan así como los que por cumplimiento al estándar internacional ISO 27001 son ineludibles para proveer seguridad a la información.

Mediante el Anexo 1 se muestra la Matriz de Análisis de Riesgos elaborada.

8. Procedimientos de seguridad de información

El plan de seguridad de la información desarrollado en el presente documento, está orientada al aseguramiento de la confidencialidad, integridad y disponibilidad de la información e incluye las normas, controles y procedimientos en los siguientes dominios:

- Organización de la seguridad
- Clasificación y control de activos de información
- Seguridad de personal
- Seguridad física y ambiental
- Seguridad de comunicaciones y operaciones
- Control de accesos
- Adquisición, Desarrollo y Mantenimiento de sistemas de información
- Gestión de incidentes
- Gestión de Continuidad del Negocio

- Cumplimiento

8.1 Organización de la seguridad

Objetivo de control: administrar la seguridad de la información dentro de la organización y establecer el marco gerencial y las responsabilidades para controlar su implementación.

Descripción: El Oficial de Seguridad de la información es el encargado de proponer los controles de seguridad de información adecuados que cumplan con el Plan de Seguridad de Información y permitan reducir el riesgo de eventos perjudiciales para la organización.

El jefe de cada área debe colaborar con la Implementaclón y velar por el cumplimiento de los controles de seguridad de Información relacionados a su área. Es responsabilidad de todos los usuarios de la organización, clientes y proveedores tecnológicos cumplir y hacer cumplir estas políticas.

Controles:
a) Organización interna

Comisión de Seguridad de Información.

- BLANCO SAFI cuenta con una Comisión de Seguridad de Información que se encargará de promover la seguridad de información dentro de la organización y elevar los requerimientos para el cumplimiento y mejora del SGSI al Comité de Gerencia.
- El Comité de Gerencia será el encargado de recibir los requerimientos de la Comisión de Seguridad de Información, evaluarlos y determinar su aprobación y asignación de recursos de ser el caso.
- La Comisión de Seguridad de Información estará conformada por el Gerente General, el Oficial de Seguridad y el jefe de Sistemas. Adicionalmente podrán participar el asistente de sistemas a cargo del sistema Spectrum y el representante de la empresa Digital Dynamics a cargo del soporte de la infraestructura de hardware y software de la SAFI.

COMISIÓN DE SEGURIDAD DE INFORMACIÓN			
Rol	**Presidido por**	**Nombre**	**Área**
Comité de Gerencia	Gerente General	María Luisa Aguirre	Gerencia General
Oficial de Seguridad de Información	Gerente de Riesgos	Violeta Rivera	Riesgos

Responsable de Seguridad de Información	Jefe de Sistemas	Jose Florindez	Sistemas

- El Oficial de Seguridad será el encargado de velar por el cumplimiento de los controles implementados, así como recomendar controles o mejoras de seguridad de información.
- El área de Auditoria interna, será la encargada de coordinar las revisiones a las normas de seguridad de informaci ón implementadas.
- El Responsable de Seguridad de Información estarán a cargo de establecer, implementar y mantener el Sistema de Gestión de Seguridad de Información (SGSI) de BLANCO SAFI.
- Todo el personal está obligado a comunicar cualquier brecha, incidencia o evento de seguridad de información de manera oportuna al Oficial de Seguridad y al Gerente de Operaciones a cargo de las funciones de sistemas de la SAFI,

Asignación de responsabilidades sobre seguridad de información.

La responsabilidad de la Seguridad de Información en BLANCO SAFI, comprende las siguientes instancias:

- La Gerencia General será la encargada de establecer las políticas de seguridad de información de la organización.
- La Gerencia de Riesgos será la encargada de apoyar y asistir a las demás unidades de la organización para la aplicación de la metodología de gestión del riesgo operacional, que sirve como base para el establecimiento de controles.
- El Jefe de sistemas y el representante de la empresa Digital Dynamics serán los encargados de generar, implementar y mantener el SGSI.
- El Oficial de Seguridad es el encargado de velar por el cumplimiento y correcto funcionamiento del SGSI.
- Es responsabilidad de todo el personal, proveedores y terceros de BLANCO SAFI, cumplir la presente política, así como participar en la identificación de riesgos de seguridad de información.
- El incumplimiento, omisión o negligencia en relación a la seguridad de información es tipificada por como falta grave y sancionada según el RIT.
- BLANCO SAFI deberá asegurar a todo el personal, los recursos necesarios para la comunicación de brechas y/o incidentes de seguridad de información.
- El área de Recursos Humanos, será la encargada de hacer de conocimiento las políticas de seguridad de información a todo el personal y proveedores que inicien su labor en BLANCO SAFI.
- El Oficial de Seguridad de información está a cargo de comunicar al personal sobre cualquier modificación a las políticas de seguridad de información.

Proceso de autorización de recursos para el tratamiento de información.

- La adquisición de un nuevo recurso informático se realizará de acuerdo a la normativa respectiva, controlando el nivel de exposición al riesgo.

- La autorización para el acceso y uso de recursos informáticos deberá ceñirse a la normativa respectiva.

Acuerdos de confidencialidad.

- El personal de BLANCO SAFI y sus proveedores firmarán cláusulas donde se les obligue a la confidencialidad de la información a la que tiene acceso como consecuencia del desempeño de sus funciones o de su desenvolvimiento dentro de la organización, tanto en los negocios de la organización así como en el ámbito administrativo.
- Una cláusula de confidencialidad de información se incluirá en los contratos y en el RIT, para el caso del personal de BLANCO SAFI.
- Una cláusula de confidencialidad de información se incluirá en los contratos, para el caso de proveedores de bienes, servicios y terceros.
- La vigencia de esta obligación de confidencialidad, se extenderá incluso hasta después del cese de la relación contractual o laboral con la organización, de manera indefinida.

Contacto con las autoridades.

- La organización externa reguladora de la seguridad de información para BLANCO SAFI es la Superintendencia de Mercado de Valores (SMV).
- Se acogerán como buenas prácticas aquellas normas dictadas por las entidades reguladoras del estado (INDECOPI).

Contacto con grupos de interés especial.

- Las políticas de seguridad de información se mantendrán actualizadas respecto de las normativas internacionales acerca de seguridad de información, tales como ISO/IEC, ANSI, COBIT u otros, así como de las buenas prácticas de empresas que han implementado o se especializan en la implementación de dichos estándares.
- Es responsabilidad del Oficial de Seguridad proponer modificaciones a las normativas de acuerdo a lo indicado en el numeral anterior.

Revisión independiente de la seguridad de la información.

- El alcance de la organización para la gestión de la seguridad de información y su implementación (objetivos de control, controles, políticas, procedimientos u otros) serán revisados y/o actualizados cuando ocurran cambios significativos en la organización y de manera periódica. Esta revisión debe ser tanto por la Comisión de Seguridad de Información como por una empresa de auditoría externa especializada.
- Esta revisión es necesaria para asegurar la conveniencia, eficacia y suficiencia del SGSI así como para detectar la necesidad de mejoras y cambios.

b) Terceras partes.

Identificación de riesgos por el acceso de terceros

- Antes de la contratación de proveedores que tengan acceso a la información de la Compañía, se realizará una evaluación de riesgos.

- Los proveedores que tengan acceso a activos de información de BLANCO SAFI cumplirán con todos los controles establecidos en este documento y otros adicionales considerados en el contrato.

8.2 Clasificación y control de activos de información

Objetivo de control: establecer los controles de seguridad de información necesarios para cada activo de información dependiendo de su clasificación.

Descripción: la Jefatura de Sistemas y el Oficial de Seguridad es la encargada de definir una metodología de clasificación de los activos de información de la organización, según su confidencialidad, integridad y disponibilidad, en base a la cual se definirá su criticidad, se realizará el marcado correspondiente y se implementarán las medidas de protección, acceso, transporte y destrucción adecuadas.

Controles:
a) Responsabilidad sobre los activos de información

Inventario de activos de información
- Es responsabilidad de la Jefatura de Sistemas, realizar y mantener permanentemente el inventario de activos de información, y realizar periódicamente el inventario físico de dichos activos.
- Es responsabilidad del Oficial de Seguridad, verificar la ejecución periódica del inventario y su actualización.

Propiedad de los activos de información
- BLANCO SAFI es el propietario de los activos de información de la organización, y delega dicha propiedad a los jefes de cada área con la finalidad de descentralizar y mejorar la eficiencia en la administración de la seguridad de información.
- Los jefes de área también delegarán la propiedad de los activos de información de manera jerárquica al personal a su cargo, por lo que dicho personal será responsable directamente de la custodia de los activos de información asignados para el cumplimiento de sus funciones e indirectamente de aquellos activos que se encuentran en su medio ambiente de trabajo, manteniendo los jefes de área la responsabilidad ya asignada.
- El área de Sistemas está a cargo de la custodia de los activos de información que se encuentran instalados en el Centro de Cómputo Principal, por lo cual deberá implementar los controles necesarios para preservar su seguridad.

Uso adecuado de los activos de información.
- Los usuarios deberán seguir las instrucciones de la normativa respectiva para el uso adecuado de los activos de información.
- El jefe de cada Gerencia debe verificar que el personal a su cargo dé una adecuada protección a los activos de información asignados.

- Los usuarios no realizarán actividades no autorizadas, ni tratarán de vulnerar la seguridad de los activos de información de BLANCO SAFI. Cualquier intento o acción que pueda debilitar o debilite el nivel de seguridad de los activos de información será considerado como falta que podrá ser sancionada según el Reglamento Interno de Trabajo (RIT).

b) Clasificación de activos de información.

La Clasificación de activos inicial se elaborará como parte del manual de riesgos y del análisis de impacto de negocios, posteriormente será actualizado por el oficial de Seguridad en coordinación con el propietario del activo de información, realizará la clasificación de los respectivos activos, de acuerdo a la normativa respectiva.

La Clasificación de los activos de información efectuada a la fecha es la siguiente:

BLANCO SAFI - INVENTARIO DE ACTIVOS DE INFORMACIÓN

CRITICIDAD	ACTIVO	SUBPROCESO	PROCESO
A	Información sobre Fondo	Registro de Fondo ante SUNAT (RUC) y apertura de libros contables	Estructuración e inscripción de un Fondo
		Crear Fondo en el sistema de Fondos	
		Publicación de Fondo	Colocación del Fondo (Captura de partícipes)
		Entregar los números de cuenta a cada partícipe para realizar los aportes	
		Ejecuta proceso de desembolso	Desembolso
		Registra operaciones de desembolso en sistema de Fondos	
A	Información de partícipe	Solicitar al partícipe, información relacionada a PLAFT	Colocación del Fondo (Captura de partícipes)
		Pago de intereses a las cuentas de los partícipes	Pago a Partícipes
A	Información de cliente (Resultados de evaluación crediticia)	Evaluar situación crediticia del cliente	Inversiones y comité de inversiones
B	Contrato de inversión	Elaborar contrato para cliente	Inversiones y comité de inversiones
B	Sistema de Fondos Spectrum	Registro de Fondo ante SUNAT (RUC) y apertura de libros contables	Estructuración e inscripción de un Fondo
		Crear Fondo en el sistema de Fondos	

		Registro del partícipe y su aporte en el sistema	Colocación del Fondo (Captura de partícipes)
		Elaborar contrato para cliente	Inversiones y comité de inversiones
		Ejecuta proceso de desembolso	
		Registra operaciones de desembolso en sistema de Fondos	
		Pago de intereses a las cuentas de los partícipes	Pago a Partícipes
		Ejecutar proceso de valorización de la cuota	Valorización de las cuotas
B	Servidor de aplicación	Registro de Fondo ante SUNAT (RUC) y apertura de libros contables	Estructuración e inscripción de un Fondo
		Crear Fondo en el sistema de Fondos	
		Registro del partícipe y su aporte en el sistema	Colocación del Fondo (Captura de partícipes)
		Elaborar contrato para cliente	Inversiones y comité de inversiones
		Ejecuta proceso de desembolso	
		Registra operaciones de desembolso en sistema de Fondos	
		Pago de intereses a las cuentas de los partícipes	Pago a Partícipes
		Ejecutar proceso de valorización de la cuota	Valorización de las cuotas
C	Certificado de participación	Registro del partícipe y su aporte en el sistema	Colocación del Fondo (Captura de partícipes)

LEYENDA

CRITICIDAD	
A	**Imprescindible para la Gestión de Riesgos**
B	**Necesario**
C	**Importante. Se requiere pero puede someterse a las reglas del RTO y RPO**

8.3 Seguridad de personal

Objetivo de control: reducir los riesgos de error humano, comisión de ilícitos o uso inadecuado de los activos de información.

Descripción: todo el personal y proveedores tendran conocimiento y recibirán capacitación sobre las políticas de seguridad de información, así como las funciones y responsabilidades a las que ésta conlleva.
El proceso de selección de personal y de proveedores permitirá reducir el riesgo de su contratación que puedan dañar a la organización. Se firmarán acuerdos de confidencialidad que se extiendan incluso después del cese de la relación laboral o contractual. Se deben especificar las sanciones en caso de incumplimiento.

Controles:

a) Seguridad antes del empleo.

Inclusión de la seguridad en las responsabilidades y funciones laborales

- Se hará de conocimiento del personal y de los proveedores sobre las políticas de seguridad de información así como las funciones y responsabilidades a las que ésta conlleva.
- Estas funciones y responsabilidades deben estar claramente definidas y documentadas.

Selección y política de personal

- Previo a la contratación de personal o proveedores, se verificará sus antecedentes respectivos, en proporción a los requisitos de la organización, la clasificación de información a ser accedida y a los riesgos percibidos.
- Se asegurará que el personal que está siendo contratado signifique un riesgo administrado por la organización.

Acuerdos de Confidencialidad.

- En la contratación personal nuevo o de proveedores, se asegurará la firma del Acuerdo o Cláusula de Confidencialidad, descrito anteriormente, especificando además en el contrato las responsabilidades y derechos del empleado y de la Compañía en relación a la protección de la información, así como su manipulación y uso dentro y fuera de las instalaciones de la Compañía.
- El personal y proveedores de BLANCO SAFI quedan terminantemente prohibidos de acceder a información no autorizada, divulgar, eliminar, alterar o realizar copias no autorizadas de la información a la que tenga acceso por motivo de sus funciones o por su desenvolvimiento dentro de la organización.

b) Durante el empleo.

Responsabilidades de las Gerencias

- Es responsabilidad de todos los gerentes y jefes de área de BLANCO SAFI velar por el cumplimiento por parte del personal y proveedores, de las políticas establecidas en el presente documento.

Concientización, educación y entrenamiento en seguridad de la información.

- Todo proveedor debe ser informado con respecto a las políticas de seguridad de información vigentes.

- Todo el personal de BLANCO SAFI será capacitado e informado de manera continua y actualizada respecto a las responsabilidades, políticas, controles y procedimientos establecidos en seguridad de información.
- La información brindada en esta capacitación será acorde con la función desempeñada y estará enfocada en la formación de una cultura en seguridad de información, la toma de conciencia y la identificación y comunicación de riesgos e incidencias de seguridad.
- Las reuniones de trabajo donde se discute y maneja información sensible, se realizarán en salas cerradas para que personas ajenas a dicha información no tengan acceso.
- El personal y proveedores mantendrá la información tanto física como electrónica utilizada para el cumplimiento de sus funciones, en lugares seguros de acuerdo a la clasificación de dicha información.
- Todo el personal protegerá la información que se transmite por teléfono o en conversaciones, de manera que no se exponga información confidencial de la Compañía de manera casual.

Proceso disciplinario.

- Es responsabilidad de todo el personal de BLANCO SAFI, comunicar al Oficial de Seguridad y Responsable de la Seguridad de información, sobre el incumplimiento o violación de las políticas de seguridad de información por parte de otro trabajador.
- Se impondrá la sanción necesaria según la normativa respectiva sobre procesos laborales y el RIT, en base al nivel de incidencia o daño que dicho incumplimiento o violación haya causado, según la evaluación del Responsable de Seguridad de Información y de la Unidad de Personal.

c) Finalización o cambio de empleo.

Responsabilidades de finalización.

- El Jefe de Personal informará oportunamente a la Jefatura de Sistemas, sobre el fin de contrato del personal con BLANCO SAFI, a fin de que puedan tomar las medidas preventivas y correctivas necesarias.
- En el caso de proveedores, es responsabilidad del Jefe de Administración, informar oportunamente a la Gerencia de Operaciones, sobre el fin de contrato de proveedores, para tomar las medidas preventivas y correctivas necesarias.
- Es responsabilidad de la Jefatura de Sistemas recibir la notificación de salida del personal o proveedores, revocar los accesos respectivos y desactivar los identificadores generados para dicho personal o proveedores, así como realizar las acciones de salvaguarda correspondientes.
- Las funciones y operaciones realizadas serán ser documentadas por el personal saliente, para la continuidad de la misma por parte del personal de reemplazo.

Retorno de activos.

- Todo el personal o proveedor que se separe de la organización, debe retornar todos los activos de información asignados para la realización de sus funciones.

- Es responsabilidad de la Gerencia de Finanzas, designar a un responsable de la verificación de devolución de los activos de información por parte del personal o proveedores salientes.

Cambio de funciones

- Es responsabilidad del Jefe de Personal informar a la Jefatura de Sistemas, sobre el cambio de funciones del personal de BLANCO SAFI, al recibir la notificación de cambio de funciones del personal, modificar los accesos respectivos de los identificadores generados para dicho personal según el perfil correspondiente.

8.4 Seguridad física y ambiental

Objetivo de control: evitar accesos físcos no autorizados, así como daños e interferencia a las sedes, equipos e información de la organización.

Descripción: los recursos y equipos de tratamiento de información deben ubicarse en áreas seguras claramente definidas y protegidas de accesos no autorizados, daños, desastres naturales e interferencias.
Se contará con dispositivos auxiliares tales como extintores, sensores de humo, alarmas, UPS, cámaras de seguridad y otros, cuando el nivel de clasificación de la información lo requiera. Así mismo autorizar y registrar todas las visitas a los locales de la organización y traslados de equipos.

Controles:

a) Áreas seguras.

Perímetro de seguridad física

- Las áreas de almacenamiento de información tendrán un perímetro físico con un nivel de seguridad adecuado de acuerdo a su clasificación.
- Las áreas de procesamiento de información se encontrarán en áreas de acceso limitado o restringido cuando sea necesario, dependiendo de su clasificación.
- Las áreas de acceso limitado y restringido serán visualmente identificables para el personal de BLANCO SAFI.
- Las áreas de procesamiento de información contarán con mecanismos de identificación, acceso físico y suministros de soporte físico, de acuerdo al nivel de clasificación de la información.
- Existirá un área centralizada de recepción manual de documentos u otros elementos provenientes del exterior de la Compañía, cuyo origen sea claramente identificable y que evite el acceso de extraños a las áreas no públicas.

Controles físicos de entrada

- El Oficial de Seguridad es el encargado de administrar las medidas de control de acceso físico a las instalaciones de BLANCO SAFI.

- En el caso de la Oficina Administrativa, el agente de seguridad de turno solicitará los datos y el motivo de la visita de cualquier persona ajena a la Compañía que desee ingresar a ésta, para posteriormente anunciarla y derivarla al área correspondiente.
- El ingreso a áreas de acceso interno, limitado y restringido será explícitamente autorizado y con algún elemento físico visible de identificación, que distinga la condición de personal, proveedor o visitante.
- Todas las visitas al personal de la Oficina Administrativa serán registradas por el agente de seguridad de turno.
- Las visitas programadas serán anunciadas al agente de seguridad de turno para que sean rápidamente identificadas.
- El ingreso a áreas de acceso limitado y restringido contará con algún elemento de identificación adicional.

Seguridad de oficinas, despachos y recursos

- Las oficinas e instalaciones se diseñarán de manera que protejan la información que en ellas se almacena o procesa, que no sea fácilmente accesible a personas ajenas a la Compañía.
- En lo posible, las oficinas quedarán cerradas cuando no hay personas en su interior.
- Los directorios y las guías telefónicas internas que identifiquen la ubicación de los recursos de información críticos no serán accesibles por personas ajenas a la Compañía.
- Al dejar momentáneamente el sitio de trabajo o al finalizar la jornada, los escritorios y áreas de trabajo deben quedar desprovistos de documentos críticos. Estos quedarán bajo llave en archivadores, credenzas, cajones, cajas fuertes u otros medios seguros.

Protección contra amenazas externas y ambientales.

- Los materiales peligrosos e inflamables se almacenarán distantes a las áreas de tratamiento de información.
- Existirán medios e información de respaldo ubicados a una distancia conveniente, en ubicaciones diferentes de los equipos principales.
- Las áreas de tratamiento de información crítica no serán ubicadas en zonas del edificio vulnerables al ingreso de extraños, a desastres en instalaciones colindantes o a desastres naturales.

El trabajo en áreas seguras

- El acceso a áreas de acceso limitado y restringido serán autorizado por los jefes de las unidades orgánicas respectivas y supervisadas continuamente.
- No se permitirá el uso de equipos de video, fotográficos, de audio u otras formas de registro salvo autorización del Gerente General, con conocimiento del jefe del área afectada.

b) Seguridad de los equipos.

Instalación y protección de equipos.

- Los equipos de procesamiento de información crítica serán protegidos instalándolos en áreas de acceso limitado o restringido.
- Los equipos contarán con mecanismos que impidan o detecten los accesos o instalaciones no autorizados de componentes internos de hardware.
- Los equipos instalados en ubicaciones críticas contarán con mecanismos de anclaje que impidan el traslado de los mismos sin autorización.
- Se divulgarán las condiciones ambientales como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información.
- Se revisará periódicamente las instalaciones de cableado eléctrico, así como de tuberías y/o cañerías que sean colindantes a los activos de información de la Compañía. (Ver control propuesto en Manual de Gestión de Riesgos para el riesgo R03)

Suministros de soporte físico

- Se contará con dispositivos de soporte físico que permitan un óptimo, continuo y seguro funcionamiento de los equipos de cómputo, tales como ventiladores, UPS, estabilizadores, detectores de humo, alarmas u otros; de acuerdo a su nivel de clasificación.
- Los dispositivos de soporte físico serán probados periódicamente para un correcto funcionamiento.
- El personal designado para usar suministros de soporte será entrenado para su uso.
- Se contará con extintores convencionales en oficinas administrativas y con extintores de Halotron en el Data Centre. (Ver control propuesto en Manual de Gestión de Riesgos para el riesgo R01)

Seguridad del cableado

- El cableado eléctrico y de telecomunicaciones seguirá las normas y estándares internacionales correspondientes que garanticen el funcionamiento eficiente de la red.
- La red cableada de telecomunicaciones contará con mecanismos de detección de interferencias, intercepciones o daños, y en lo posible no estar expuesta a manipulación por personas ajenas o no autorizadas por la Compañía.
- El cableado estructurado pasará periódicamente por un proceso de certificación que sea realizada por una entidad externa.

Mantenimiento de equipos

- Los equipos informáticos y suministros de soporte recibirán mantenimiento preventivo periódicamente.
- Sólo personal del área de Sistemas o personas autorizadas realizarán las labores de mantenimiento de los equipos informáticos y suministros de soporte ubicados en el Centro de Cómputo, de acuerdo a la normativa respectiva.
- El mantenimiento preventivo de equipos informáticos o suministros de soporte será oportunamente comunicado a los custodios de los equipos.
- Se registrarán todos los fallos y mantenimientos preventivos y correctivos de los equipos.

Seguridad de equipos fuera de los locales de la organización

- Todo traslado de activos será debidamente autorizado por el custodio del activo y el área de Administración. En el caso de hardware será autorizado adicionalmente por la Jefatura de sistemas. El traslado será registrado en el inventario de activos.
- En los casos en que el traslado del activo sea continuo por motivo de las funciones que el custodio realiza (ejemplo: computadora portátil), se realizará según la normatividad respectiva.
- Todo equipo que requiera de una conexión remota, se someterá a una evaluación de riesgos.

Seguridad en la reutilización o eliminación de equipos

- Se verificará la destrucción de la información de los equipos informáticos que vayan a ser reutilizados o eliminados, mediante mecanismos que aseguren que esta información no sea recuperable, y de acuerdo a la normativa respectiva.

8.5 Seguridad de comunicaciones y operaciones

Objetivo de control: garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Descripción: Se contará con procedimientos documentados para las actividades del sistema asociados con el procesamiento e intercambio de información, y recursos de comunicaciones.
Se planificará la capacidad de los sistemas de información y monitorear el uso de los mismos por parte del personal y de proveedores, para evitar problemas de procesamiento de información, considerando ambientes de desarrollo, prueba y producción separados.
Se contará con mecanismos de protección, detección y eliminación de código malicioso e intrusos en la red interna, así como de recuperación y respaldo automático de la información y procesos críticos.

Controles:

a) Procedimientos y responsabilidades de operación.

Documentación de procedimientos operativos.

- Se elaborará y mantendrám los procedimientos y las guías de usuarios finales, de configuración, de sistemas de información y recursos de comunicación.
- Se contará con los procedimientos documentados de los procesos de contingencia y respaldo por cada sistema o proceso de información crítico.
- Se tendrá identificado a los responsables de la operatividad de cada sistema de informaci ón, así como a los contactos de emergencia respectivos.

Gestión de cambios

- Todos los cambios en los sistemas de información, instalaciones de procesamiento o software base se realizarán de acuerdo a las normativas respectivas de instalación, operación y mantenimiento, que permita identificar y registrar dichos cambios. Estos cambios serán autorizados por la Jefatura de sistemas y probados por la unidad propietaria.
- Todo cambio en el sistema estará de acuerdo a los objetivos establecidos en el Plan Operativo Anual, salvo autorización de rango gerencial.

Segregación de tareas

- Se controlará que las funciones del personal no permitan realizar un mal uso, intencional o accidental, de los sistemas de información, ocasionado por el otorgamiento de accesos excesivos.
- Es responsabilidad del Oficial de Seguridad recomendar la segregación de tareas y control dual para los procesos o tareas críticas, acorde con la complejidad de dichos procesos y el tamaño de la organización.

Separación de los recursos para desarrollo y producción.

- Se establecerán ambientes informáticos separados para desarrollo y producción (procesadores, dominios o directorios distintos), de manera que la funcionalidad de un ambiente no afecte al otro.
- El ambiente de desarrollo y pruebas simulará la configuración del ambiente de producción lo más posible, pero no debe contener los mismos datos, salvo autorización del custodio de los sistemas.
- La aprobación del pase de una aplicación o sistema de un ambiente a otro, se realizará de acuerdo a la normativa respectiva.
- El acceso a los ambientes de desarrollo, pruebas y producción será segregado.

b) Gestión de servicios externos

Provisión de servicios.

- El servicio entregado por proveedores incluirá parámetros de seguridad de información dentro del contrato establecido con BLANCO SAFI o del Acuerdo de Nivel de Servicio (SLA - Service Level Agreement), de ser el caso.
- El nivel de servicio de proveedores tecnológicos será evaluado y aceptado por la Comisión de Seguridad de Información.

Seguimiento y revisión de servicios de proveedores

- Se monitoreará y revisará periódicamente los registros y reportes emitidos por los servicios de proveedores, para verificar el cumplimiento de los parámetros de seguridad de información establecidos.
- La Jefatura de Sistemas y el Oficial de de Seguridad participarán en la revisión del servicio de proveedores tecnológicos.
- Las unidades orgánicas comunicarán las fallas e incidentes en los servicios de proveedores tecnológicos a la Jefatura de sistemas.

Gestión de cambios en servicios de terceros.

- Se registrarán todos los cambios y mejoras realizados en los sistemas de comunicaciones u operaciones por servicios externos según la normativa correspondiente.
- Todo cambio en un sistema de comunicación u operaciones por parte un tercero será autorizado por la Jefatura de sistemas.

c) Planificación y aceptación del sistema.

Planificación de la capacidad

- Se proyectará a futuro las capacidades del sistema para que mantenga un funcionamiento adecuado y requerido, y tomar las medidas preventivas y correctivas del caso.
- Esta proyección estará alineada al Plan Operativo Anual de la organización.
- Se monitoreará el uso de los recursos críticos para identificar y evitar mal uso, problemas de mala configuración o de congestión en la red.

Aceptación del sistema.

- La aceptación de nuevos sistemas de información considerará parámetros de seguridad de información tales como:
  - Rendimiento y capacidad de los equipos informáticos
  - Procedimientos de recuperación ante errores y reinicio
  - Procedimientos de pruebas
  - Procedimiento de Contingencia y Respaldo
  - Usabilidad y capacitación a usuarios
  - Documentación y manuales
  - Otras medidas de seguridad de información adoptadas

d) Protección contra código malicioso

Medidas y controles contra código malicioso.

- No descargará, instalará o tratará de instalar software no autorizado en los equipos de BLANCO SAFI, así como ingresar a páginas Web inseguras que puedan dañar dichos equipos.
- El área de sistemas revisará periódicamente la instalación no autorizada de software en los equipos asignados a usuarios.
- En caso un usuario detecte código malicioso en un equipo, deberá informar inmediatamente a la Jefatura de sistemas para que ejecuten el procedimiento respectivo.
- Se contará con las herramientas necesarias y actualizadas que permitan la detección y eliminación de código malicioso de manera automática.
- Se contará con procedimientos que permitan la recuperación ante una contingencia causada por código malicioso.

e) Gestión de Respaldo y Recuperación.

Procedimiento de copias de respaldo de la información. (Ver control propuesto en Manual de Gestión de Riesgos para los riesgos R01, R02 y R03)

- La información procesada en los sistemas será respaldada de acuerdo a los plazos establecidos en el RPO (Punto objetivo de recuperación), el que se ha definido en 8 horas.
- En consecuencia, se efectuará 1 copias diaria de la información en modalidad incremental. Dichas copias se realizarán de manera automática y programada durante procesos nocturnos, usando para ello 1 disco duro externo.
- La copia diaria se almacenará dentro del local de la Compañía pero lejos del data centre. El lugar destinado deberá estar adecuadamente acondicionado para mantener su integridad y evitar el acceso no autorizado de este.
- Se utilizarán 5 discos para las copias diarias, uno por cada día.
- Adicionalmente se emitirán 2 copias semanales en modalidad Total, usando para ello también dos discos duros externos adicionales y diferentes de aquellos donde se almacenan las copias diarias.
- Por otro lado, una de las copias semanales se almacenará dentro del local de la Compañía pero lejos del data centre, pudiendo usarse el mismo lugar donde se mantienen una de las copias diarias. El lugar destinado deberá estar adecuadamente acondicionado par mantener su integridad y evitar el acceso no autorizado de este.
- La segunda copia semanal será almacenada en el local de una empresa de terceros, establecida a la fecha como IRON MOUNTAIN. El disco remitido a este lugar semanalmente podrá ser intercambiado con el que se mantiene en el lugar de almacenamiento interno.
- Se utilizarán 4 discos para las copias semanales, uno por cada semana.
- La información de los discos diarios se reescribirá después de un mes y la de las copias semanales después de un año.
- La información contenida en los backups será la base de datos, el código fuente del sistema Spectrum, la información del servidor de archivos y la del correo electrónico. Adicionalmente, los siguientes documentos han sido definidos como información crítica para la continuidad de las operaciones de la Compañía:
  - File del fondo,
  - File de los clientes
  - File de los partícipes
  - Manuales de operación
- Se realizará el respaldo periódico de la información crítica de BLANCO SAFI de acuerdo a la normativa respectiva.
- Toda la información contable, de impuestos y de tipo legal será conservada de acuerdo con las normas de ley vigentes.
- Los medios y procedimientos de respaldo se someterán a pruebas periódicamente para garantizar su buen funcionamiento cuanto menos una vez al mes.
- La recuperación de la información se realizará según sea necesario considerando primero la copia local y de ser nìesario la copia externa.

f) Gestión de la seguridad de red.

Controles de red

- Para la conexión de sedes y equipos remotos, se utilizarán conexiones seguras, privadas, dedicadas y/o encriptadas.
- Se establecerán cláusulas o acuerdos de Nivel de Servicio con el proveedor de servicio de red, que asegure la disponibilidad de la misma.
- La red contarán con mecanismos de detección de intrusos y de intercepción de información.
- Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la Compañía serán restringidas a la Gerencia de Operaciones.
- Las conexiones de los equipos de cómputo y comunicaciones de BLANCO SAFI se realizarán de acuerdo a la normativa respectiva, sólo por personal autorizado por la Jefatura de sistemas.

Seguridad en los servicios de red.

- La administración de las cuentas de acceso a Internet, correo electrónico y otros servicios de red, se realizarán según la normativa respectiva, por la Gerencia de Operaciones.
- Cada jefe de área determina el acceso del personal a su cargo a los servicios de red, según amerite las funciones y actividades de cada trabajador.
- Los servicios de red contará con mecanismos de detección y eliminación de código malicioso
- El correo electrónico no será utilizado para enviar cadenas de mensajes, mensajes relacionados con actividades ilegales, no éticas o no relacionados con los propósitos de la organización. Se asignará una capacidad de almacenamiento fija para cada cuenta de correo electrónico.

g) Utilización de los medios de Información.

Gestión de medios removibles

- El acceso y uso de medios removibles será según la normativa correspondiente y deberá contar con la recomendación del Jefe de Sistemas y deberá ser autorizado por el Gerente General.
- Los medios removibles serán almacenados en áreas de acceso de acuerdo al nivel de clasificación de la Información.

Eliminación de medios

- La Información almacenada en medios removibles será borrada de manera segura cuando ya no sea necesario su uso.
- La eliminación de información crítica de medios removibles, así como la eliminación de dichos medios se realizará según la normativa respectiva, asegurando que dicha información no sea recuperable.
- Se registrará la eliminación de medios removibles.

h) Intercambio de Información.

Políticas y Procedimientos para el intercambio de Información y software.

- El intercambio de información entre BLANCO SAFI y un tercero se realizará según el procedimiento establecido entre BLANCO SAFI y dicho tercero antes del inicio del intercambio.
- Todo intercambio de información con terceros se realizará sobre la base de acuerdos formales, los resultados de la evaluación de riesgos y estándares de intercambio.
- Se notificará el envío, despacho y/o recepción de información, asegurando la trazabilidad.
- Se contará con mecanismos para la detección y protección contra código malicioso que se puede encontrar en la información transmitida de forma electrónica.
- Se contará con mecanismos para proteger la información transmitida de intercepción, copiado, modificación, cambio de ruta y destrucción.
- Toda transferencia de información que implique el movimiento de dinero, sea este de manera unitaria o masiva, deberá requerir de la firma de dos funcionarios; y en el caso del uso de los sistemas bancarios se utilizará dispositivos electrónicos de seguridad (tokens). (Ver control propuesto en Manual de Gestión de Riesgos para los riesgos R15 y R18)

Medios físicos en tránsito

- Se establecerá una lista de mensajeros autorizados entre BLANCO SAFI y terceros con la que se intercambie información.
- Se comprobará la identidad de los mensajeros autorizados, tanto en la entrada a la Compañía, como en el momento de la entrega o recepción de información o medios.
- Los medios serán entregados sólo al destinatario o a un representante, dependiendo del nivel de clasificación de la información contenida.
- El medio de tránsito será suficientemente resistente para evitar los daños físicos o manipulación, de acuerdo al nivel de clasificación de la información contenida.

Seguridad en la mensajería electrónica

- Se implementará mecanismos para el bloqueo del ingreso y salida de mensajería no autorizada a la red de BLANCO SAFI.
- Los servicios de mensajería electrónica cumplirán con las regulaciones legales vigentes.
- Se asegurará el emisor, la dirección y transporte correcto del mensaje.

Sistemas de información de negocios.

- Se contará con la documentación de la interconexión de los sistemas de información de negocios.

i) Monitoreo

Registros de auditoría.

- Se contará con registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la Compañía, así como mantener pistas adecuadas de auditoría.
- Los sistemas de información contará con registros de auditoría que almacenen información sobre actividades de los usuarios, activaciones y desactivaciones de los sistemas, excepciones, alarmas y eventos de seguridad de información, los cuales serán guardados durante un periodo definido para asistir futuras investigaciones y para el monitoreo de control de acceso.

Seguimiento del uso de los sistemas.

- Se monitoreará el uso del sistema y de instalaciones de procesamiento de información, y sus resultados serán revisados periódicamente.
- Se incluirá parámetros como: accesos autorizados, trazabilidad, operaciones privilegiadas, intentos de acceso no autorizado, alertas o fallas del sistema, cambios o intentos de cambio a la configuración y controles del sistema de seguridad.
- Dicho seguimiento se considerarán de acuerdo al nivel de clasificación de la información.
- La periodicidad de las revisiones será según la criticidad de los procesos, valor de la información y experiencias anteriores.

Protección de la información de registro.

- Las instalaciones y/o sistemas de almacenamiento de registros estarán protegidas con mecanismos de acceso.
- Se detectará cualquier modificación a los archivos de registro.
- Se monitoreará periódicamente la capacidad de almacenamiento para los registros.

Registro de actividades de administradores y operadores.

- Se registrará la actividad de los administradores del sistema, identificando a las personas, hora de ingreso, motivo del uso de la cuenta de acceso y acciones realizadas.
- Las actividades diarias no se realizarán a través de cuentas con accesos privilegiados.

Registro de errores.

- La Jefatura de sistemas registrará los errores e incidentes reportados por los usuarios o registrados en el sistema, donde se especifique el escalamiento y las medidas correctivas ejecutadas.

8.6 Control de accesos

Objetivo de control: administrar el acceso lógico a los equipos informáticos, información y aplicaciones, de manera que accederán a ellos sólo a las personas autorizadas.

Descripción: cada usuario (o grupo de usuarios) contará con un identificador de usuario (o de grupo) y una contraseña conocida sólo por dicho usuario (o grupo), mediante los cuales tendrá acceso a los sistemas de información autorizados, de acuerdo al perfil asignado por la jefatura de su área.
Se verificará la estructura de las contraseñas de forma que sean seguras. Así mismo se revisarán periódicamente los permisos otorgados de manera que esté en concordancia con la función desempeñada por cada empleado.

Controles:

a) Requisitos de negocio para el control de accesos.

Política de control de accesos.

- El nivel de acceso a un sistema de información se otorgará de acuerdo a:
    - La clasificación de la información
    - Funciones del usuario
    - Perfiles de acceso estandarizados
    - Pedido, autorización y administración de acceso
    - Segregación de funciones
    - Revisión peri ódi ca
    - Retiro y modificación de derechos de acceso
- Estos parámetros deberán reflejarse en la normativa respectiva de accesos lógicos.

b) Gestión de acceso de usuario.

Registro de usuario.

- La solicitud y registro de usuarios y cuentas se realizará de acuerdo a la normativa respectiva de accesos lógicos.
- Cada usuario de los sistemas de información de BLANCO SAFI contará con:
    - Identificador o Nombre de usuario: que corresponde a la identidad de la persona y es único dentro de la red y de la aplicación.
    - Password o contraseña: que será conocido sólo por el usuario.
- En circunstancias excepcionales que se justifiquen por sus ventajas o por una función de negocio, se usará identificadores de usuario compartidos para un grupo de usuarios o un trabajo específico. En estos casos se contará con la autorización del jefe del área y tener control de qué persona está usando un identificador de grupo en un momento dado.
- La creación de cuentas de usuario será aprobado por la jefatura de área o propietario, será ejecutado por el área de sistemas.
- El identificador de un usuario eliminado no se volverá a asignar a otra persona en el futuro.
- En los casos de salida de personal, los permisos y accesos a los sistemas de información serán retirados.
- En los casos de movimiento de personal, los permisos y accesos a los sistemas de información serán cambiados, de acuerdo al nuevo rol que ejercerá el empleado.

- Toda creación, modificación o eliminación de usuarios será registrada manualmente por el área de sistemas, y en lo posible, por el log de la aplicación.

Gestión de privilegios.

- La definición y autorización de perfiles de usuarios a las aplicaciones internas de BLANCO SAFI será realizada por los jefes de las unidades orgánicas propietarias, de acuerdo a la normativa respectiva.
- La asignación de perfiles a los usuarios de las aplicaciones internas de BLANCO SAFI será ejecutada por la Unidad de Tecnologías de Información.

Gestión de contraseñas de usuario.

- La contraseña del correo es personal. Inicialmente se le otorgará una contraseña al usuario, la cual será obligatoriamente cambiada durante su primer registro.
- La contraseña cumplirán con los requerimientos de complejidad especificados:
    - La longitud será mayor a 8 caracteres,
    - La composición de la clave será compleja. Contendrá al menos una letra mayúscula, una minúscula y/o número.
- Las contraseñas guardarán un registro histórico de 6 contraseñas.
- La contraseña podrá ingresarse hasta 3 intentos fallidos, al siguiente intento fallido, ésta se bloqueará.
- Las contraseñas serán forzadas a cambiarse periódicamente cada 90 días, pudiendo considerar la criticidad de la aplicación, perfil de usuario y uso.
- La contraseña se mantendrá secreta. No será compartida con otros usuarios.
- La contraseña no será visualizada en pantalla mientras se digita.
- Aquellos usuarios que por motivos de criticidad de sus accesos cuenten con dispositivos de autenticación adicionales a la contraseña (tarjetas inteligentes, tókens u otros), tendrán la responsabilidad de mantener la confidencialidad de los mismos.
- Las contraseñas temporales o por defecto serán enviadas a los usuarios de manera segura, y serán cambiadas inmediatamente por los mismos una vez recibidas y verificadas.

Revisión de los derechos de acceso de los usuarios.

- Se realizará revisiones periódicas sobre los derechos de acceso concedidos a los usuarios, acorde con el movimiento de personal y los cambios en la organización. Esta revisión será coordinada entre el Oficial de Seguridad y la jefatura del área del usuario. (Ver control propuesto en Manual de Gestión de Riesgos para el riesgo R20)
- Se revisará con mayor frecuencia los accesos de los usuarios con privilegios especiales.
- Se registrará todas las revisiones y cambios en las cuentas de usuario.

c) Responsabilidad del usuario.

Uso de contraseñas.

- Los usuarios a los que se les asigna un identificador, preservarán la confidencialidad de la contraseña asociada a dicho identificador. Ningún usuario utilizará el identificador de otro usuario.
- Se evitará el registro por escrito de las contraseñas.
- Los usuarios cambiarán sus contraseñas asignadas en caso tengan sospecha de su conocimiento por parte de otra persona, y notificarán del hecho al Oficial de Seguridad.
- Los usuarios seleccionarán contraseñas seguras, que no sean fácilmente deducibles.
- No se incluirá las contraseñas en ningún mecanismo automático de conexión que las deje almacenadas en el equipo.

Equipo informático de usuario desatendido.

- Al dejar un equipo desatendido temporalmente, el usuario debe bloquear el acceso a su PC.
- Al terminar la jornada de trabajo o ausentarse de la oficina por un periodo prolongado de tiempo, se cancelará las sesiones de usuario dentro de las aplicaciones, además de bloquear la pantalla.
- Se cerrará la sesión de administrador u operativo de los servidores cuando se ha concluido con la labor.

Política de pantalla y escritorio limpio

- La información crítica impresa o almacenada de manera electrónica estará protegida de accesos no autorizados, especialmente cuando no estén en uso.
- La información impresa a eliminar será desechada de manera segura y que no permita su reconstrucción total o parcial.
- Las terminales de usuario contarán con mecanismos de bloqueo de pantalla automáticos y a voluntad. En caso de inoperatividad en el equipo, este se bloqueará en un lapso de 15 minutos.
- El acceso a scanner, fotocopiadoras u otros será bloqueado cuando se encuentren desatendidos.

d) Control de acceso en red.

Uso de los servicios de red.

- Los perfiles de acceso y normativas de acceso lógico considerará los servicios de red y conexiones a las redes a los que un usuario puede tener acceso.
- Se considerará la verificación de los medios usados para el acceso a los servicios de red.
- Se contará con dispositivos adicionales de conexión a internet. (Ver control propuesto en Manual de Gestión de Riesgos para el riesgo R05)

Autenticación de usuario para conexiones externas.

- Se implementará mecanismos de identificación de un usuario que se conecta remotamente a la red de la organización, así como la identificación del punto de conexión remota.

Identificación de equipos en la red.

- Se contará con identificadores de los equipos que se conectan a la red. Estos identificadores serán asignados según la normativa respectiva.
- Se identificará qué redes o segmentos de red se pueden contar los equipos remotos.

Segregación de las redes.

- Se implementará dominios o grupos de red necesarios para controlar los accesos lógicos a la red y flujos de información, teniendo en cuenta el impacto en el rendimiento de la red.

Control de encaminamiento en la red.

- Se implementará control de ruteo de redes para asegurar que las conexiones y los flujos de información entre computadores no violen las políticas de control de acceso de las aplicaciones de negocio.

e) Control de acceso al sistema operativo.

Procedimiento de conexión segura.

- Para la conexión de equipos a la red se considerará:
  - Limitar y registrar el número de intentos fallidos de conexión, luego de lo cual el usuario quedará deshabilitado por un periodo de tiempo.
  - Limitar el tiempo de la conexión, luego del cual el usuario se autenticará nuevamente.

Identificación y autenticación de usuario.

- Los usuarios contarán con un identificador de usuario único en una aplicación, con la que se permita hacer seguimiento de sus actividades.
- Las actividades regulares de un usuario no serán realizadas desde cuentas privilegiadas.

Sistema de Gestión de contraseñas.

- El sistema o módulo de gestión de contraseñas permitirá la configuración y verificación automática de los controles establecidos en los acápites anteriores (Gestión de contraseña de usuario y Uso de contraseñas).

Uso de las facilidades del sistema.

- Se restringirá el uso de las facilidades del sistema separados del acceso a las aplicaciones.
- El acceso a las facilidades del sistema será para propósitos específicos, limitado al mínimo número de usuarios.
- El acceso a las facilidades del sistema será por perfiles.

Desconexión automática de sesiones.

- Los sistemas de información, según su criticidad y uso, desconectarán automáticamente las sesiones de conexión tras un periodo definido de inactividad que sea configurable por cada sistema.

f) Control de acceso a información y aplicaciones.

Restricción de acceso a la información.

- Se asegurará que las salidas de los sistemas de información se envíen únicamente a los terminales autorizados.
- En la generación de perfiles, se controlará los derechos de acceso a lectura, escritura, borrado y ejecución.

Aislamiento de sistemas sensibles.

- Los sistemas de información críticos estará conectados en ambientes, entornos informáticos y/o segmentos de red aislados.
- Cuando el sistema de información crítico se ejecute en entornos compartidos, se identificará los sistemas con los que compartan recursos y será validado por el propietario de la información.

g) Informática Móvil y Teletrabajo

Informática móvil

- El ingreso, salida y uso de equipos de informática móvil se realizará según la normativa respectiva y de manera autorizada por la gerencia respectiva.

Teletrabajo

- El teletrabajo se realizará vía conexiones seguras a la red de la organización.
- Los equipos utilizados para realizar el teletrabajo contará como mínimo con las mismas medidas de identificación, instalación de software y protección contra código malicioso que los equipos que se encuentran en las instalaciones de la organización.

8.7 Adquisición, desarrollo y mantenimiento de sistemas

Objetivo de control: brindar un adecuado nivel de seguridad de información a los sistemas y aplicaciones, desde su desarrollo y durante todo su ciclo de vida.

Descripción: se contará con un procedimiento para la adquisición, desarrollo y mantenimiento de sistemas que considere: validación y acceso al código fuente, validación datos de entrada y salida, procesamiento, registros de auditoría, documentación, reportes, pruebas y pase a producción.
En casos de adquisición de software, se establecerá niveles de servicio así como el alineamiento a las normativas de Desarrollo y Mantenimiento de Sistemas respectivas.

Controles:

a) Requisitos de seguridad de los sistemas de información.

Análisis y especificación de los requisitos de seguridad.

- La especificación de requerimientos de seguridad para sistemas de información nuevos (adquiridos o desarrollados internamente), se considerará:
    - Lenguaje que seár utilizado, vigente y soporte actualizado
    - Controles para el ingreso y actualización de la información
    - Control de accesos
    - Registros de Auditoría
    - Rutinas que se deben tomar en cuenta
    - Pautas para las pantallas y reportes
    - Separación de ambientes de desarrollo, pruebas y producción

b) Seguridad de las aplicaciones del sistema

Validación de los datos de entrada.

- Se aplicará controles y mejores prácticas de validación de los datos de entrada de las transacciones, datos de referencia y tablas de parámetros, que permitan identificar: valores fuera de rango, caracteres inválidos, datos incompletos o inconsistentes.
- Los sistemas comprobará la integridad de los datos de entrada, especialmente aquellos que interactúan con información crítica.

Control del procesamiento interno.

- Se contará con procedimientos y/o mecanismos de comprobación para detectar cualquier tipo de corrupción de información por consecuencia de errores del proceso o por actos deliberados.
- Se implementará restricciones que minimicen el riesgo de fallas en los sistemas de información, que permitan su recuperación y que impida su ejecución hasta la resolución del problema.
- Se implementará controles de sesión, comprobación de cuadres y ejecución ordenada de programas.

Validación de los datos de salida.

- Se contará con un procedimiento de validación de datos de salida que verifique que la información generada es correcta y apropiada.
- El sistema generará información suficiente para determinar la exactitud, completitud y precisión de los datos de salida.
- Se implementará un reporte que considere el cuadre diario de depósito en el Fondo por cuenta. (Ver control propuesto en Manual de Gestión de Riesgos para el riesgo R09)

c) Seguridad de los archivos del sistema.

Control del software en producción

- El pase a producción, configuración de cambios de los sistemas y código fuente, lo realizará personal autorizado (encargado del sistema Spectrum), según la normativa respectiva, con conocimiento del Jefe de Sistemas.
- Las pruebas para el pase de un programa a producción será planeadas, ejecutadas, documentadas y controlados sus resultados, para garantizar la

integridad de la Información en producción. Estas pruebas se realizará en un ambiente distinto al de producción.
- Se mantenerá un registro de todos los cambios realizados en el sistema.
- Se almacenará las versiones de los sistemas anteriores a un cambio hasta que se compruebe que el cambio ha sido exitoso.

Protección de los datos de prueba del sistema.
- Se implementará como mínimo los mismos controles de acceso de los sistemas en producción, a los sistemas en prueba.
- Se borrará la información operativa del sistema en prueba en cuanto esta se complete.
- Se registrará la copia y uso de la información de pruebas.

Control de acceso al código fuente de los programas.
- Se restringirá el acceso al código fuente, limitado sólo a personal autorizado del área de Desarrollo, de acuerdo a la normativa respectiva.
- Se registrará los accesos y modificaciones al código fuente.

d) Seguridad en los procesos de desarrollo y soporte.

Procedimientos de control de cambios.
- Se contará con un formato para la solicitud, aprobación y prueba del cambio que considere:
  - Clasificación del cambio según su alcance y su urgencia considerando aquellos que correspondan a:
    (1) Cambios por fallas inesperadas del aplicativo
    (2) Cambios por requerimientos legales
    (3) Cambios por mejoras funcionales
    (4) Cambios por la implementación de un nuevo sistema
  - Autorización para los cambios del sistema, según el proceso al que impacta.
  - Registro de todos los cambios y su autorización
  - Pruebas del cambio por parte del solicitante.
  - Aceptación de los cambios por parte del solicitante
  - Actualización de la documentación del sistema
  - Control de versiones
- Se asegurará que los cambios a aplicar no comprometan los controles de seguridad de información ya implementados.
- Los cambios será planificados para no afectar la operatividad del sistema.
- Se establecerá un procedimiento de cambios en situaciones de emergencia no requieran todos los controles establecidos en situaciones normales.

Revisión técnica de los cambios en el sistema operativo.
- Se revisará y probará los módulos o programas que han sido materia de cambios, para asegurar que no afectan al funcionamiento o seguridad del sistema operativo.
- Se garantizará la asignación de recursos para revisiones, mantenimientos, pruebas y cambios en el sistema operativo.

Restricciones en los cambios a los paquetes de software.

- Se limitará los cambios a los paquetes de software proporcionados por proveedores tecnológicos, de manera que no debilite su estructura y no genere un gran impacto para la Compañía por el mantenimiento de dicho software.
- Se considerará en la planificación, la adquisición de las actualizaciones de software de proveedores tecnológicos.

Fuga de información.

- Se implementará mecanismos para evitar la fuga de información, tales como:
  - Escaneo de medios de salida y comunicaciones
  - Monitoreo regular de las actividades del personal y del sistema, que sea permitido por la ley.
  - Monitoreo del uso de recursos informáticos.

Desarrollo externo del software.

- El desarrollo de software por proveedores tecnológicos cumplirá con las normativas relacionadas al desarrollo y mantenimiento de sistemas de información y todos los controles asociados.
- Al recibir el sistema terminado, el área de sistemas junto con la unidad usuaria realizará todas las pruebas, bajo los mismos procedimientos establecidos para el desarrollo interno, a fin de certificar la calidad, seguridad y exactitud del trabajo realizado.
- Se considerará en el contrato acuerdos de licenciamiento, propiedad del código, derechos de propiedad intelectual y servicio de soporte y mantenimiento.

e) Gestión de vulnerabilidades técnicas.

Control de vulnerabilidades técnicas.

- Se contará con conocimiento y mantenerse actualizado de las vulnerabili dades técnicas de los sistemas utilizados que permita identificar los riesgos asociados y tomar acciones preventivas.
- Los parches serán evaluados en su desempeño en el mercado antes de que sean instalados a fin de asegurar que sean efectivos y no causen efectos secundarios contraproducentes.
- Se monitoreará y evaluará la gestión de las vulnerabilidades técnicas para asegurar su efectividad y eficiencia.

8.8 Gestión de incidentes

Objetivo de control: asegurar que los incidentes y debilidades de seguridad de información sean detectados y comunicados de manera correcta y oportuna, que permita que se realice una acción correctiva y adecuada a tiempo.
Descripción: se contará con procedimientos formales y conocidos para el reporte de incidentes o fallas en la seguridad que puedan ser detectados por usuarios del

sistema. Así mismo se contará con mecanismos automáticos centralizados de detección de eventos en la red y sistemas de información.
Todos los eventos serán registrados y corregidos mediante procedimientos formales de cambios.

Controles:
a) Comunicación de eventos y debilidades de seguridad de la información.

Comunicación de eventos de seguridad de la información.

- Los eventos de seguridad de información se reportarán oportunamente al Oficial de Seguridad, según las normativas de gestión de incidencias, sin afectar esto a los procesos de reporte de eventos de riesgo operativo y de pérdida normadas por la organización.
- Cuando sea necesario, se guardará evidencia del evento, para poder investigar las causas del mismo.
- Los empleados o proveedores que generen un evento de seguridad de información de manera intencional o accidental, será considerado como falta que podrá ser sancionada según el RIT.

Comunicación de debilidades de seguridad.

- Las debilidades de seguridad de información se reportarán oportunamente al Oficial de Seguridad.
- Ningún empleado o proveedor tratará de probar o explotar una vulnerabilidad, lo cual será considerado como falta que podrá ser sancionada según los criterios de BLANCO SAFI.

b) Gestión de incidencias y mejoras de la seguridad de la información.

Responsabilidades y procedimientos.

- Los sistemas de información contarán con registros de eventos de seguridad, y en lo posible generar alertas.
- Se llevará un registro de incidencias de falla de software. (Ver control propuesto en Manual de Gestión de Riesgos para el riesgo R06)
- Se identificará a los responsables de responder a eventos y/o incidencias de seguridad de información.
- Se considerará para la solución de un evento y/o incidencias: planes de contingencia, análisis de causa, contención, acciones correctivas, reporte a la gerencia, registros de auditoría.
- Todas las medidas correctivas y acciones de emergencia serán documentadas y realizadas sólo por personal autorizado.

Aprendiendo de las incidencias de seguridad de la información.

- Se almacenará la información relacionada a los tipos, causas, costos y soluciones de los incidentes de seguridad de información que sirva para la resolución de futuros eventos.

Recolección de evidencia

- Cuando una acción de seguimiento contra una persona u organización, después de un incidente de seguridad de información, implique acción legal, la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante. Para ello los sistemas críticos cumplirán con cualquier estándar o código para la producción de evidencia admisible.
- El acceso a evidencia informática será solo por personal autorizado de la Gerencia de operaciones y el representante de la empresa Digital Dynamics S.A.

8.9 Gestión de continuidad del negocio

Objetivo de control: contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Descripción: se implementará un proceso de gestión de continuidad del negocio para reducir a niveles aceptables, la interrupción causada por desastres o fallas en los procesos críticos, a través de controles preventivos, procedimientos de respaldo, de contingencia y de recuperación.

Controles:
a) Aspectos de la gestión de continuidad del negocio.

- Inclusión de la seguridad de la información en el proceso de la gestión de continuidad del negocio.
- Se contará con un plan de continuidad del negocio por cada sistema de información que considere:
  - Identificación de vulnerabilidades, riesgos e impacto, priorizando los procesos críticos de negocio.
  - Identificación de activos implicados en los procesos críticos del negocio
  - Asignación de recursos financieros, humanos, técnicos y ambientales
  - Adquisición de seguros adecuados
  - Asignación de responsabilidades
  - Mantenimiento del plan

  Los detalles de este procedimiento se pueden consultar en el Plan de Continuidad de Negocios de BLANCO SAFI.

Continuidad del negocio y evaluación de riesgos.
- Se identificará los eventos que pueden causar interrupciones a los procesos de negocio, su probabilidad e impacto para la organización y para la seguridad de información.
- El plan de continuidad de negocio será implementado de acuerdo a los resultados de la evaluación de riesgos y a los eventos identificados.

Redacción e implantación de planes de continuidad que incluyan la seguridad de la información.

- Se contará con planes de mantenimiento y recuperación de las operaciones para asegurar la disponibilidad de la información al nivel y en las escalas de tiempo requeridas, tras la interrupción y falla de sus procesos críticos.
- Se considerará los siguientes aspectos:
  - Identificación de procedimientos de emergencia y acuerdos de responsabilidades.
  - Identificación de pérdidas aceptables de información y servicios.
  - Procedimientos documentados de recuperación y restauración de operaciones.

  Los detalles de este procedimiento se pueden consultar en el Plan de Continuidad de Negocios de BLANCO SAFI.

Marco de planificación para la continuidad del negocio.

- Se tenerá esquemas únicos para la definición de planes de cont inuidad, que considere el alcance, condiciones de activación, responsables de ejecución, propietario.
- Se contará con:
  - Procedimientos de respaldo y restauración, que permita mantener la información disponible en otra localización en caso de contingencia.
  - Procedimientos de contingencia que describan las acciones a realizar tras una contingencia que amenace las operaciones del negocio, para desplazar de forma temporal a lugares alternativos las actividades principales del negocio
  - Procedimientos temporales de operación y reanudación de operaciones.

Prueba, mantenimiento y reevaluación de planes de continuidad.

- Se probará los planes de continuidad periódicamente para asegurarse de su actualización y eficada, asegurando que dichos planes indiquen cómo y cuando probar cada elemento del plan.
- Se contará con varios escenarios y simulaciones para la ejecución de las pruebas, las cuales serán orgnizadas y ejecutadas por la brigada de emergencia y el equipo continuidad de negocio. (Ver control propuesto en Manual de Gesti ón de Riesgos para el riesgo R02)
- Se realizará pruebas de continuidad de los servicios y recursos de los proveedores tecnológicos.

Los detalles de este procedimiento se pueden consultar en el Plan de Continuidad de Negocios de BLANCO SAFI.

8.10 Cumplimiento

Objetivo de control: impedir infracciones y violaciones de las leyes del derecho civil y penal, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad de información.

Descripción: se definirá, documentará y buscará asesoría de órganos especializados y/o de control, sobre los requisitos legales, regulatorios y contractuales que deben ser considerados en la implementación de controles de seguridad de información.

Controles:
a) Conformidad con los requisitos legales

Identificación de la legislación aplicable.

- Se definirá, documentará, cumplirá y mantendrá de forma documentada, todos los requisitos legales, regulatorios y contractuales para los sistemas de información de BLANCO SAFI.
- Es responsabilidad de la Unidad Legal, mantener informada a la Comisión de Seguridad de Información sobre cualquier regulación aplicable a seguridad de información que afecte a la organización.

Derechos de Propiedad Intelectual (DPI)

- Se contará con cláusulas de cumplimiento de restricciones legales, reguladoras y contractuales sobre el uso de material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario, especificados en los contratos con BLANCO SAFI.
- La instalación de software no autorizado será considerado como falta y será sancionado según RIT.

Protección de los registros de la organización.

- Se protegerá los registros de la organización frente a su pérdida, destrucción y falsificación, en concordancia con los requisitos legales, regulatorios y contractuales.
- Se incluirá una alerta dentro de la base de datos del sistema que permitirá identificar si los clientes o potenciales clientes se encuentran registrados en las listas negras internacionales. (Ver control propuesto en Manual de Gestión de Riesgos para el riesgo R08)

Protección de datos de carácter personal y de la intimidad de las personas.

- Se contará con cláusulas de privacidad y de protección de datos en los contratos con BLANCO SAFI, de acuerdo con la legislación vigente.

Prevención en el mal uso de los recursos de tratamiento de la información.

- Se implementará mecanismos para controlar que los recursos informáticos sean utilizados sólo para fines del negocio autorizados.

- El personal con acceso a recursos de tratamiento de información, harán uso de los mismos siguiendo lo especificado en las normativas de uso adecuado de activos de información.

b) Conformidad con políticas y normas de seguridad y conformidad técnica.

Conformidad con políticas y normas de seguridad.

- Los jefes de las unidades orgánicas se asegurarán que se cumplan correctamente todos las normativas de seguridad de información en su área de responsabilidad, e informar oportunamente al área de sistemas y Jefe de Personal en caso de no cumplimiento.

Comprobación de la conformidad técnica.

- El área de Sistemas comprobará la conformidad técnica de los sistemas de información con las normas de seguridad de información, ya sea manual o automáticamente.

9. Elaboración, validación, aprobación y vigencia

El presente Plan de Seguridad de la Información ha sido elaborado en concordancia con la Gerencia de Riesgos, la Gerencia de Operaciones, la Gerencia Comercial y de Negocios, la Unidad Legal y el área de Sistemas. Ha sido aprobada por la Gerencia General y el Directorio. Está en vigencia desde el día siguiente de su publicación.

10. Anexos

Anexo 1.

BDO

BLANCO SAFI - MATRIZ DE RIESGOS OPERACIONALES

N°	PROCESO	SUBPROCESO	ACTIVO	CRITICIDAD	RTO	RPO	TIPO DE RIESGO	TIPO DE EVENTO	AMENAZA	PROBABILIDAD	IMPACTO	VALORIZACIÓN	CONTROL	RIESGO INHERENTE	CONTROL PROPUESTO	RIESGO RESIDUAL ESPERADO
R01	Estructuración e inscripción de un Fondo	Elabora reglamento de Participación	Reglamento de Participación	B	NA	NA	Administrativo	Daño Físico	Incendio / Corto circuito	Bajo	Interrupción de la operación por pérdida de la información	Medio	No definido	Medio	Extintores y Copia legalizada almacenada en lugar externo	Bajo
R02		Elabora contratos para Inversionistas de Fondo	Contratos					Daño Físico	Terremoto	Bajo	Interrupción de la operación por pérdida de la información	Medio	No definido	Medio	Simulacros y Copia legalizada almacenada en lugar externo	Bajo
R03		Envía información sobre el Fondo a la SMV, a fin de inscribirlo en el Registro Público del Mercado de Valores	Información sobre Fondo Público					Daño Físico	Inundación	Bajo	Interrupción de la operación por pérdida de la información	Medio	No definido	Medio	Revisión periódica de instalaciones y Copia legalizada almacenada en lugar externo	Bajo
R04		Registro de Fondo ante SUNAT (RUC) y apertura de cuentas corrientes y libros contables	Información sobre Fondo Público	B	NA	NA	Legal	Error en el proceso	Incumplimiento legal	Bajo	Multa de los entes reguladores por ausencia de información	Alto	Seguimiento de cumplimiento de fechas establecidas	Medio	Documentación	Bajo
R05					<=4	NA	Tecnológico	Fallas del sistema	Interrupción del sistema por falla en la conexión de internet	Bajo	Imposibilidad de registrar el Fondo Público	Bajo	No definido	Bajo	Contar con dispositivo adicional de conexión	Bajo
R06		Crear Fondo en el sistema de Fondos	Sistema de Fondos Spectrum / Información sobre Fondo	B	<=4	NA	Tecnológico	Fallas del sistema	Interrupción del sistema por falla o error en el software	Bajo	Interrupción en la gestión del Fondo	Bajo	No definido	Bajo	Registro de incidencias de fallas del software	Bajo
R07		Publicación de Fondo	Información sobre Fondo Publico	B	NA	NA	Administrativo	Error en el proceso	Error administrativo	Bajo	Retraso en el proceso	Medio	Revisión por parte de la Gerencia Inversiones	Medio	NA	Bajo

BDO

BLANCO SAFI - MATRIZ DE RIESGOS OPERACIONALES

N°	PROCESO	SUBPROCESO	ACTIVO	CRITICIDAD	RTO	RPO	TIPO DE RIESGO	TIPO DE EVENTO	AMENAZA	PROBABILIDAD	IMPACTO	VALORIZACIÓN	CONTROL	RIESGO INHERENTE	CONTROL PROPUESTO	RIESGO RESIDUAL ESPERADO
R08	Colocación del Fondo (Captura de partícipes)	Entregar los números de cuenta a cada partícipe para realizar los aportes	Información sobre Fondo Publico	B	NA	NA	Administrativo	Fraude interno	Interrupción en el proceso por fraude	Bajo	Abono en número de cuenta errado	Alto	Cuadre diario de depósito en el Fondo por cuenta	Medio	Incluir en el contrato de suscripción, los números de cuenta	Bajo
R09		Registro del partícipe (Contrato de suscripción)	Contrato de suscripción de partícipe	B	<=4	NA	Administrativo	Error en el proceso	Error administrativo	Bajo	Información de las condiciones de contrato errada	Medio	Revisión por parte de la Gerencia Inversiones	Medio	NA	Bajo
R10		Solicitar al partícipe, información relacionada a PLAFT	Información de partícipe	B	NA	NA	Legal	Fraude externo	Interrupción en el proceso por fraude	Bajo	Pérdida de imagen corporativa	Alto	Revisión a cargo del Oficial de Cumplimiento y Ejecutivo de Inversiones	Medio	Implementar alertas detectivas en el sistema, en base a listas negras	Bajo
R11		Registro del partícipe y su aporte en el sistema	Sistema de Fondos Spectrum / Certificado de	C	<=4	<=8	Tecnológico	Fallas del sistema	Interrupción del sistema por falla o error en el software	Bajo	Interrupción en la gestión del Fondo	Medio	No definido	Medio	Gestión manual y emisión manual del certificado durante 1 semana	Bajo
R12	Inversiones y comité de inversiones	Revisar información financiera del cliente	Información de cliente	A	<=4	<=8	Tecnológico	Fallas del sistema	Interrupción del sistema por falla o error en el software	Medio	Indisponibilidad de la información crediticia del cliente (Sentinel)	Medio	Verificación manual	Medio	NA	Bajo
R13		Evaluar situación crediticia del cliente	Resultados de evaluación de cliente	A	NA	NA	Administrativo	Error en el proceso	Interrupción en el proceso por fraude	Bajo	Resultados errados de la evaluación de cliente	Medio	Verificación manual pos-desembolso, Seguro crediticio y Proceso de Compliance	Medio	NA	Bajo
R14		Elaborar contrato para cliente	Contrato de inversión	A	NA	NA	Administrativo	Error en el proceso	Error administrativo	Bajo	Condiciones erradas en el Contrato	Medio	Revisión por parte de la Gerencia Legal	Medio	NA	Bajo
R15					NA	NA	Administrativo	Fraude interno	Interrupción en el proceso por fraude	Bajo	Desembolso en número de cuenta errado	Alto	Dos firmas (Gerencia de Operaciones y Gerencia de Finanzas)	Medio	NA	Bajo

BDO

BLANCO SAFI - MATRIZ DE RIESGOS OPERACIONALES

N°	PROCESO	SUBPROCESO	ACTIVO	CRITICIDAD	RTO	RPO	TIPO DE RIESGO	TIPO DE EVENTO	AMENAZA	PROBABILIDAD	IMPACTO	VALORIZACIÓN	CONTROL	RIESGO INHERENTE	CONTROL PROPUESTO	RIESGO RESIDUAL ESPERADO
R16	Desembolso	Ejecuta proceso de desembolso	Desembolso de recursos del Fondo	A	NA	NA	Tecnológico	Fraude interno	Interrupción en el proceso por fraude	Bajo	Transferencia del recurso del fondo en número de cuenta errado	Alto	Dos firmas (Gerencia de Operaciones y Gerencia de Finanzas)	Bajo	NA	Bajo
R17					NA	NA	Legal	Fraude Externo	Interrupción en el proceso por fraude	Bajo	Información del fondo errada	Alto	Verificación Legal (Control de sesión Notarial y Firma de pagaré en blanco)	Bajo	NA	Bajo
R18		Registra operaciones de desembolso en sistema de Fondos	Sistema de Fondos Spectrum	C	<=4	NA	Administrativo	Error en el proceso	Error administrativo	Bajo	Registro errado de la operación	Medio	Verificación manual del Jefe de Operaciones y Gerencia de Finanzas	Medio	NA	Bajo
R19					<=4	<=8	Tecnológico	Fallas del sistema	Interrupción del sistema por falla o error en el software	Bajo	Interrupción en la gestión del Fondo	Medio	No definido	Medio	Gestión manual	Bajo
R20	Pago a Partícipes	Pago de intereses a las cuentas de los partícipes	Información de partícipe	A	NA	NA	Administrativo	Fraude interno	Interrupción en el proceso por fraude	Bajo	Abono en número de cuenta errado	Alto	Verificación manual	Medio	Cuadre mensual o trimestral de los abonos	Bajo
R21					<=4	<=8	Tecnológico	Fallas del sistema	Interrupción del sistema por falla o error en el cálculo de intereses	Bajo	Interrupción en la gestión del Fondo	Medio	No definido	Medio	Gestión manual	Bajo
R22	Valorización de las cuotas	Ejecutar proceso de valorización de la cuota	Sistema de Fondos Spectrum / Valor cuota	C	<=4	<=8	Tecnológico	Fallas del sistema	Interrupción del sistema por falla o error en el cálculo de la cuota	Medio	Cálculo errado en el valor de la cuota	Alto	Verificación manual	Alto	Revisión periódica de funciones críticas dentro del software	Bajo

LEYENDA

CRITICIDAD	
A	Imprescindible para la Gestión de Riesgos
B	Necesario
C	Importante. Se requiere pero puede someterse a las reglas del RTO y RPO

PROBABILIDAD	
Alto	1 vez al mes
Medio	1 vez cada 6 meses
Bajo	1 vez al año

VALORIZACIÓN DEL IMPACTO	
Alto	> 2 días laborables. Pérdida económica de S/ 27,000
Medio	<= 2 días laborables. Pérdida económica de S/ 10,800
Bajo	<= 05 días laborables. Pérdida económica de S/ 2,700