[2] ANEXO 13

Indicadores de seguridad de la información

El oficial en jefe de seguridad de la información de la institución de financiamiento colectivo, en relación con los indicadores de riesgo en materia de seguridad de la información a que se refiere la fracción XI del artículo 66, de las presentes disposiciones, deberá:

1. Evaluar dichos indicadores, los cuales deberán ajustarse a los umbrales contenidos en este anexo para cada indicador. En caso de definir umbrales diferentes, deberá documentar el motivo.
2. Definir planes de remediación para aquellos riesgos en los que los resultados de la evaluación arrojen valores que se encuentren dentro de los umbrales medios y altos de riesgo establecidos en el presente anexo o, en su caso, aquellos definidos por la institución de financiamiento colectivo, siempre que estos se encuentren en un umbral alto por, al menos, dos periodos consecutivos.
3. Dar mantenimiento continuo, ya sea para agregar, eliminar o actualizar los indicadores claves de riesgo y de desempeño de seguridad de la información ya existentes, los cuales siempre deberán estar alineados a la estrategia de la institución de financiamiento colectivo y al Plan Director de Seguridad de la información de esta.
4. Medir y evaluar su evolución con la periodicidad indicada en las siguientes tablas, o antes en caso de eventos inusuales.
5. En caso de que no apliquen todos los supuestos, indicar que no son aplicables y explicar el motivo.

Tipo	Definición	Sub Tipo	Sub Clase de Eventos	Ejemplos
I. Fraude Interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente, o bien, soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la Institución de Tecnología Financiera.	1.1 Actividades no autorizadas.	1.1.1 Operaciones no reveladas (intencionalmente). 1.1.2 Operaciones no autorizadas (con pérdidas pecuniarias). 1.1.3 Valoración errónea de posiciones (intencional).	Operaciones no comunicadas; operaciones no autorizadas (con pérdidas pecuniarias); valoración errónea de posiciones, y omisión intencional de normativa.
		1.2 Robo y Fraude Internos.	1.2.1 Fraude / depósitos sin valor. 1.2.2 Extorsión / malversación / robo. 1.2.3 Apropiación indebida de activos. 1.2.4 Destrucción dolosa de activos. 1.2.5 Falsificación Interna. 1.2.6 Contrabando 1.2.7 Apropiación de cuentas, de identidad, entre otros. 1.2.8 Incumplimiento / evasión de impuestos (intencional) 1.2.9 Cohecho. 1.2.10 Abuso de información privilegiada (no a favor de la empresa).	Robo; malversación; apropiación indebida; destrucción de activos; falsificaciones; suplantación de identidad; y cohechos; manipulación de cuentas.
		1.3. Seguridad de los sistemas.	1.3.1 Vulneración de sistemas de seguridad. 1.3.2 Daños por ataques informáticos. 1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	Abuso y utilización de información privilegiada o confidencial; alteración de aplicaciones informáticas; robo de contraseñas, y accesos informáticos prohibidos.
II. Fraude Externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	2.1 Hurto y Fraude Externos.	2.1.1 Robo / estafa / extorsión /cohecho. 2.1.2 Falsificación Externa / Suplantación de personalidad. 2.1.3 Uso y/o divulgación de información privilegiada. 2.1.4 Espionaje industrial. 2.1.5 Contrabando.	Documentaciones falsificadas o manipuladas (transferencias, etc.); suplantación de identidad; disposiciones indebidas; monedas falsas; billetes deteriorados o fuera de curso legal; robos en las instalaciones de la IFC, y uso indebido de tarjetas robadas o falsificadas .
		2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 2.2.2 Daños por ataques informáticos. 2.2.3 Robo de información (con pérdidas pecuniarias). 2.2.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	Acceso informático no autorizado; manipulación de aplicaciones informáticas; daños por ataques informáticos, y robo de información.
VI. Incidencias en el Negocio y Fallos en los Sistemas	Pérdidas derivadas de incidencias en el negocio y de fallas en los sistemas.	6.1 Sistemas	6.1.1 Hardware. 6.1.2 Software. 6.1.3 Telecomunicaciones. 6.1.4 Interrupción / incidencias en el suministro.	Interrupción / incidencias en los suministros y líneas de comunicación; errores en los programas informáticos; fallos en hardware y software; sabotajes; interrupciones del negocio;

Tipo	Definición	Sub Tipo	Sub Clase de Eventos	Ejemplos
				fallos informáticos y programación de virus.

ID	Nombre	Descripción	Dominio	Tipo	Sub Tipo	Sub Clase de Eventos	Tipo de Indicador	Periodo	Unidad de Medi-ción	Cálculo	Variable X	Variable Y	Riesgo Alto	Riesgo Medio	Riesgo Bajo
KRI0001	Incidentes mediante ataques directos contra los sistemas internos.	Número de incidentes que hayan sido originados por ataques hacia los sistemas internos de la Institución de Tecnología Financiera, en el periodo establecido.	Ataques lógicos.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Trimestral.	Cantidad.	Variable X	Número de casos de incidentes identificados.	-	Más de 1.	Igual a 1.	Igual a 0.
KRI0002	Casos de fraude en la plataforma.	Porcentaje de casos donde se identifica un fraude, que haya sido originado por ataques hacia la Plataforma. .	Ataques lógicos.	II. Fraude Externo	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100	Número de casos de fraude en la Plataforma.	Número de Clientes que usan la Plataforma.	Más del .01 %.	Entre el 0.005 % y el 0.01 %.	
KRI0003	Equipos de la Infraestructura Tecnológica de los que se gestiona su configuración de seguridad.	Porcentaje de equipos de Infraestructura Tecnológica dentro de la Plataforma y/o proceso de revisión de estándares de configuración segura, con respecto al total de los equipos de la IFC durante el periodo establecido.	Cumplimiento.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Mensual.	Porcentual.	(X/Y)*100	Número de equipos dentro de la plataforma o proceso de revisión de estándares de configuración segura.	Número total de equipos.	Menos del 85 %.	Entre 85 % y 95 %.	Más de 95 %.
KRI0004	Nivel de cumplimiento de configuración segura de servidores de los que se gestiona su configuración.	Porcentaje promedio de nivel de cumplimiento de servidores contemplados dentro de la herramienta y/o proceso de revisión de estándares de configuración segura.	Cumplimiento.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Mensual.	Promedio porcentual.	Promedio(X)	% de cumplimiento del estándar de configuración segura de cada uno de los Servidores.	-	Menos del 90 %.	Entre 90 % y 95 %.	Más de 95 %.
KRI0005	Usuarios con roles y perfiles inadecuados.	Porcentaje de usuarios con perfiles inadecuados dentro de las aplicaciones de la IFC, con respecto al total de usuarios en todas las aplicaciones de la Institución de Tecnología Financiera.	Cumplimiento.	I. Fraude Interno	1.3. Seguridad de los sistemas.	1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	Correctivo.	Semestral.	Porcentual.	(X/Y)*100	Número de usuarios con perfiles incorrectos, considerando todas las aplicaciones.	Número total de usuarios considerando todas las aplicaciones.	Más del 3 %.	Entre 1% y 3 %.	Menos del 1 %.
KRI0006	Aplicaciones sin roles y perfiles.	Porcentaje de aplicaciones las cuales no poseen la capacidad ni el perfilamiento de roles	Cumplimiento.	I. Fraude Interno.	1.3. Seguridad de los sistemas.	1.3.3 Robo de información (con pérdidas pecuniarias).	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de aplicaciones sin capacidad de	Número total de aplicaciones.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.

		y permisos, o que dichos perfiles no están implementados, esto con respecto al total de aplicaciones.				1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización					perfilamiento, o perfilamiento no implementado.				
KRI0007	Incidentes de seguridad de la información en general	Número total de incidentes reportados durante el periodo establecido referentes a seguridad de la información.	Información.	Aplica a: I. Fraude Interno II. Fraude Externo VI. Incidencias en el Negocio y Fallos en los Sistemas.	Aplican a: 1.3. Seguridad de los sistemas 2.2 Seguridad de los Sistemas. 6.1 Sistemas.	Aplican a: 1.3.1 Vulneración de sistemas de seguridad 1.3.2 Daños por ataques informáticos. 1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización. 2.2.1 Vulneración de sistemas de seguridad. 2.2.2 Daños por ataques informáticos. 2.2.3 Robo de información (con pérdidas pecuniarias). 2.2.4 Utilización inadecuada de claves de acceso y/o niveles de autorización. 6.1.1Hardware. 6.1.2 Software. 6.1.3 Telecomunicaciones. 6.1.4 Interrupción / incidencias en el Suministro	Reactivo.	Mensual.	Cantidad.	Variable X.	Número de incidentes de seguridad. de la información	-	Más de 5.	De 2 a 5.	Menos de 2.
KRI0008	Plataformas tecnológicas obsoletas y/o desactualizadas	Porcentaje de plataformas tecnológicas que se encuentran sobre versiones obsoletas y/o sin soporte por el fabricante	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Semestral	Porcentual.	(X/Y)*10.	Número de plataformas tecnológicas obsoletas.	Total de plataformas tecnológicas.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %
KRI0009	Caídas de sistemas relacionados con Los servicios brindados a sus Clientes	Número de caídas de sistemas relacionados con los servicios brindados a sus Clientes mayores a 10 minutos.	Infraestructura.	VI. Incidencias en el Negocio y fallas en los sistemas	6.1 Sistemas.	6.1.4 Interrupción / incidencias en el Suministro.	Reactivo.	Mensual.	Cantidad.	Variable X.	Numero de caídas de sistemas.	-	Más de 1.	Igual a 1.	Igual a 0.
KRI0010	Incidentes de seguridad por vulnerabilidades de sistemas provistos por proveedores (terceros).	Porcentaje de incidentes de seguridad causados por vulnerabilidades en sistemas e infraestructura tecnológica provistos por proveedores (terceros) que no pertenezcan a la	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 2.2.2 Daños por ataques informáticos. 2.2.3 Robo de información (con pérdidas pecuniarias).	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes de seguridad de atribuidos a vulnerabilidades en sistemas provistos por	Número total de incidentes de seguridad.	Más del 5 %.	Entre 0.1 % y 5 %.	Menor a 0.1 %.

		nómina de la IFC, reportados durante el periodo establecido, con respecto al total de incidentes de seguridad.				2.2.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.					proveedores (terceros).				

KRI0011	Vulnerabilidades críticas pendientes de corregir detectadas en las pruebas de hackeo ético.	Número de vulnerabilidades en los sistemas de información que, de acuerdo con las pruebas de hackeo ético, se cataloguen como críticas, las cuales tengan más de un mes de antigüedad a partir de su fecha de detección.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Mensual.	Cantidad.	Variable X.	Número de vulnerabilidades críticas pendientes de corregir con antigüedad de más de un mes.	-	Más de 2.	Entre 1 y 2.	Igual a 0.
KRI0012	Indisponibilidad de los sistemas de TI.	Porcentaje promedio del tiempo de indisponibilidad de los sistemas contra el tiempo total del periodo establecido.	Infraestructura.	VI. Incidencias en el Negocio y Fallas en los Sistemas.	6.1 Sistemas.	6.1.4 Interrupción / incidencias en el Suministro.	Reactivo.	Mensual.	Promedio Porcentual.	Promedio(X).	Promedio de tiempo de indisponibilidad de los sistemas de TI.	-	Más del 0.5 %.	Entre 0.25 % y 0.5 %.	Menos de 0.25 %.
KRI0013	Incidentes críticos y de alta prioridad en ambientes productivos.	Porcentaje de incidentes calificados como críticos y de alta prioridad en ambientes de producción respecto al total de incidentes en producción.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes en producción calificados como críticos.	Número total de incidentes en producción.	Mayor o igual a 0.5 %.	Mayor a 0% y menor 0.5 %.	Igual a 0 %.
KRI0014	Componentes de la infraestructura tecnológica expuestos a internet sin pruebas de hackeo ético y/o análisis de vulnerabilidades.	Porcentaje de los componentes de la infraestructura tecnológica de la organización expuestos hacia internet a los cuales no se haya realizado hackeo ético o análisis de vulnerabilidades, con respecto al total de equipos en más de 3 meses.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de activos expuestos a internet que no hayan realizado pruebas de hackeo ético o análisis de vulnerabilidades.	Número de activos expuestos a internet.	Más del 3 %.	Entre el 1 % y 3 %.	Menos del 1 %.
KRI0015	Vulnerabilidades críticas pendientes de corregir detectadas en los	Número de vulnerabilidades en los sistemas de información que, de acuerdo con los análisis de	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Cantidad.	Variable X.	Número total de vulnerabilidades críticas.	-	Más de 2	Entre 1 y 2	Igual a 0

	análisis de vulnerabilidades.	vulnerabilidades se cataloguen como críticas, las cuales, tengan más de un mes de antigüedad a partir de su fecha de detección.												
KRI0016	Infraestructura Tecnológica obsoleta y/o sin soporte.	Cantidad de equipos e Infraestructura Tecnológica, que se encuentran en versiones obsoletas o sin soporte, en comparación con toda la infraestructura de IT activa en el periodo establecido.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de equipos e infraestructura obsoleta.	Número total de equipos activos.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.
KRI0017	Servidores sin solución *antimalware.*	Porcentaje de servidores sin *antimalware* respecto del total de servidores.	*Malware.*	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores sin *antimalware*.	Número total de servidores.	Más del 6 %.	Entre 3% y 6 %.	Menor a 3 %.
KRI0018	Servidores con firmas de *antimalware* desactualizadas.	Porcentaje de servidores con firmas de *antimalware (malware signatures)* desactualizados respecto del total de servidores con *antimalware* en cada IFC	*Malware.*	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores con firmas *antimalware* desactualizadas.	Número total de servidores con *antimalware*.	Más del 6 %	Entre 3% y 6 %	Menor a 3 %
KRI0019	*Workstations* sin solución *antimalware*	Porcentaje de *workstations* sin *antimalware* con respecto al total de equipos	*Malware*.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de *workstations sin antimalware.*	Número total de *workstations.*	Más del 8 %.	Entre 4% y 8 %.	Menor a 4 %.
KRI0020	*Workstations* con firmas de *antimalware* desactualizadas.	Porcentaje de las *workstations* que cuentan con las firmas de antimalware *(malware signatures)* desactualizadas con respecto al total de equipos de cómputo con antimalware instalado.	Malware.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de *workstations* con firmas *antimalware* desactualizadas.	Número de *workstations* con *antimalware.*	Más del 8 %.	Entre 4% y 8 %.	Menor a 4 %.
KRI0021	Incidentes de seguridad atribuidos a personal de proveedores (terceros).	Porcentaje de incidentes de seguridad relacionados a personal de proveedores (terceros) que no pertenezcan a la nómina de la IFC, reportadas durante el	Incidentes.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes de seguridad relacionados con personal de proveedores (terceros).	Número de incidentes de seguridad total de personal de proveedores (terceros).	Más del 5 %.	Mayor a 0 % y menor 5 %.	Igual a 0 %.

		periodo establecido, con respecto al total de incidentes de seguridad.												
KRI0022	Servidores con versiones de sistema operativo obsoletas.	Porcentaje total de servidores con versiones de sistema operativo obsoletas comparado contra número total de servidores.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores con versiones de sistema operativo obsoletas.	Número total de servidores.	Más de 10 %.	Entre 5% y 10 %.	Menor a 5 %.
KRI0023	Aplicaciones en producción con cumplimiento parcial o deficiente de los controles de seguridad.	Porcentaje de las aplicaciones en producción con cumplimientos parciales o deficientes, con respecto a las políticas de seguridad establecidas, en cuestiones de seguridad, con respecto al total de aplicaciones.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de controles de seguridad deficientes en aplicaciones en producción.	Número total de controles de seguridad.	Más de 5 %.	Entre 2 % y 5 %.	Menos de 2 %.
KRI0024	*Data base managers (DBM)* con versiones de tecnología obsoletas o no soportadas.	Porcentaje de manejadores de *data base managers(DBM)*, los cuales son versiones de tecnologías obsoletas o no soportadas por el fabricante, en comparación con el total de *data base managers (DBM)* activos en el periodo establecido.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de *data base managers (DBM)* obsoletas o no soportadas.	Número total *data base managers* (DBM).	Más del 10 %.	Entre 5 % y 10 %.	Menos del 5 %.
KRI0025	Aplicaciones obsoletas o no soportadas.	Porcentaje de aplicaciones dentro de la IFC, las cuales se encuentran obsoletas o sin soporte por el fabricante, con relación a todas las aplicaciones activas durante el periodo establecido.	Software.	II. Fraude Externo. VI. Incidencias en el Negocio y Fallos en los Sistemas.	2.2 Seguridad de los Sistemas. 6.1 Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 6.1.2 Software.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de aplicaciones obsoletas o no soportadas.	Total de aplicaciones activas.	Más de 5 %.	Entre 2 % y 5 %.	Menos de 2 %.
KRI0026	Servidores sin cobertura de parches de seguridad.	Porcentaje de servidores sin los parches de seguridad más recientes, con respecto al total de servidores activos durante el periodo establecido.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores sin los parches de seguridad más recientes instalados.	Total de servidores.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.
KRI0027	*Workstations* sin cobertura de parches de seguridad.	Porcentaje de *workstations* sin los de parches de seguridad más recientes indistinto del sistema operativo de que se trate, con respecto al total de *workstations* de la IFC	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y))*100.	Número *workstations* sin los parches de seguridad más recientes instaladas totales.	Número de *workstations* totales.	Más del 3 %.	Entre 1 % y 3 %.	Menos del 1 %.

KRI0028	*Data base managers (DBM)* sin cobertura de parches de seguridad.	Porcentaje de *data base managers (DBM)* sin cobertura de los parches de seguridad más recientes, con respecto al total de *data base managers (DBM)* durante el periodo establecido.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de *data base managers (DBM)* sin cobertura de parches de seguridad.	Número total de *data base managers (DBM).*	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.