1. Política de Seguridad de Información

Este documento sustituye la política de seguridad originalmente emitida bajo el apartado 700 – Informática, con fecha 1 de mayo de 2014.

FIRMA: **JOHN ANTHONY SANTA MARIA OTAZUA** **DIRECCIÓN GENERAL**		
p/ Comité Directivo de Seguridad de Información		
FIRMA: **KARINA AWAD PEREZ** **DIRECCIÓN DE RECURSOS HUMANOS**	**FIRMA:** **CONSTANTINO SPAS MONTESINOS** **DIRECCIÓN ADMINISTRACIÓN Y FINANZAS**	**FIRMA:** **RAFAEL SUAREZ OLAGUIBEL** **DIRECCIÓN DE TRANSFORMACION**

POLÍTICA DE SEGURIDAD DE INFORMACIÓN

1. La Dirección General y el Comité Directivo de Coca Cola FEMSA (KOF)[1] consideran que la Seguridad de la Información y de los Sistemas de Información es crítica y prioritaria para la consecución de su Misión, Visión y Objetivos Estratégicos. Esto debido a que:

   a. El cibercrimen está creciendo aceleradamente convirtiéndose en una amenaza para los individuos, las organizaciones y la sociedad, agravada por el dinamismo de las tecnologías de información.

   b. Los riesgos relacionados con dichas tecnologías constituyen Riesgos de Negocio que pueden impactar la reputación de KOF, sus resultados económicos y/o el valor de su acción.

   c. La estrategia de negocio de KOF está fuertemente apalancada por las Tecnologías de Información, lo cual implica una dependencia y vulnerabilidad crecientes.

Objetivo

2. Esta política establece el nivel de prioridad y el enfoque de la Seguridad de Información (SI) en KOF, así como los lineamientos estratégicos y los principales roles y responsabilidades.

3. Como parte de esta política se emitirán las normas de operación indicadas en el anexo #1, ampliando o complementando conceptos mencionados en este documento (las "Normas de Operación").

Definiciones

4. **Seguridad de Información (SI):** Conjunto de medidas destinadas a proteger la disponibilidad, integridad y confidencialidad de la información y de los Sistemas de Información, aplicadas a la tecnología, los procesos y las personas.[2]

5. **Sistemas de Información:** Se refiere a la totalidad de recursos de tecnología de información utilizados para gestionar la información y las transacciones de KOF.

6. **Activos de Información:** Comprende la información, los Sistemas de Información y otros recursos relacionados con estos, necesarios para soportar los procesos de negocio.

7. **Apetito de Riesgo:** Es el nivel de riesgo que KOF está dispuesto a aceptar en sus procesos de negocio, basado en un análisis de impacto y probabilidad de ocurrencia.

8. **Dueño de Proceso:** Es la dirección funcional responsable de un proceso o función en la organización, sea operativo o de soporte, acorde con la funcionalización de KOF.

9. **Impactos de Negocio:** Posibles impactos para KOF derivados de riesgos de SI: Interrupción de operaciones; Fraude; Robo o pérdida de información; Responsabilidad legal por mal manejo de información de terceros; Daño reputacional y/o del valor de la acción; e Incumplimiento regulatorio.

10. **Incidente Serio de SI:** Materialización de un riesgo de SI que ha sobrepasado los controles establecidos y que puede originar un Impacto de Negocio o una crisis.[3]

---

[1] El "Comité Directivo de KOF" en esta política se refiere al Director General y a sus reportes directos.

[2] La protección de la información comprende cuando esta es creada, almacenada, transmitida, procesada y eliminada, sea en medios digitales y/o físicos.

[3] Los términos "Incidente serio" y "crisis" son equivalentes al sistema MIRC.

Organización y Gobernanza

11. Se establece una separación de funciones entre la Gobernanza y las Operaciones de SI.

    a. La Gobernanza recae en el Director de SI (también referido como CISO o Chief Information Security Officer) quien reporta al Director de Finanzas (CFO).

    b. Las Operaciones de SI corresponden a la Dirección de Tecnologías de Información (TI) a través del Gerente de Tecnologías de Seguridad y de las demás gerencias de TI en su respectiva función.

12. Se conforma un Comité Directivo de SI cuyo principal rol es proveer el compromiso y patrocinio del Comité Directivo de KOF hacia la estrategia de SI y asegurar la alineación de esta con la estrategia del negocio. Está conformado por quienes encabezan las direcciones de Finanzas, Transformación, Recursos Humanos, TI y SI, así como el CISO de FEMSA.

13. El CISO, con el apoyo del Director de TI, reportará el estatus de la SI y de la ejecución de la estrategia al Comité Directivo de KOF y al Comité de Auditoría del Consejo de Administración.

14. En lo que se refiere a servicios de TI administrados por terceros, los de seguridad serán operados por un proveedor distinto del resto. Cuando esto no sea posible por razones prácticas o técnicas, el director de TI y el CISO acordarán la distribución de actividades de seguridad.

Enfoque de la SI

15. KOF adopta un enfoque preventivo y sistémico, mediante un Sistema de Gestión de la SI[4] que le permita lograr una madurez medible y la mejora continua de la SI. El Comité Directivo de SI establecerá el nivel de madurez objetivo y el plazo para alcanzarlo, siendo parte de dicho proceso la implementación gradual de esta política y de las normas complementarias.

Seguridad desde el diseño

16. La SI es un habilitador para el desarrollo de negocios seguros y sostenibles, por lo tanto, debe ser considerada desde el diseño en los nuevos desarrollos y proyectos, en la adquisición de tecnologías de información o de servicios que las involucren, así como durante la vida útil de las mismas.

17. Las áreas de TI, Abastecimiento y Dueños de Proceso asegurarán que el nivel adecuado de SI[5] sea incorporado oportunamente. Su costo será considerado como parte de la respectiva funcionalidad.

18. Las direcciones Legal, Abastecimiento, TI y SI establecerán, en los contratos correspondientes, los los requisitos y condiciones relacionados con la SI en las adquisiciones de bienes y servicios, acorde con el riesgo que estas representen.

Cultura de Seguridad de Información

19. Las direcciones de SI y Recursos Humanos[6] en conjunto, establecerán y ejecutarán programas anuales para desarrollar una cultura de SI que se consolide en el mediano y largo plazo. Dichos

---

[4] El Sistema de Gestión será implementado y gestionado por la Dirección de SI.

[5] El "nivel adecuado de SI" será definido por TI con base en la criticidad de la información y del proceso involucrado, establecida previamente por el Dueño del Proceso.

[6] Lo hará a través de la gerencia de Cultura y Comunicación.

programas comprenden la difusión de normatividad, la concientización y el entrenamiento hacia las diferentes audiencias de la organización.

Gestión de Riesgos de Seguridad de Información

20. Como parte del Sistema de Gestión de la SI, se adopta una metodología de gestión de riesgos, con el objetivo de priorizar esfuerzos e inversiones hacia los procesos de negocio más relevantes y sus respectivos Activos de Información.

21. Corresponde a los Dueños de Proceso el análisis de riesgos relacionados con los Activos de Información de sus procesos, a fin de proporcionar al Comité Directivo de KOF insumos para la toma de decisiones sobre Apetito de Riesgo. Para esto contarán con el soporte y la metodología establecida por la Dirección de SI.

22. La definición del Apetito de Riesgo y la aceptación de riesgos relevantes por encima del mismo corresponde a los miembros del Comité Directivo de KOF. Es función del CISO gestionar el nivel de aprobación requerido[7] y a su vez, emitir una recomendación previa en dichas decisiones.

Gestión de la SI del Sistema de Control Industrial (OT[8])

23. Las direcciones de TI, Cadena de Suministro y SI definirán los límites entre la red OT y la red de datos de KOF, así como las reglas técnicas y la configuración bajo las cuales ambas redes convivirán. Corresponde a la dirección de TI la segregación tecnológica de ambas redes.[9]

24. La dirección de Cadena de Suministro establecerá medidas de seguridad para la OT acordes con el Apetito de Riesgo, para lo cual se apoyará en asesoría especializada. Las direcciones de SI y TI apoyarán en este esfuerzo.

Respuesta a Incidentes Serios de SI

25. La organización desarrollará capacidades de detección y respuesta a Incidentes Serios de SI en las siguientes instancias, que deberán ser documentadas y ejercitadas al menos una vez al año.

26. **Manejo técnico de incidentes**: Las direcciones de TI y SI implementarán las capacidades de respuesta técnica, mediante una combinación de recursos propios y externos especializados.

27. **Manejo y resolución de crisis:** La dirección de Asuntos Corporativos incorporará los Incidentes de SI como parte de la metodología MIRC y liderará su despliegue a nivel Corporativo y local.

28. **Continuidad de negocios:** Los escenarios de Incidentes Serios de SI serán incorporados en los planes de continuidad de negocios (BCP) por parte de las operaciones (países) o Dueños de Proceso, según corresponda, con el apoyo de las direcciones de TI y SI.

29. **Restauración de los Sistemas de Información:** La Dirección de TI considerará los Incidentes de SI dentro de su plan de recuperación de desastres (DRP).[10]

---

[7] La Norma de Operación "Gestión de Riesgos de SI" contendrá los criterios de escalación para esos casos.
[8] Las tecnologías de información que soportan el control industrial se conocen como "Operational Technology".
[9] Será documentado en la Norma de Operación "Seguridad del sistema de control industrial (OT)"
[10] BCP: Business continuity plan / DRP: Disaster recovery plan.

Cumplimiento regulatorio

30. El cumplimiento de las leyes de protección de datos personales deberá ejecutarse y verificarse a nivel de cada Operación (país) y de la Oficina Central, respecto a las leyes que les aplique.

31. Para esto, en cada Operación (país) y en la Oficina Central se designará un abogado, parte de su equipo Legal, responsable de validar y asesorar sobre el cumplimiento de dicha legislación ("Compliance Officer"). A la vez se integrará un equipo de las áreas de Recursos Humanos, TI y Finanzas que establecerá los procesos y controles para tal efecto. Se deberán proveer los recursos necesarios para el cumplimiento de estas legislaciones.

32. La exposición en internet, publicación y/o transferencia de datos personales a terceros por cualquier medio debe evaluarse previamente a la luz de las leyes mencionadas. El Compliance Officer y el equipo mencionados en el párrafo anterior deben asegurar los controles legales, administrativos y tecnológicos, así como el apego a la normatividad interna[11].

33. El software instalado en equipos propiedad de KOF o arrendados debe ser institucional, adquirido legalmente y debe contar con licencia de uso y soporte del fabricante.

34. Los Dueños de Proceso serán responsables de establecer controles para que la información de negocios de KOF, relativa a sus procesos, se difunda o revele en estricto apego a las regulaciones de valores de México, los Estados Unidos de América, o de las geografías donde KOF cotice valores; para lo que deberán apoyarse en la asesoría de la dirección Legal.

Responsabilidades de los usuarios y líderes

35. Los empleados y el personal tercero tienen la responsabilidad de velar por la seguridad de los Activos de Información en el ámbito de su rol, cumpliendo con la normatividad que les aplique y colaborando con su implementación.

36. Es responsabilidad de los líderes promover una cultura acorde con la SI en sus equipos de trabajo e implementar la normatividad interna que les corresponda en su ámbito de responsabilidad.

37. Los Activos de Información propiedad de KOF deben ser utilizados únicamente para los fines previstos. Está prohibida la extracción, entrega o transmisión a terceros de información de KOF sin la debida autorización.

Plan Anual de Actividades de SI

38. Basado en los lineamientos de esta política, las direcciones de TI y de SI, deben elaborar un plan anual de actividades en materia de SI. La evaluación por parte de un tercero debe considerarse al menos cada dos años y la remediación de hallazgos contemplarse dentro de dichos planes.

Evaluación y mejora continua

39. El Sistema de Gestión de la SI debe ser evaluado periódicamente por un ente independiente, con el fin de asegurar su apego a esta política y a las normas de operación establecidas.

40. La Dirección de SI coordinará la revisión de esta política y de las Normas de Operación que la complementan en forma anual, manteniéndolas alineadas con la estrategia del negocio.

[11] Será emitida una Norma de Operación sobre "Privacidad y protección de la información personal".

Anexo #1

Normas de Operación[12]

1. Seguridad de información y el recurso humano
2. Administración de activos
3. Clasificación de información
4. Control de accesos
5. Controles de cifrado
6. Seguridad física y ambiental
7. Seguridad de operaciones, tales como:
    a. Procedimientos operacionales y responsabilidades
    b. Protección contra malware
    c. Respaldos
    d. Registro y monitoreo de actividades de usuarios
    e. Control de software operacional
    f. Gestión de vulnerabilidades técnicas
8. Seguridad de las comunicaciones
9. Adquisición, desarrollo y mantenimiento de sistemas
10. Relaciones con proveedores y terceros
11. Gestión de incidentes de seguridad
12. Gestión de la continuidad de negocios ante incidentes de seguridad
13. Reglas para el usuario final, tales como:
    a. Uso aceptable de activos
    b. Escritorio y pantalla limpios
    c. Transferencia de información
    d. Dispositivos móviles y teletrabajo
    e. Restricciones en la instalación y uso de software
    f. Respaldos de información
14. Privacidad y protección de la información personal
15. Gestión de Riesgos de Seguridad de Información
16. Seguridad en la nube
17. Cumplimiento regulatorio y de normatividad interna y contractual
18. Seguridad del sistema de control industrial (OT)

[12] Adaptado del estándar internacional ISO/IEC 27001:2013. Estas normas de operación serán definidas e implementadas gradualmente, conforme a “road map” aprobado por el Comité Directivo de SI.

Política de Seguridad de Información Matriz RACI - principales roles y responsabilidades nov-19

	Tópico	Índice	Comité Directivo de KOF	Direcciones de										
				Finanzas	Transfor-mación	RH	CDS e Ingeniería	Asuntos Copora-tivos	División (Paises)	Dueños de proceso*	SI (CISO)	TI	Abasto	Legal
1	Gobierno de SI (Comité Directivo de SI)	**11**	**I**	**R**	**R**	**R**					**A/R**	**R**		
2	Operaciones de SI	11									**C**	**A/R**		
3	Sistema de Gestión de SI	15	**I**	**I**	**I**	**I**					**A/R**	**C**		
4	Incorporación de seguridad desde el diseño y vida útil de aplicaciones	16,17								**A/R**	**C**	**R**	**R**	
5	Incorporación de seguridad en el desarrollo y mantenimiento	16,17								**A**	**C**	**R**		
6	Requerimientos contractuales en la adquisición de bienes y servicios	18									**A/R**	**C**	**R**	**R**
7	Desarrollo de Cultura de SI	19,36	**I**			**R**			**I/R**	**I/R**	**A/R**			
8	Gestión de Riesgos de SI:													
9	- Identificación y análisis de riesgos en los procesos de negocio	21								**A/R**	**R**	**C**		
10	- Definición de apetito de riesgo y aceptación de riesgos relevantes	22	**A/R**							**C**	**C**			
11	Gestión de la SI del Sistema de Control Industrial	23,24					**A/R**				**R**	**R/C**		
12	Respuesta a Incidentes serios de SI:													
13	- Manejo técnico de incidentes (CIRP)	26									**R**	**A/R**		
14	- Manejo y resolución de crisis (MIRC)	27						**A/R**	**R**		**C**			
15	- Continuidad de negocios (BCP)	28	**A**						**R**	**R**	**C**	**C**		
16	- Restauración de sistemas de información (DRP)	29							**C**	**C**	**C**	**A/R**		
17	Cumplimiento de leyes de privacidad	30,31, 32		**R**		**R**			**A/R**			**R**		**R**
18	Cumplimiento de LMV en la difusión de información	34		**A**						**R**				**C**
19	Plan anual de actividades de SI	38	**I**	**C**	**C**	**C**					**A/R**	**R**		
20	Evaluación y mejora continua	39,40		**I**	**I**	**I**					**A/R**			

* Los "Dueños de proceso" mayoritariamente corresponden a las direcciones de segundo nivel en las áreas de CDS, Desarrollo Comercial, Finanzas y Recursos Humanos, a raíz de la funcionalización, aunque en algunos casos podrían existir procesos liderados desde las direcciones Divisionales.