

"NORMATIVA DE TECNOLOGÍA DE INFORMACIÓN PARA LAS ENTIDADES FISCALIZADAS POR LA SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS"

SECCIÓN I

DISPOSICIONES GENERALES

Artículo 1. Objetivo

La presente normativa contiene los lineamientos generales que la Superintendencia General de Entidades Financieras utilizará para evaluar la administración, los sistemas, los equipos, la seguridad, la utilización y los controles aplicados al Área de Tecnología de Información de las entidades fiscalizadas, con el fin de velar por la estabilidad y la eficiencia del sistema financiero.

Artículo 2. Ámbito de aplicación

Esta normativa será de aplicación general para todas las entidades fiscalizadas por la Superintendencia General de Entidades Financieras.

Artículo 3. Definiciones

Para efectos de aplicación de la presente normativa, deberán considerarse las siguientes definiciones desde la perspectiva de Tecnología de Información:

Arquitectura de información: Estructura lógica de las bases de datos de la entidad.

Auditor externo calificado: Profesional certificado CISA (Auditor Certificado de Sistemas de Información por sus siglas en inglés "*Certified Information Systems Auditor*") emitido por la ISACA (Asociación de Auditoría y Control de Sistemas de Información, por sus siglas en inglés "*Information Systems Audit and Control Association*").

Base de datos: Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de la entidad.

Bitácora: Registro manual o electrónico que provee información necesaria para identificar e investigar algún problema o incidente.

Cableado estructurado: Es un sistema de cableado planificado para hacer frente a las reconfiguraciones, la detección de fallas y el crecimiento futuro en una red que toma en cuenta requerimientos de seguridad, etiquetado, ordenamiento y flexibilidad.

Configuración base: Parámetros mínimos de configuración que deben tener los equipos y sistemas.

Control: Para efectos de esta normativa se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para procurar que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

Entidad: Se refiere a todas las instituciones bancarias, cooperativas, empresas financieras no bancarias, mutualistas, y otros establecidos por leyes especiales, sujetos a la supervisión de la Superintendencia General de Entidades Financieras.

Pared de fuego (“*Firewall*”): Combinación de computadores, enrutadores, filtradores de paquetes, subredes, *Software*, y las políticas y procedimientos que gobiernan estos componentes, utilizados para proteger la entidad de ataques provenientes de Internet u otra red pública.

Infraestructura tecnológica: Edificio, equipo y sistemas con que cuenta la entidad para procesar la información.

Manual de puestos: Contiene las funciones y responsabilidades de cada uno de los puestos que conforman la estructura organizativa del Departamento de Tecnología de Información.

Plan de continuidad: Documento donde se detallan los procedimientos por seguir en caso de una contingencia, con el fin de no afectar el funcionamiento normal de la entidad.

Políticas: Conjunto de prácticas establecidas por el Órgano Directivo de la entidad, por medio de las cuales se definen los cursos de acción a seguir por la Administración.

Procedimiento: Método o sistema estructurado para ejecutar instrucciones. Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.

Procesamiento en el exterior: Proceso sobre la información propia de la entidad, realizado con equipo y sistemas en otro país.

Proveedor: Persona física o jurídica que vende, alquila o renta un bien o servicio de Tecnología a la entidad.

Riesgo: La posibilidad de que un evento no deseado ocurra afectando la actividad normal de la entidad.

Seguridad lógica: Seguridad a nivel del Software para proteger los sistemas y datos.

Tecnología de información (TI): *Software*, *Hardware*, comunicaciones y datos.

Usuario final: Personal que utiliza los recursos de Tecnología de Información con el fin de alcanzar los objetivos de la entidad.

Artículo 4. Factores

Para efectos de aplicación de la presente normativa, deberán considerarse los siguientes factores:

Confiability: Los sistemas deben brindar información correcta, completa, oportuna y exacta, que será utilizada en la operación de la entidad y en la toma de decisiones, la preparación de estados financieros e información gerencial y su remisión a organismos reguladores.

Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada.

Disponibilidad: Los recursos y la información deben estar disponibles en tiempo y forma, cada vez que sean requeridos por los usuarios.

Efectividad: La información y los procesos deben ser relevantes y pertinentes para el proceso del negocio, además de presentarse en forma correcta, coherente, completa y que pueda utilizarse oportunamente.

Eficiencia: El proceso de la información debe realizarse mediante una óptima (más productiva y económica) utilización de los recursos.

Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

SECCIÓN II

CALIFICACIÓN CUANTITATIVA DEL ÁREA DE TECNOLOGÍA DE INFORMACIÓN

Artículo 5. La Superintendencia General de Entidades Financieras comunicará a las entidades bajo su supervisión una calificación cuantitativa sobre el área de Tecnología de Información; en adelante TI, producto de una evaluación “in situ”, de conformidad con la Matriz de Calificación ([Anexo 1](#)). La evaluación comprenderá nueve áreas denominadas: Administración del área de TI, Seguridad lógica y acceso a los datos, Seguridad física, Sistemas de información, Software y bases de datos, Hardware, redes y comunicaciones, Continuidad de las operaciones, Servicios financieros por Internet y Descentralización de procesamiento en el exterior. Como resultado de la evaluación, cada área obtendrá un porcentaje entre 0 y 100%, y será ubicado en rangos según los cuales se asume menor o mayor riesgo, sea en nivel normal, irregularidad 1, irregularidad 2 o irregularidad 3 de acuerdo con la siguiente tabla.

Área	Normal	Irregularidad 1	Irregularidad 2	Irregularidad 3
Administración del área de TI	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Seguridad lógica y acceso a los datos	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Seguridad física	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Sistemas de información	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Software y bases de datos	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Hardware , redes y comunicaciones	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Continuidad de las operaciones	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Servicios financieros por Internet	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%
Descentralización de procesamiento en el exterior	Mayor o igual a 85%	Mayor o igual a 70% pero menor a 85%	Mayor o igual a 55% pero menor a 70%	Menor a 55%

Internamente, las entidades deberán desarrollar sus propios procedimientos de evaluación que les permitan autoevaluarse en cada una de las áreas, de acuerdo con esta normativa.

La calificación general (CG) dependerá del tipo de entidad que se esté evaluando. El tipo de entidad está relacionado con la tenencia de las dos últimas áreas de evaluación (Servicios financieros por Internet y Descentralización de procesamiento en el exterior) y el valor de riesgo asignado a cada una de las áreas, se distribuirá de acuerdo con la siguiente tabla:

Área	Tipo de Entidad 1	Tipo de Entidad 2	Tipo de Entidad 3	Tipo de Entidad 4
Administración del área de TI	14%	14%	14%	14%
Seguridad lógica y acceso a los datos	14%	14%	14%	14%
Seguridad física	12%	12%	12%	12%
Sistemas de información	12%	12%	12%	12%
Software y bases de datos	12%	12%	12%	12%
Hardware , redes y comunicaciones	11%	11%	11%	11%
Continuidad de las operaciones	11%	11%	11%	11%
Servicios financieros por Internet	7%	7%	0%	0%
Descentralización de procesamiento en el exterior	7%	0%	7%	0%
	100%	93%	93%	86%

La calificación general se obtendrá a partir de la sumatoria del valor de riesgo obtenido en cada una de las áreas de evaluación (VROA) y considerando la siguiente tabla:

Tipo de entidad	Fórmula
1	$CG = S(VROA)$
2	$CG = (S(VROA)*100)/93$
3	$CG = (S(VROA)*100)/93$
4	$CG = (S(VROA)*100)/86$

Una vez obtenida la calificación general, la entidad se ubicará en alguno de los estados, según la siguiente tabla:

ESTADO	CALIFICACIÓN GENERAL
Normal	Mayor o igual que 85%
Irregularidad 1	Mayor o igual que 70% y menor que 85%
Irregularidad 2	Mayor o igual que 55% y menor que 70%
Irregularidad 3	Menor que 55%

Para obtener la calificación de las áreas y la calificación general de la entidad, se utilizarán en todo momento dos dígitos decimales sin redondeo.

Cuando una entidad presente cinco o más áreas en algún grado de irregularidad, automáticamente se le conferirá el grado de irregularidad 1, siempre y cuando su calificación general no la ubique un grado de irregularidad mayor.

Una vez remitido el informe a la entidad fiscalizada, la Superintendencia le otorgará un plazo no menor de tres días ni mayor de diez días hábiles para efectuar los alegatos y suministrar las pruebas de descargo que considere pertinentes. Posterior a la evaluación de las pruebas por el personal de la Superintendencia, se comunicará por escrito el informe final a la entidad, otorgándole un plazo de 10 días hábiles para presentar un plan de acción que permita subsanar las debilidades mencionadas en el informe. Contra el informe final podrán interponerse los recursos de revocatoria y apelación los cuales deben ser presentados ante este Despacho dentro del plazo de los tres días hábiles siguientes a la notificación del oficio. El recurso de revocatoria será resuelto por el Superintendente General y el recurso de Apelación por el Consejo Nacional de Supervisión del Sistema Financiero. La interposición de alguno o ambos recursos no suspende los efectos del acto. Si la entidad decide no efectuar alegatos y aceptar las observaciones contempladas en el primer informe, este será considerado como el informe final y de igual forma se le otorgará un plazo de 10 días hábiles para presentar el plan de acción.

La calificación general del área de TI, se mantendrá hasta la próxima visita de supervisión de TI que efectúe la Superintendencia. Si la entidad desea que se varíe esta calificación, antes de la visita de supervisión, podrá presentar una solicitud en este sentido a la Superintendencia adjuntando un informe preparado por la auditoría interna de TI de la entidad o en su defecto podrá contratar los servicios de un auditor externo calificado, para que lo emita. El informe preparado por la auditoría interna o el auditor externo calificado contratado al efecto, deberá contener una evaluación de todas las debilidades mencionadas en el último informe de TI remitido por esta Superintendencia a la entidad supervisada. A este informe deberá adjuntarse toda la evidencia que respalde los resultados obtenidos en dicha evaluación, para su posterior valoración por el personal de esta Superintendencia. Para esto, la Superintendencia contará con un plazo de 30 días hábiles contados a partir del día hábil posterior a la recepción de la solicitud, para comunicar a la entidad la calificación obtenida. Contra la resolución que comunique esta calificación podrán interponerse los recursos de revocatoria y apelación los cuales deben ser presentados ante este Despacho dentro del plazo de los tres días hábiles siguientes a la notificación del oficio. El recurso de revocatoria será resuelto por el Superintendente General y el recurso de Apelación por el Consejo Nacional de Supervisión del Sistema Financiero. La interposición de alguno o ambos recursos no suspende los efectos del acto.

SECCIÓN III

ADMINISTRACIÓN DEL ÁREA DE TECNOLOGÍA DE INFORMACIÓN

Artículo 6. La entidad debe realizar un proceso de planificación de TI de acuerdo con la planeación estratégica institucional, que facilite la consecución de sus logros futuros.

Artículo 7. La entidad debe identificar, organizar, capacitar y desarrollar a los usuarios finales en el uso efectivo de la tecnología, seguridad, riesgos y responsabilidades relacionadas con el desarrollo normal de sus funciones. Asimismo, mantener un programa de capacitación de acuerdo con las prioridades de la administración, que permita maximizar las contribuciones que brinda el personal del área de TI. Esta capacitación deberá incluirse en el presupuesto anual y ser consistente con los requerimientos mínimos de la organización.

Artículo 8. La entidad debe procurar que a través de métodos y esquemas de trabajo, se facilite la consecución de los objetivos planteados. Para esto la entidad debe:

- a. Velar porque la ubicación del área de TI, se encuentre en un nivel razonable de independencia funcional dentro de la estructura organizacional.
- b. Definir y mantener actualizado el manual de puestos para el personal de TI, de manera que las funciones y responsabilidades queden claramente establecidas.
- c. Definir los procedimientos que permitan la contratación y adquisición de recursos de TI.
- d. Establecer una metodología que permita administrar adecuadamente los proyectos internos y externos (outsourcing), de acuerdo con los recursos proyectados e invertidos.

Artículo 9. La entidad debe procurar a través de diferentes mecanismos, que los miembros de la organización actúen de modo que contribuyan al logro de los objetivos. Para esto la entidad debe:

- a. Establecer y comunicar los objetivos de la administración y las políticas de TI, a los niveles pertinentes.
- b. Contar con personal técnicamente capacitado o en su ausencia contratarlo externamente.

Artículo 10. La entidad debe implantar los mecanismos de control necesarios para la supervisión de las tareas. Para esto la entidad debe:

- a. Verificar el cumplimiento de los controles y objetivos establecidos para los procesos de TI.
- b. Contar con un contrato vigente de prestación de servicios para el caso en que sus servicios de TI no sean propios.

- c. Velar por el cumplimiento de sus obligaciones legales, regulatorias y contractuales, en los plazos y formas establecidas, así como las que terceros han establecido con la entidad.

Artículo 11. La entidad que subcontrate parte o la totalidad de su procesamiento de datos en nuestro país, deberá incluir en los contratos que suscriba, una cláusula que permita a esta Superintendencia la supervisión de las tareas contratadas en las instalaciones del proveedor.

SECCIÓN IV

SEGURIDAD LÓGICA Y ACCESO A LOS DATOS

Artículo 12. La entidad debe administrar adecuadamente la seguridad lógica de los recursos de TI. Para esto la entidad debe:

- a. Establecer políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos.
- b. Establecer políticas y procedimientos que permitan dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos.

Artículo 13. La entidad debe mantener una adecuada seguridad en todos aquellos puntos con acceso a redes públicas de datos. Para esto la entidad debe:

- a. Definir controles que permitan restringir el tráfico hacia dentro y fuera de la red institucional (Pared de fuego).
- b. Establecer políticas y procedimientos de prevención, detección y corrección de virus.
- c. Establecer políticas y procedimientos que regulen la utilización del correo electrónico.

SECCIÓN V

SEGURIDAD FÍSICA

Artículo 14. La entidad debe establecer políticas y procedimientos relacionados con la ubicación, construcción, acceso físico al (a los) centro(s) de cómputo y comunicaciones.

Artículo 15. La entidad debe contar con procedimientos de control que regulen las condiciones ambientales del (los) centro(s) de cómputo y comunicaciones, que proporcionen un ambiente físico conveniente para su funcionamiento y protejan los recursos materiales y al personal de TI contra peligros naturales o fallas humanas.

SECCIÓN VI

SISTEMAS DE INFORMACIÓN

Artículo 16. La entidad debe procurar a través de procedimientos de trabajo, el diseño e implementación de sistemas de información eficaces, seguros y que impidan la modificación no autorizada, asimismo se ajuste al cumplimiento de las leyes, reglamentos y normativa vigente que les sean aplicables. Para esto la entidad debe:

- a. Implementar una metodología para el ciclo de vida del desarrollo de sistemas, que asegure la calidad de los sistemas de información y satisfaga los requerimientos del usuario.
- b. Definir una adecuada separación de los ambientes de desarrollo y producción, de forma que el personal de desarrollo no tenga acceso al ambiente en producción.

Artículo 17. La entidad debe velar por la adecuada disponibilidad, capacidad y el desempeño de los sistemas de información.

Artículo 18. La entidad debe contar con políticas y procedimientos relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, que asegure que los mismos permanezcan completos, precisos y válidos.

SECCIÓN VII

SOFTWARE Y BASES DE DATOS

Artículo 19. La entidad debe administrar adecuadamente sus bases de datos. Para esto la entidad debe:

- a. Definir la arquitectura de información para organizar y aprovechar de la mejor forma los sistemas de información.
- b. Establecer políticas y procedimientos actualizados relacionados con la instalación, administración, migración, mantenimiento y seguridad de las bases de datos.
- c. Definir mecanismos para controlar la integridad, disponibilidad, capacidad y el desempeño de las bases de datos.
- d. Definir períodos de almacenamiento y eliminación de información, acordes con los requerimientos legales.

Artículo 20. La entidad debe definir políticas y procedimientos para la adecuada instalación, mantenimiento y administración de *Software* debidamente autorizado. Además, todo su *Software* deberá actualizarse con las últimas mejoras de seguridad publicadas por el proveedor, de la versión que están utilizando y que todavía cuenta con soporte por parte del proveedor. Lo anterior con el fin de reducir su vulnerabilidad, producto de las deficiencias en los sistemas de seguridad, sistemas operativos, base de datos, antivirus, entre otros.

SECCIÓN VIII

HARDWARE , REDES Y COMUNICACIONES

Artículo 21. La entidad debe administrar adecuadamente el *Hardware*, las redes y las líneas de comunicación. Para esto la entidad debe:

Realizar estudios de capacidad y desempeño del *Hardware* y las líneas de comunicación, que permitan determinar en forma oportuna, necesidades de ampliación de capacidades o actualizaciones de equipos.

Establecer mecanismos para procurar que todas las redes instaladas, ya sean eléctricas, de voz o de datos, cumplan con los requerimientos mínimos vigentes de cableado estructurado. Entre estos deberán considerarse la documentación, el etiquetado, ductos para el cableado y el aterrizamiento del mismo.

Establecer políticas y procedimientos para la instalación y mantenimiento del *Hardware* y su configuración base, que proporcionen la plataforma de TI apropiada para soportar las aplicaciones de la entidad y reduzcan la frecuencia e impacto de las fallas de desempeño del *Hardware*.

Artículo 22. La entidad debe administrar adecuadamente su red de Cajeros Automáticos. Para esto la entidad debe:

- a. Establecer políticas y procedimientos para la ubicación, protección y mantenimiento de los cajeros automáticos.
- b. Mantener en línea los cajeros automáticos con los sistemas de información de la entidad, de tal forma que en todo momento se cuente con la información actualizada de los saldos de los clientes.

- c. Establecer políticas y procedimientos para la comunicación al cliente sobre el uso adecuado de los cajeros automáticos.
- d. Mantener activas y definir periodos de retención para las bitácoras que permitan la reconstrucción de las transacciones efectuadas en los cajeros automáticos .

SECCIÓN IX

CONTINUIDAD DE LAS OPERACIONES

Artículo 23. La entidad debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de emergencia, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares.

Artículo 24. La entidad debe establecer un plan de continuidad, donde se detallen acciones, procedimientos y recursos que considere los riesgos posibles, que afecten de forma parcial o total la operativa normal de los servicios de TI. Este plan deberá ser aprobado por la máxima autoridad de la entidad y ser comunicado a los niveles pertinentes. Además, este plan debe probarse al menos una vez al año.

Artículo 25. La entidad debe contar con una infraestructura adecuada, que contemple el suministro de energía eléctrica para la continuidad del negocio en caso de fallas temporales en la red pública.

Artículo 26. La entidad debe contar con cobertura de seguros para los principales equipos de cómputo y comunicaciones que permita mitigar el riesgo provocado por incendio, impacto de rayo, explosión, implosión, humo, gases o líquidos corrosivos, corto circuito, variaciones de voltaje, huelga, motín, robo, asalto y fenómenos naturales.

SECCIÓN X

SERVICIOS FINANCIEROS POR INTERNET

Artículo 27. La entidad debe establecer y comunicar a sus clientes las condiciones legales y operativas bajo las cuales se brindará el servicio financiero por Internet, que determinen cuándo, cómo, dónde y a quién se le dará el servicio.

Artículo 28. La entidad debe administrar adecuadamente la seguridad lógica de los servicios financieros por Internet. Para esto la entidad debe:

- a. Establecer
- b. Implementar mecanismos de seguridad que protejan la integridad y privacidad de la información sensible cuando el canal de transmisión sea Internet.
- c. Implementar y dar mantenimiento a los mecanismos de seguridad en todos aquellos puntos con acceso al servicio financiero por Internet. Estos mecanismos deberán probarse al menos dos veces al año.
- d. Mantener activas y definir periodos de retención para las bitácoras que permitan la reconstrucción de las transacciones efectuadas mediante los servicios financieros por Internet

Artículo 29. La entidad debe considerar dentro del plan de continuidad, un apartado donde se detallen acciones, procedimientos y recursos que consideren los riesgos posibles, que afecten de forma parcial o total la operativa normal de los servicios financieros por Internet.

Artículo 30. La entidad debe velar por la adecuada disponibilidad, capacidad y el desempeño de los servicios financieros por Internet

Artículo 31. La entidad debe comunicar a los clientes que utilicen los servicios financieros por Internet, cuando se abandona el sitio web de la entidad y se accesa el de un tercero.

SECCIÓN XI

DESCENTRALIZACIÓN DE PROCESAMIENTO EN EL EXTERIOR

Artículo 32. La entidad que requiera descentralizar parte o la totalidad de su procesamiento en el exterior (fuera del país), debe comunicar el detalle de esta situación a la Superintendencia General de Entidades Financieras, al menos, con 45 días hábiles de anticipación al inicio de sus operaciones en el sitio remoto. En la comunicación deberá incluirse el detalle de las actividades descentralizadas, una descripción del entorno de procesamiento, el sitio remoto, los encargados de su operación y los responsables de su control. Durante este periodo la Superintendencia evaluará la información remitida y se coordinarán las pruebas al plan de contingencias mencionadas con el Artículo 34. Para el caso de las entidades que, a la entrada en vigencia de esta normativa ya tienen descentralizado su procesamiento en el exterior, deben ajustarse a lo solicitado en esta sección, dentro de los primeros 45 días hábiles de vigencia de esta normativa.

Artículo 33. La entidad debe, para todas las actividades relacionadas con el procesamiento en el exterior, ajustarse a la normativa vigente en TI de la Superintendencia General de Entidades Financieras y facultarla para su verificación “in situ”, cuando lo considere necesario.

Artículo 34. La entidad debe considerar dentro del plan de continuidad, la interrupción del procesamiento en el sitio remoto. En este caso, la entidad debe contar con las medidas necesarias que le permitan continuar con su procesamiento normal en nuestro país. Esta sección debe ser probada en presencia de personal de la Superintendencia General de Entidades Financieras, antes de iniciar el procesamiento en el sitio remoto y al menos una vez al año. Para esto, la entidad debe comunicar a esa Superintendencia la intención de efectuar las pruebas, con 20 días hábiles de anticipación.

Artículo 35. La entidad supervisada deberá solicitar al organismo encargado del procesamiento en el sitio remoto, en caso que este sea supervisado, una certificación extendida por el organismo supervisor de su país, que haga constar que tiene conocimiento de la descentralización de operaciones y especificar si supervisará estas actividades como parte de su programa normal. Esta certificación deberá remitirse a la Superintendencia General de Entidades Financieras adjunta a la comunicación del Artículo 32 de esta Normativa.

Artículo 36. La entidad debe remitir a la Superintendencia General de Entidades Financieras, durante el mes de mayo de cada año, todos aquellos informes sobre el área de tecnología de información en el sitio remoto, emitidos por las auditorías internas y externas. Estos informes deben traducirse al idioma castellano por un traductor autorizado.

SECCIÓN XII

DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 37. Durante el primer año de vigencia de la normativa y solo por este periodo, se utilizarán los siguientes valores para establecer el nivel de riesgo de cada una de las áreas de evaluación de Tecnología de Información.

Área	Normal	Irregularidad 1	Irregularidad 2	Irregularidad 3
Administración del área de TI	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%
Seguridad lógica y acceso a los datos	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%
Seguridad física	Mayor o igual a	Mayor o igual a	Mayor o igual a	Menor a 40%

	80%	60% pero menor a 80%	40% pero menor a 60%	
Sistemas de información	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%
Software y bases de datos	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%
Hardware , redes y comunicaciones	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%
Continuidad de las operaciones	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%
Servicios financieros por Internet	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%
Descentralización de procesamiento en el exterior	Mayor o igual a 80%	Mayor o igual a 60% pero menor a 80%	Mayor o igual a 40% pero menor a 60%	Menor a 40%

De igual forma, durante el primer año de vigencia de la normativa y solo por este periodo, se utilizarán los siguientes valores para obtener el estado de la entidad, referente al área de Tecnología de Información.

ESTADO	CALIFICACIÓN GENERAL
Normal	Mayor o igual que 80%
Irregularidad 1	Mayor o igual que 60% y menor que 80%
Irregularidad 2	Mayor o igual que 40% y menor que 60%
Irregularidad 3	Menor que 40%

Una vez concluido este periodo, se utilizarán los valores establecidos en el Artículo 5 de esta normativa.

Artículo 38. Las entidades que a la entrada en vigencia de esta normativa, tengan vigentes contratos de procesamiento de datos externo, deberán incluir las condiciones establecidas en el Artículo 11 al renovar los contratos.

Artículo 39. La presente Normativa entrará en vigencia un año después de su publicación en el Diario Oficial “La Gaceta”.

Anexo 1

Matriz de Calificación

Esta matriz se utiliza para evaluar y calificar el entorno de Tecnologías de Información de las entidades fiscalizadas por la SUGEF. Específicamente, se trabaja sobre nueve áreas de evaluación, que en conjunto estructuran el entorno de TI.

Matriz de calificación de Tecnología de Información Institución: _____ Tipo de Entidad: _____ Período: _____ Hecho por: _____ Fecha: _____							
Área de Revisión	Objetivos	Calificación					
Administración de TI	6 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Evaluar la existencia de un plan estratégico en Tecnologías de Información acorde a los objetivos y estrategias de la Entidad.						
1	Evaluar la existencia de políticas y procedimientos orientados al mantenimiento de un programa de educación continua para los usuarios finales; así como un plan de capacitación según prioridades (presupuestado) para el personal del área de Tecnología de Información.						
1	Evaluar si los métodos y esquemas de trabajo facilita la consecución de los objetivos planteados.						
1	Evaluar si los miembros de la organización contribuyen al logro de los objetivos planteados.						
1	Evaluar si los mecanismos de control aseguran la realización y supervisión de las tareas.						
1	Verificar en caso que se subcontrate parte o la totalidad del procesamiento de la entidad en nuestro país, la existencia de una cláusula en el contrato que permita realizar una supervisión en las instalaciones del proveedor por parte de esta Superintendencia.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Seguridad lógica y acceso a datos	2 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Evaluar si la entidad posee una adecuada administración de la seguridad lógica de los recursos de TI.						

1	Evaluar la seguridad para todos aquellos puntos con acceso a redes públicas de datos.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Seguridad física	2 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Evaluar las políticas y procedimientos relacionados con la ubicación, construcción, acceso del centro de cómputo y comunicaciones.						
1	Evaluar las políticas y procedimientos de control que regulen las condiciones ambientales del centro de cómputo.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Sistemas de información	3 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Evaluar el diseño e implementación de sistemas de tal forma que se impida la modificación no autorizada de las aplicaciones.						
1	Evaluar la existencia de políticas y procedimientos que regulen la disponibilidad, capacidad y el desempeño de los sistemas de información.						
1	Evaluar la existencia de políticas y procedimientos de control para la entrada, proceso y salida de datos de los sistemas de información en producción.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Software y Bases de Datos	2 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Evaluar si existe una adecuada administración de las bases de datos de la entidad.						
1	Evaluar la existencia de políticas y procedimientos para la adecuada administración y mantenimiento (actualización) del Software con el fin de reducir sus vulnerabilidades.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Hardware , redes y comunicaciones	2 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación

1	Evaluar si existen políticas y procedimientos que permitan una adecuada administración del Hardware, redes y las líneas de comunicación.						
1	Evaluar si la entidad cuenta con políticas y procedimientos que permitan una adecuada administración de Cajeros Automáticos.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Continuidad de las operaciones	4 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Evaluar las políticas y procedimientos para el respaldo y recuperación de la información.						
1	Evaluar que la entidad cuente con un plan de continuidad del negocio, donde se detallen acciones, procedimientos y recursos que considere los riesgos posibles.						
1	Evaluar si la entidad cuenta con una infraestructura que contemple el suministro de energía eléctrica para la continuidad del negocio.						
1	Evaluar si la entidad cuenta con suficiente cobertura en seguros para los principales equipos de cómputo y comunicaciones.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Servicios Financieros por Internet	5 Puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Evaluar las condiciones legales y operativas bajo las cuales se brindará el servicio financiero por Internet.						
1	Evaluar si existen políticas y procedimientos que definan una adecuada administración de la seguridad lógica de los servicios financieros por Internet.						
1	Evaluar si el plan de continuidad del negocio considera un apartado donde se detalle las acciones, procedimientos y recursos que considere los riesgos posibles, que afecten de forma parcial o total la operativa normal de los servicios financieros por Internet.						
1	Evaluar la disponibilidad, capacidad y el desempeño de los servicios financieros por Internet.						
1	Evaluar la existencia de políticas y procedimientos de comunicación y advertencia a los clientes cuando estos abandonan el sitio web de la entidad y accesan el de un tercero.						

<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						
Descentralización de procesamiento en el exterior	5 puntos	C 100	PA 75	PB 35	NC 0	NA	Justificación
1	Comunicación a la Superintendencia.						
1	Cumplimiento de Normativa de TI vigente.						
1	Descentralización en el Plan de continuidad.						
1	Certificación del organismo supervisor en el sitio remoto.						
1	Informe de auditorías internas y externas traducidos al idioma castellano.						
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						

C: Cumple, la entidad muestra un excelente desempeño respecto al factor evaluado.

PA: Cumple Parcialmente Alto, la entidad muestra algunas deficiencias, pero en general el desempeño respecto al factor evaluado es bueno.

PB: Cumple Parcialmente Bajo, incumple significativamente con el factor evaluado.

NC: No Cumple, la entidad incumple con el factor evaluado.

NA: No Aplica, la evaluación de estos requerimientos.

Para calcular la Calificación General del Área de Tecnología de Información se utiliza la siguiente tabla:

<i>Tipo de entidad*</i>	<i>Fórmula</i>
1	$CG = \Sigma(\text{Total obtenido por Área})$
2	$CG = (\Sigma(\text{Total obtenido por Área}) * 100) / 93$
3	$CG = (\Sigma(\text{Total obtenido por Área}) * 100) / 93$
4	$CG = (\Sigma(\text{Total obtenido por Área}) * 100) / 86$

* Para consultar el detalle del tipo de entidad, consultar Artículo 5 de la Normativa de Tecnología de Información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras.

Así se concluye que la calificación de la entidad es: _____

Ejemplo:

Se puede apreciar en la siguiente tabla un modelo de cómo se utiliza esta herramienta:

Matriz de calificación de Tecnología de Información Institución: <u>Entidad Financiera 1</u> Tipo de Entidad: <u>4</u> Período: <u>Corte al 30 de junio de 2002</u>
--

Hecho por: <u>Supervisor 1</u> Fecha: <u>10/08/2002</u>							
Área de Revisión	Objetivos	Calificación					
Administración de TI	6 puntos	Cumple 100	PA 75	PB 35	NC 0	NA	Observaciones
1	Evaluar la existencia de un plan estratégico en Tecnologías de Información acorde a los objetivos y estrategias de la Entidad.	1					
1	Evaluar la existencia de políticas y procedimientos orientados al mantenimiento de un programa de educación continua para los usuarios finales; así como un plan de capacitación según prioridades (presupuestado) para el personal del área de Tecnología de Información.		1				
1	Evaluar si los métodos y esquemas de trabajo facilita la consecución de los objetivos planteados.	1					
1	Evaluar si los miembros de la organización contribuyen al logro de los objetivos planteados.	1					
1	Evaluar si los mecanismos de control aseguran la realización y supervisión de las tareas.		1				
1	Verificar en caso que se tercerice parte o la totalidad del procesamiento de la entidad en nuestro país, la existencia de una cláusula en el contrato que permita realizar una supervisión en las instalaciones del proveedor.					1	El procesamiento de la información se ejecuta internamente en las instalaciones de la entidad.
		3	2	0	0	1	
<i>Total Área</i>	(Total respuestas Cumple *100% + Total PA * 75% + Total PB * 35% + Total NC * 0) / (Valor Total de los puntos del área – el valor de los objetivos NA)						3 + 1.5 / 5 = 0.9

C: Cumple, la entidad muestra un excelente desempeño respecto al factor evaluado.

PA: Cumple Parcialmente Alto, la entidad muestra algunas deficiencias, pero en general el desempeño respecto al factor evaluado es bueno.

PB: Cumple Parcialmente Bajo, incumple significativamente con el factor evaluado.

NC: No Cumple, la entidad incumple con el factor evaluado.

NA: No Aplica, la evaluación de estos requerimientos.