Cuestionario de Autoevaluación anual
Sistemas de Información

Nombre de la Institución:

Tipo de Dinero Electrónico: General [ ] Especial [ ] Mixto [ ] Alimentación [ ]

Fecha:

Para cada punto mencionado a continuación, indicar si han existido modificaciones respecto al último documento/información presentada a BCU. En caso afirmativo, especificar cambios suscitados en forma detallada. Asimismo, mencionar frecuencia de las revisiones y última fecha de actualización.

(Se recuerda la obligatoriedad de autorización previa del Área Sistema de Pagos en caso de modificar las normas operativas internas, cuando se afecte el proceso o los procedimientos presentados para el trámite de autorización).

Políticas y Procedimientos de Seguridad de la información	¿Han existido modificaciones?		Frecuencia de revisión	Última fecha de actualización
	SI	NO		
a. Políticas de Seguridad Lógica		x		
b. Políticas de Seguridad Física		x		
c. Plan de Respaldos	x		1 x mes	1 semana
d. Plan de Recuperación de datos	x		1 x mes	
e. Plan de pruebas de seguridad de la información.		x		

Plan de continuidad del negocio	¿Han existido modificaciones?	Frecuencia de revisión	Última fecha de actualización

		Si	NO		
f.	Mapa de procesos de alto nivel (identificando procesos críticos)		X		
g.	Plan de contingencia para procesos críticos		X		
h.	Mapa de aplicaciones propias y de terceros, críticas y no críticas				
i.	Mapa de red y arquitectura de TI		X		
j.	Identificación de hardware crítico	X		Mi Computadoira	
k.	Líneas de comunicación redundantes		X		
l.	Datacenter de Contingencia		X		
m.	Sitio de Contingencia operativa		X		
n.	Estructura Organizacional para TI (incluye atención de desastres).		X		
ñ.	Plan de comunicación ante eventos anormales		X		
o.	Plan de pruebas de continuidad de negocio.		X		
p.	Plan de recuperación de servicios informáticos		x		
q.	Matriz de riesgos de la entidad.		X		

Tercerizaciones de Servicios				
	¿Han existido modificaciones?		Frecuencia de revisión	Última fecha de actualización
	Si	NO		

r.	Políticas de tercerizaciones de servicios (en caso de existir)		x		
s.	Contratos con Proveedores Actuales	x			4 Meses (Antel)
	Nota: -Se recuerda que deberá solicitarse autorización previa en las situaciones contempladas en el art. 83 de la RNSP.				

Especificación de cambios suscitados en literales a- s: (Deberá remitirse documentación actualizada al B.C.U., incluyendo resultado de pruebas periódicas de los planes.)

BCU

Complete la siguiente información sobre pruebas efectuadas, relativas a : seguridad de la información, continuidad de negocio y pruebas de carga y stress.

Pruebas efectuadas

	¿Está estipulada la ejecución de pruebas periódicas?		Frecuencia de ejecución	Última fecha de pruebas
	SI	NO		
Pruebas sobre seguridad de la información (hackeos éticos, tests de penetración, etc.)		x		
Pruebas sobre el plan de continuidad del negocio		x		
Pruebas de restauración de datos	x		1 x año	
Pruebas de estrés y capacidad del sistema		x		

Marco global de gestión de riesgos asociados a S.I.

Pregunta
1) ¿Cómo evalúa la dirección la cultura de control de la organización?
Ninguna Evaluacion
2) ¿Existe un proceso formal para el armado del presupuesto anual del área de tecnología? ¿Qué aspectos son tomados en cuenta en el mismo?
Ningun Presupuesto
3) ¿Qué mecanismos utiliza el Directorio para mantenerse informado respecto de los cambios experimentados en el mercado en materia tecnológica?
No aplica
4) ¿Se ha definido un comité de seguridad de la información, que permita implementar un adecuado gobierno de la seguridad de la información? ¿Qué mecanismos existen para asegurar el alineamiento

BCU

entre la estrategia de negocio y estrategia de seguridad de la información?
No APLICA
5) ¿Se cuenta con un responsable encargado de velar por el cumplimiento de la normativa aplicable?
No
6) ¿Existen los incentivos adecuados a nivel de Gobierno de TI para alinear el comportamiento de los usuarios hacia una cultura de trabajo que cumpla con los requerimientos de integridad, disponibilidad, confidencialidad, confiabilidad, efectividad y eficiencia de los procesos?
No
7) ¿Cuáles son los objetivos, indicadores y metas de confiabilidad operativa, tanto cualitativos como cuantitativos? ¿Dónde y cómo se encuentran documentados? ¿Cómo se garantiza la consecución de dichos objetivos?
No lo se
8) Comentar las características y frecuencia de las instancias de capacitación del personal respecto a: ***a) Operaciones internas (sistemas, procesos, aplicaciones utilizadas).*** ***b) Concientización desde el punto de vista de seguridad de la información y control interno.*** ***¿Se realiza para todo el personal? ¿Qué criterios existen para la gestión de la capacitación del personal?***
No se, no Aplica
9) Describa brevemente los mecanismos de control interno que se ejecutan para mitigar el riesgo de transacciones mal capturadas/imputadas/inválidas. ¿Se encuentran debidamente documentados? ¿Con qué frecuencia son actualizados los manuales y de qué forma son comunicados a la organización?
No Aplica
10) ¿Existe un departamento de auditoría interna dentro de la organización? En caso afirmativo, indique qué tipo de reportes emite, con qué periodicidad y a quién reporta sus conclusiones.
No Aplica
11) ¿Se han diseñado indicadores de alerta temprana sobre posibles debilidades en los procesos inherentes a la operativa? ¿Cuáles? ¿Con qué periodicidad se someten a revisión?

Por lo general se actualiza el software una ves que windows dice que se debe de actualizar 12) ¿Ha habido modificaciones en el último año, en la determinación de riesgos (operativos o tecnológicos, humanos o naturales, externos o internos) que podrían afectar a la organización? En caso afirmativo: ¿Qué riesgos nuevos se han identificado? ¿Se han incorporado a la matriz de riesgos global de la entidad? No
13) Describir los procedimientos que se realizan para determinar la adecuación de la capacidad actual de la infraestructura de TI respecto a los requerimientos no funcionales de sus sistemas. No Aplica 14) Describir cómo se realiza la proyección del aumento de la capacidad de procesamiento, almacenamiento y tráfico en términos de frecuencia y alcance. No hay respuesta
15) ¿Cuál es el criterio para identificar y valorar los riesgos asociados a la gestión de cambios a la infraestructura, aplicaciones y procesos?
16) Describir brevemente los mecanismos previstos en la Institución para controlar la adquisición e implementación de soluciones de TI (hardware y software), en forma autorizada. yo me fijo el hardware/software que es necesario.
17) ¿Cuál es el criterio para identificar y valorar los riesgos asociados al acceso no autorizado a datos o aplicaciones, relacionados con el Fondo de instrumentos de dinero electrónico y con la gestión del mismo? Cambio de Contrase;a y denuncia al banco y a la policia.
18) ¿Cuál es el criterio para identificar y valorar los riesgos asociados a la ocurrencia de incidentes de seguridad que tengan impacto en el fondo y en la gestión del mismo? No lo se
19) Describir brevemente el procedimiento para seleccionar proveedores de servicios, indicando la metodología utilizada, cláusulas estándar previstas y otros controles relacionados con la tercerización de servicios. Por lo general se ve confiabilidad, se ve el tipo de servicio y también respaldos del propio servicio. y Seguridad

Políticas y Procedimientos de seguridad de la información.

BCU

Pregunta
1) Opera o posee alguna certificación respecto al cumplimiento de algún estándar para la gestión o implementación de medidas de protección vinculados a la Seguridad de la Información (ej: PCI-DSS, ISO 27000, ISF, NIST, etc.)? No Aplica 2) ¿Cuáles son los activos de información críticos que posee? ¿Se encuentran inventariados y clasificados? ¿Cuál es la clasificación de activos de información utilizada por la institución? No Aplica 3) Listar las situaciones en las que se presenten problemas de segregación de funciones incompatibles (respecto a lo sugerido por las buenas prácticas y estándares internacionales), y la respuesta a este tipo de riesgos por parte de la institución. No Aplica
4) ¿Existe una declaración de riesgos residuales aprobada por los titulares de la institución? No
5) ¿Cuáles son los mecanismos previstos para la prevención de fraude, desde el punto de vista de los riesgos de seguridad de la información? No Hay
6) ¿La dirección entiende que los recursos con los que cuenta para la ejecución de actividades vinculadas con la seguridad de la información son suficientes para tratar los riesgos identificados de forma razonable para la misma? Explicar. No lo se. 7) ¿Cómo es la cultura de los empleados y personal contratado respecto a la ejecución formal de los controles vinculados a la seguridad de la información? ¿En qué medida se prioriza cumplir con los plazos y requerimientos funcionales sobre los requerimientos funcionales y de cumplimiento? No lo se
8) En caso de contar con software desarrollado a medida por un equipo in-house, describir brevemente la metodología y ciclo de vida de desarrollo de software. Mediante VPN se realiza la misma conexión. (NetVpn) 9) Proveer una copia del procedimiento actual de gestión de cambios a las aplicaciones e infraestructura.

No aplica **10) ¿Es obligatoria la definición de planes de vuelta atrás al momento de gestionar cambios a los sistemas? ¿Fue necesario ejecutar alguno de ellos últimamente? Explicar.** **No lo se** **11) ¿Cuántos cambios de emergencia se realizaron en el ambiente de producción en los últimos meses? En ese mismo período: ¿cuántos cambios se implantaron en producción? ¿Cuáles son las iniciativas para reducir el porcentaje de cambios de emergencia sobre el total?**
12) Explicar brevemente cómo se asegura de identificar los requerimientos de seguridad de la información, previamente al desarrollo de modificaciones en los sistemas que dan soporte a las aplicaciones críticas. **13) Explicar cuáles son las técnicas de testing de software utilizadas y los criterios de utilización de dichas técnicas, para la validación de los componentes de los sistemas críticos, previo a su instalación en producción.** **14) ¿Se realizan pruebas de validación de usuario final (UAT) previo a la instalación de los cambios en el ambiente de producción? Describir cómo se documentan y el alcance de dichas pruebas.**
15) Describir los controles de acceso lógico a nivel de redes, sistemas operativos, bases de datos o aplicaciones presentes en la infraestructura y en el software, que previenen la instalación de modificaciones a los programas, realización de ajustes de datos o cambios en la infraestructura física o virtualizada, de forma no autorizada. Para cada uno de los ambientes descritos en la información presentada, identificar cada uno de ellos (por ejemplo: producción, pre-producción, testing, desarrollo) y los controles de seguridad lógica y física implementados para controlar el pasaje de información entre los mismos. **16) Describir los procedimientos de monitoreo que existen sobre los controles descritos en la pregunta anterior, para corroborar que dichos controles se encuentran operando.** **17) Indicar los controles compensatorios utilizados para mitigar los riesgos asociados a no poder contar con una adecuada segregación de funciones incompatibles.**
18) Describir los procedimientos realizados para monitorear las conexiones desde y hacia redes externas. **19) Listar los dispositivos de red utilizados para detectar o prevenir intrusos en la red, indicando nombre, fabricante y versión de sistema.**

¿Se utilizan honeypots? En caso afirmativo, describir las medidas tendientes a tratar el riesgo de intrusión al interior de la red. NMAP, WIRESHARK 20) Describir los procedimientos previstos para reportar incidentes de seguridad y su escalamiento. ¿Se identifican las vulnerabilidades? ¿Se realiza seguimiento de las vulnerabilidades identificadas a modo de evaluar el riesgo asociado y definir su tratamiento? Se le avisa a la Policía.
21) ¿Se han definido adecuadamente las estrategias para la realización de pruebas de vulnerabilidades y hackeo ético? (ej: pruebas internas o externas, y pruebas de "caja blanca", "caja gris" o "caja negra"). No
22) ¿Cuáles son las medidas que ha tomado para capacitar y concientizar a los usuarios de los sistemas en relación a la posibilidad de ser víctimas de Ingeniería Social? ¿A los empleados? ¿A los proveedores? ¿A los clientes? Dentro de lo posible no tener anotado nada en ningún papel y en ese caso anotarlo hasta acordarse de memoria y luego triturarlo y quemarlo.
23) ¿Se estipula en la política de seguridad de la información, la necesidad de contar con un plan de continuidad de TI y con un Plan de Recuperación de desastres detallado para que pueda ser utilizado por técnicos de TI a efectos de recuperar los servicios? SI 24) ¿Se han definido los atributos de continuidad operativa de TI? (ej: RTO, RPO, ventanas de tiempo tolerables por cada proceso de TI).
25) Indicar las actividades de TI que se encuentran tercerizadas, los indicadores de desempeño establecidos para dichas empresas tercerizadas y los mecanismos de control implementados para verificar su cumplimiento en términos de actividades, frecuencia y responsabilidades. No

Plan de continuidad de Negocio

Pregunta

1) Considerando la última prueba realizada del plan, ¿considera que el diseño del plan se adecuó a la realidad? ¿Pudo ser probado en su totalidad sin necesidad de hacer ajustes? ¿Qué lecciones aprendidas surgieron en este sentido? **No**
2) Considerando la última prueba realizada del plan, ¿los roles y responsabilidades de cada parte se encontraban claros? ¿Cómo fue el desempeño de los procedimientos de prueba en este sentido? **No**
3) Considerando la última prueba realizada del plan, ¿se descubrió la existencia de procesos o actividades que no estuvieran cubiertas por no contar con un Plan de Continuidad actualizado? ¿Se tomaron las medidas correctivas? **No**
4) La ejecución de las pruebas del plan: ¿Tuvieron impacto en la operativa normal del negocio? ¿Qué lecciones aprendidas surgieron al respecto? **5) En las pruebas del plan: ¿cómo evalúa el desempeño de las partes involucradas en la ejecución de las actividades?** **No**
6) Listar y explicar lo sucedido en los incidentes de seguridad más significativos (con mayor riesgo asociado) que hayan ocurrido en los últimos 30-90 días. **No**
7) ¿El plan de contingencia de procesos críticos, es conocido por las personas que estarán involucradas en la ejecución del mismo en situación de contingencia? ¿De qué forma? **No** **8) ¿Cuál fue el resultado de la última instancia en la que se probó el plan de contingencia? ¿Fue posible considerar escenarios de indisponibilidad total de los servicios o infraestructura crítica del ambiente de producción? ¿Cuáles fueron las lecciones aprendidas?** **No**
9) En la última prueba del plan ¿Cómo reaccionaron los proveedores críticos de TI que se encontraban previstos para implementar

procesos de continuidad y/o recuperación de servicios de TI? ¿Se tomaron medidas para mejorar dicha respuesta?   **No**

Tercerizaciones de Servicios

Pregunta
1) ¿Se han contemplado los riesgos derivados de las tercerizaciones en la matriz general de riesgos de la entidad?   **No se han contemplado**   ***2) En caso de corresponder, ¿se han contemplado específicamente los riesgos derivados de la tercerización de múltiples actividades en un único proveedor?***
3) ¿Se establecen políticas de confidencialidad respecto a la información compartida con proveedores?   **Si**
4) ¿Se han tomado las medidas para asegurar la continuidad de los servicios que dependan de proveedores externos?   **No**   ***5) ¿Se realiza seguimiento del estado de situación de los proveedores externos para prevenir dificultades en la continuidad de la prestación del servicio?***   **No**
6) ¿Existen políticas documentadas en cuanto al relacionamiento con proveedores externos?   **No**   ***7) ¿Existen contratos nuevos con proveedores externos? Listar.***   **Antel, Nueva conexion. Avast Anti Virus**   ***8) ¿Se establecen acuerdos de nivel de servicios de terceros? ¿Cuáles?***

No

9) ¿Los contratos prevén garantía sobre el mantenimiento del servicio de proveedores externos?

Si, Antel provee un servicio.

10) ¿Cuáles son los mecanismos utilizados a la hora de evaluar posibles proveedores?

Precio, Seguridad y Opiniones

11) Alguno de los servicios brindados por terceros, ¿se encuentra fuera del país? Se ha definido claramente la legislación aplicable para la validez, interpretación y efectos de los contratos respectivos, en particular en lo referido a la protección de datos personales ?

No