Firmado digitalmente por:
ALEXANDER PASCUAL DE FEUDIS KOCKOVA
Área: RUC:20547367112
Empresa: TOC PERU S.A.C.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN EN LAS OPERACIONES

OID 1.3.6.1.4.1.53748.1.1.005

1 Identificación del Documento

Identificación del documento	Política de Seguridad de Información en las Operaciones
Documento(s) relacionado(s)	Procedimiento de Gestión de Incidentes, Problemas y Vulnerabilidades
Responsable de aprobación (anual)	Directorio - Comité de Riesgo
Dueño funcional	Gerente de Riesgo
Período de revisión	Anual
Actualización	Anual

2 Control de Versiones

Versión	Descripción del cambio	Solicitado por:	Realizado por:	Aprobado por:	Fecha Aprobación	Vigente a partir de:
1	Reemplaza Política AntiVirus y Política de Respaldo de Datos	CEO				

3 Objetivo

El propósito de este documento es definir, establecer e implementar controles y procedimientos que permitan prevenir, detectar, controlar, eliminar y corregir los problemas de confidencialidad, integridad y disponibilidad de información debido a la explotación tanto de vulnerabilidades propias de softwares o medios de procesamiento, como de copias o respaldos de seguridad de la información.

4 Alcance

Esta Política aplica a todos los procesos de la Empresa.

5 Referencias

- ISO/IEC Serie 27000

- Código del Trabajo
- Ley 18.845
- Cap 20-7 Recopilación Actualizada de Normas SBIF
- FEA, Ministerio de Economía

6 Definiciones

Información

Es un activo, al igual que otros activos comerciales importantes, esencial para la continuidad del negocio y en consecuencia necesita ser protegida adecuadamente. Como resultado del creciente flujo de información a través de las redes, "La Información" se expone a un número cada vez mayor y a una variedad más amplia de amenazas y vulnerabilidades.

Seguridad de la Información

Es la protección de la información (durante todo su ciclo de vida y en todos sus formatos) respecto de un rango amplio de amenazas, procurando asegurar la continuidad del negocio, minimizar el riesgo operacional y salvaguardar la imagen de la Empresa.

ISO/IEC 27002: 2013

Es un estándar en el cual se establecen las mejores prácticas para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

Software malicioso

También denominado "malware", incluidos los virus, gusanos, troyanos o ransomwares. Éstos ingresan a la red a través de correos electrónicos de los trabajadores, la utilización de Internet, computadoras portátiles o de dispositivos de almacenamiento, y explotan las vulnerabilidades del sistema.

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad, es un equipo multidisciplinario de especialistas en Seguridad de la Información, encargado de realizar las acciones necesarias para proteger, contener, controlar y erradicar un incidente de Seguridad de la Información.

Respaldo

Repositorio cuya finalidad es la preservación, protección y custodia de la información sujeta a requisitos de disponibilidad de largo plazo. Este repositorio puede estar implementado en diversas plataformas, por ejemplo en la nube, que garanticen la disponibilidad en tiempo y forma para cumplir con los requerimientos del negocio.

7 Normas

7.1 Gestión de cambios

- Debe existir un proceso formal para la gestión de cambios productivos sobre los sistemas de procesamiento (servidores, BD, aplicaciones, servicios webs, etc.).

- El Gerente de Operaciones y Tecnología, o a quien éste delegue, es responsable del proceso de gestión de cambios, independientemente de los proveedores que operen, ejecute o custodien los sistemas de procesamiento.

- El proceso de gestión de cambios deberá controlar al menos que:

  a. Exista documentación que justifique el cambio o puesta en producción, la cual puede corresponder a incidencias, mejoras, necesidades de negocio, etc.

  b. Existan las aprobaciones de las partes interesadas/impactadas con el cambio o puesta en producción.

  c. Exista evidencia de ejecución de pruebas a fin de verificar que el cambio no impacta negativamente en la seguridad del sistema.

  d. Exista documentado el procedimiento de desinstalación o vuelta atrás, en caso de tener inconvenientes con el cambio o puesta en producción.

  e. Exista por parte del Oficial de Seguridad de la Información, o de quien delegue, la aprobación de los requerimientos de seguridad de la información definidos para todo cambio y/o puesta en producción.

  f. Luego de aprobar y ejecutar un cambio mayor que afecte varios sistemas de procesamiento críticos, se realice una revisión del tipo hacking ético, para detectar vulnerabilidades que deben ser resueltas en el corto plazo.

7.2 Protección contra software malicioso

El Oficial de Seguridad de la Información, o a quien éste delegue, será responsable de implementar soluciones antimalwares (virus, troyanos, spyware, ransomware, etc.), para disminuir el riesgo y mitigar los impactos de infección, propagación y ejecución causada por ellos, en todos los sistemas que, generalmente, se ven afectados por estos softwares maliciosos (en especial, computadoras personales y servidores).

Las soluciones anti softwares maliciosos se deberán configurar de tal manera que se mantenga actualizado, previa confirmación de no impacto en el servicio, ejecute análisis periódicos y genere registros de auditoría. Para así pueda detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.

El Oficial de Seguridad de la Información, deberá:

a. Controlar periódicamente que los agentes de antivirus/antimalware funcionen activamente, se encuentren actualizados y que los usuarios no puedan deshabilitarlos ni alterarlos.

b. Implementar controles para la detección, prevención y recuperación ante afectaciones de software malicioso en combinación con la concientización adecuada de los usuarios.

c. Controlar que el registro de Log de la herramienta contra software malicioso, se mantenga habilitado.

d. Ejecutar periódicamente y en forma automática un escaneo antivirus/antimalware completo en los equipos.

e. Monitorear la vigencia del contrato con el proveedor de la herramienta contra software malicioso para asegurar que el software instalado se mantenga actualizado.

El Oficial de Seguridad de la Información, ante incidentes de seguridad de la información a causa de software malicioso, deberá:

a. Analizar la magnitud daños causados por acción del software malicioso.

b. Registrar cantidad de equipos afectados, alcance del software malicioso, consecuencias, y fecha de ocurrencia del evento.

c. Evaluar la integridad de los archivos y/o programas, luego de la eliminación del software malicioso.

d. Investigar para determinar responsables del incidente.

e. Evaluar casos de contaminación reiterada, para adoptar medidas y evitar reincidencias.

El Oficial de Seguridad de la Información debe:

a. Capacitar y concientizar a los usuarios sobre los riesgos de pérdida de información por efecto de softwares maliciosos y comunicarles la metodología definida para combatirlos.

b. Ser el único ente válido para comunicar información de alertas o incidentes relacionados con software malicioso.

c. Ante una contaminación masiva, deberá ser tratado según lo dispuesto en el plan de recurperacion de desastres.

Instalación en Estaciones de Trabajo

Se debe instalar un producto anti-virus en todas las estaciones de trabajo

Educar a los usuarios en cómo actualizar el software anti-virus, cuando este proceso no es centralizado.

Todo usuario que detecte la existencia de un virus, debe notificar a la brevedad su existencia al administrador de red o mesa de ayuda.

Instalación de GateWay Antivirus sobre Mail Relay

Para chequear los mensajes de correo electrónico entrantes y salientes, se debe instalar y configurar un Mail Relay como Gateway Anti-virus.

Se debe definir un conjunto de extensiones de archivos anexos en los correos que no son permitidos de ingresar/salir por el GateWay o Firewall.

Instalación Anti-virus en estaciones de trabajo

Configuración recomendada para el software Anti-Virus:

Habilitar Full-Time, background, real time, auto-protect o modo similar

Habilitar Start-Up Scanning de memoria, registros master/boot, archivos de sistema El

log debe estar habilitado para toda la actividad relacionada con virus.

Está prohibido cambiar la configuración o deshabilitar el software anti-virus, sin la autorización del área de Sistemas.

Usar controles heurísticos de software antivirus.

Usar herramientas que impidan la ejecución sin advertencia de archivos adjuntos a los mensajes electrónicos.

7.3 Registro de actividad de usuarios

- Se deberán implementar mecanismos necesarios para registrar y rastrear las actividades de los usuarios, con la finalidad de prevenir, detectar y minimizar posible impactos sobre la información.
- Mientras las tecnologías lo permitan, se deberán mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y otros eventos de seguridad de la información.
- El Gerente de Operaciones y Tecnología, o a quien éste delegue, será responsable de implementar correctamente los registros (Logs) de auditoría en todos los componentes de sistemas, para vincular todo acceso a componentes del sistema con usuarios específicos.
- Los registros (Logs) deben configurarse de tal forma que se puedan reconstruir los siguientes eventos:

  a. Accesos de usuarios a información clasificada como confidencial o secreta.

  b. Acciones realizadas por usuarios con altos privilegios o privilegios de administración.

  c. Intentos de acceso lógico no autorizados.

  d. Creación de nuevas cuentas.

  e. Aumento de privilegios, cambios, incorporaciones y eliminaciones de cuentas con altos privilegios o privilegios de administración.

f. Inicialización, detención o pausa de los registros de auditoría.

g. Creación y eliminación de objetos en el nivel del sistema.

• Cada evento registrado debe contar las siguientes entradas para auditoría:

A. Identificación de usuarios.

A. Tipo de evento.

A. Fecha y hora.

B. Indicación de éxito o fallo.

C. Origen del evento.

D. Identidad o nombre de los datos, componentes del sistema o recursos afectados.

• Se deben implementar los controles necesarios para proteger contra posibles alteraciones y accesos no autorizados la información de los Logs.

• Se deben realizar copias de seguridad de los archivos de Logs de manera oportuna en servidores de registros centralizados que sean difíciles de modificar, los cuales se deben conservar por al menos un año.

• El Oficial de Seguridad de la Información, o a quien éste delegue, es responsable de:

a. Implementar mecanismos de detección oportuna de fallas de los sistemas de control de seguridad de la información (Firewalls, IDS/IPS, Antivirus, etc.).

b. Implementar los procedimientos necesarios para responder de forma oportuna ante fallas de los sistemas de control de seguridad de la información.

7.4 Gestión de la vulnerabilidad técnica

7.4.1 Vulnerabilidades

El Oficial de Seguridad de la Información es responsable de:

a. Definir y formalizar un proceso o procedimiento para la gestión de vulnerabilidades. El cual debe constar de la identificación, asignación de clasificación de riesgo (alto, medio, bajo) y mitigación de las vulnerabilidades (plazo: 30 días para altas y 90 días para medias). Debido a la inexistencia de riesgo o riesgo muy bajo, el cual es asumido por la organización, las vulnerabilidades categorizadas como informativas o bajas deben ser descartadas del plan de mitigación.

b. Definir las direcciones IP que deben incluir los análisis de vulnerabilidades.

c. Realizar análisis, a lo menos trimestral, de vulnerabilidades sobre plataformas tanto internas como externas, estaciones de trabajo y dispositivos de comunicaciones y seguridad.

d. Realizar revisiones del tipo hacking ético, tanto a nivel interno como externo de las plataformas, al menos una vez al año.

e. Utilizar fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad

f. Establecer como parte de los requerimientos de seguridad, que se realice una revisión de seguridad a los productos o aplicaciones antes de enviarlo a producción o de ponerlo a disposición de los clientes. Asimismo, controlar que las vulnerabilidades detectadas sean mitigadas antes de la puesta en producción.

g. Definir estándares de desarrollo seguro de sistemas de información. Y controlar su correcta implementación.

El Gerente de Operaciones y Tecnología, o a quien éste delegue, es responsable de:

a. Implementar, los lineamientos de desarrollo seguro según los estándares vigentes.

b. Capacitar a los desarrolladores ya sean interno o externos, por lo menos anualmente, en las técnicas de desarrollo seguro.

7.4.2Parchado

El Gerente de Operaciones y Tecnología, o a quien éste delegue, es responsable de:

a. Definir y formalizar un proceso o procedimiento para la gestión de parches de seguridad.

b. Mantener implementados los parches de seguridad que ofrecen protección contra vulnerabilidades conocidas, sobre todo software y componente del sistema.

c. Que todo parche importante o crítico debe ser analizado e implementado prioritariamente dentro de un mes desde la publicación.

7.4.3Configuración de Seguridad

El Oficial de Seguridad de la Información, o a quien éste delegue, es responsable de:

a. Desarrollar estándares de configuración de seguridad para todos los componentes de sistemas, que concuerden con las mejores prácticas de seguridad de sistemas aceptadas en la industria, o en su defecto, adoptar las recomendaciones del fabricante.

b. Mantener actualizados los estándares de configuración de seguridad a medida que se identifiquen nuevas vulnerabilidades.

c. Controlar que toda puesta en producción de componentes de sistemas cumplan con los estándares de configuración de seguridad definidos.

d. Controlar periódicamente que la configuración de seguridad de los componentes de sistemas, cumplan con los estándares vigentes.

El Gerente de Operaciones y Tecnología, o a quien éste delegue, es responsable de implementar y/ mantener correctamente, en todos los componentes de sistemas, la configuración definida en los estándares vigentes.

7.5 Respaldos o copias de seguridad de la información

7.5.1 Respaldos de información

A. Debe existir un proceso formal para la generación, transporte, custodia, mantención y control de respaldos de información, de sistemas de procesamiento (servidores).

B. El Gerente de Operaciones y Tecnología, o a quien éste delegue, es responsable del proceso de respaldo de información digital, tanto de la correcta ejecución de respaldos como del control de disponibilidad e integridad de ellos. Independientemente de los proveedores tecnológicos que operen, ejecuten o custodien los respaldos.

C. Todo respaldo se debe almacenar alejado de los sitios de procesamiento y seguro tanto desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, como de su seguridad física y lógica.

D. Todo envío de cajas de almacenaje con respaldos de documentación física, para almacenamiento externo, deben ser entregados el detalle de los respaldos que lleva la caja de almacenaje. Dicho detalle debe permanecer en el interior de la caja para posteriormente sellarla con los sellos de seguridad definidos.

E. Debe existir un registro histórico de respaldos de documentación física, que se encuentran actualmente bajo custodia interna, externa o que han estado bajo esta última. Esto para mantener un control sobre la asignación, custodia, reciclaje, y eliminación/destrucción de documentación, según corresponda, para así obtener datos estadísticos.

A. El Gerente de Administración y Finanzas, o a quien delegue, es responsable de mantener el registro histórico de información física respaldada y almacenada externamente.

B. El Gerente de Operaciones y Tecnología, o a quien delegue, es responsable de mantener el registro histórico de los respaldos de información electrónica almacenados externamente.

7.5.2 Respaldos de información electrónica

A. El proceso de respaldo se debe realizar en horarios adecuados, de tal forma que no afecten el funcionamiento sistemático de la operatoria.

B. El explotador debe verificar que todo respaldo programado haya finalizado correctamente una vez haya concluido el proceso.

C. Todo respaldo generado debe ser revisado y probado antes de eliminar la información de los equipos de procesamiento, con el fin de comprobar que los datos respaldados estén disponibles e íntegros.

D. Los respaldos en medios electrónicos no deben ser alterados, modificados, borrados ni intervenidos.

E. El Gerente de Operaciones y Tecnologías es responsable de verificar periódicamente si los respaldos se ejecutaron correctamente.

F. El Gerente de Operaciones y Tecnologías es responsable de realizar periódicamente verificaciones aleatorias a los respaldos electrónicos, efectuando una recuperación para comprobar que la información haya quedado correctamente respaldada.

G. Debe existir un registro de la información electrónica que haya presentado errores en el proceso de respaldo, para luego verificar si se reintentó y corrigió el error.

H. Toda copia de datos desde producción, ya sea directamente desde los medios de procesamiento o desde un respaldo, para fines distintos a los usos en ambiente productivo, debe ser autorizada formalmente por el correspondiente propietario de la información.

7.5.3Frecuencia y período de retención (* plazos dispuestos en Normativa Externa)

A. La generación de respaldo debe obedecer a una necesidad de continuidad operacional (por contingencias) y/o la necesidad de recuperación por diversos motivos (solicitud de alguna autoridad administrativa o judicial, emisores, comercios, etc.).

C. Independiente de la vigencia de los respaldos definida, se prohíbe destruir documentos o información que tenga relación directa o indirecta con operaciones, negocios, asuntos o litigios vigentes.

D. La frecuencia en todos los casos estará dada por la necesidad del negocio:

Frecuencia	Descripción	Periodo Retención
Diario	LOG TOC METER	6 años
Mensual	Registro de Enrolamiento de FEA en papel	6 años
Una vez	LLaves en PKI	6 años
Diario	CRL , Listas de Revocacion de Certificados	6 años

7.5.4Consideraciones

7.5.4.1 Conservación de originales

A. Registro de Enrolamiento de Certificados de Firma Electrónica Avanzada en papel.

B. Libros, documentos y correspondencia que digan relación directa o indirecta con operaciones que mantengan registradas en su contabilidad o con algún asunto o litigio pendiente.

A. Libros de actas de juntas de accionistas, de sesiones de directorio o comités resolutivos.

B. Antecedentes necesarios para certificar el tiempo servido y la renta percibida por los trabajadores.

C. Todo documento relacionado con la historia institucional de la Empresa.

7.5.4.2 Información Financiero Contable – Tributaria de la Empresa

A. Libros, formularios, correspondencia, documentos y papeletas. El plazo de conservación será desde la fecha del último asiento operado en los respectivos documentos o archivos o desde la fecha en que se haya extendido según sea el caso.

E. No podrá ser eliminada información de operaciones, negocios o asuntos vigentes o pendientes que correspondan a:

a. Solicitudes relacionadas con emisión o entrega de documentos;

b. Copias de estados de cuentas;

c. Copias de traspasos contables;

d. Libros o estados de cuenta subsidiarios o auxiliares.

F. Podrán ser eliminados, siempre y cuando se trate de operaciones, situaciones o asuntos concluidos o finiquitados previamente micrograbadas o microcopiadas y que no sea necesario conservar el original, documentación correspondiente a:

a. Duplicados de recibos o de comprobantes de depósitos en cuenta corriente o en otras cuentas a la vista o a plazo;

b. Traspasos de acciones;

c. Copias de contratos, convenios y correspondencia de distinta naturaleza.

7.5.4.3 Información Laboral

A. Mientras la relación laboral se mantenga vigente, no pueden destruirse los documentos. Una vez finalizada una relación laboral, la información y/o documentación que dan cuenta de ella deben ser mantenidos por el período definido.

A. En caso que documentos den cuenta de una obligación tributaria de la empresa, sea en relación a su calidad de agente retenedor de impuesto o como sustento de un gasto necesario para producir la renta, deben ser mantenidos según los plazos tributarios.

7.5.4.4 Información Propia del Procesamiento de Transacciones

A. El plazo de permanencia será el definido caso a caso en el contrato con cada cliente, y la necesidad de los procesos de negocio.

7.5.5 Reutilización y/o destrucción de medios de respaldo

A. Toda destrucción de documentación respaldada en papel, debe realizarse de manera controlada, previa autorización del dueño de la misma. Incorporando en el registro histórico: la fecha y método

de destrucción, así como las partes que asistieron a la actividad en calidad de observadores del proceso.

B. El área de finanzas es la responsable de definir si los dispositivos desincorporados ya no contarán con vida útil para las actividades de TOC BIOMETRICS, por lo cual será el área encargada de solicitar la destrucción de los equipos desechados.
C. El área de soporte y seguridad de la información deberán definir, actualizar y ejecutar los procedimientos de destrucción de medios tecnológicos lógicos o físicos que llegasen a contener información sensible para TOC BIOMETRICS

7.5.6 Restauración y pruebas a los de respaldos

Como responsable del proceso de respaldos, el Gerente de Operaciones y Tecnología, o a quien éste delegue, debe velar para que:

A. Se realicen pruebas de restauración de respaldo a los equipos de procesamiento, teniendo en cuenta las necesidades de contar con la información operativa en línea de acuerdo a los requerimientos específicos del negocio.

G. Se realicen pruebas periódicas en aquellos respaldos que por su naturaleza no son requeridos frecuentemente o aquellos que poseen información de sistemas críticos para el negocio, con el fin de asegurar la disponibilidad de la información.

H. Todos los resultados de pruebas deben ser registrados.

I. Sólo personal autorizado solicite respaldos de información o la recuperación de los mismos, obedeciendo siempre a requerimientos del negocio debidamente justificados.

Se define como motivos justificados para la restauración a: contingencias, actividades de análisis de procesos y pautas, atención de solicitudes de clientes o entes reguladores o pérdida de correo electrónico de usuarios internos.

J. La información correspondiente a la recuperación de respaldos sea ser incorporada en el registro histórico: motivo, destinatario, fecha y hora de la entrega y recepción, además de la firma del solicitante.

K. Sólo personal autorizado pueda tener acceso a datos restaurados con información confidencial.

8 Aprobaciones

La presente Política ha sido aprobada por …..