**2019**

**Proyecto:**

**Implementación de SGSI en el área de TI.**

**TCI S.A.**

Soluciones Informáticas

Empresa dedicada al desarrollo de sistemas informáticos concernientes a Facturación Electrónica y Operaciones Aduaneras.

1. **OBJETIVO**
   1. Objetivo General

Establecer un sistema de gestión de seguridad de la información que permita al área de TI en TCI a proteger la confidencialidad de la información, asegurando que sea accesible a los clientes, colaboradores y terceros con una legítima necesidad de saber salvaguardando la integridad de la información para garantizar su exactitud y totalidad, además, mantener la disponibilidad de la información y los sistemas de información que soportan los procesos de TCI.

* 1. Objetivo Específico

Establecer políticas, normas y procedimientos que permitan el intercambio de información entre las distintas áreas de manera segura sin dejar de lado la confidencialidad.

Establecer reglas concisas para cada actor dentro de la organización TI con el fin de prevenir riesgos y vulnerabilidades que puedan afectar el prestigio y confianza establecida en la empresa.

Establecer estándares de trabajo mediante las políticas.

1. **ALCANCE**

Aplica al área de TI y su interacción con los clientes externos. Los puntos principales son:

* Gestión de Aplicaciones
* Administración e Implementación de proyectos
* Gestión de Incidentes
* Gestión de Infraestructura

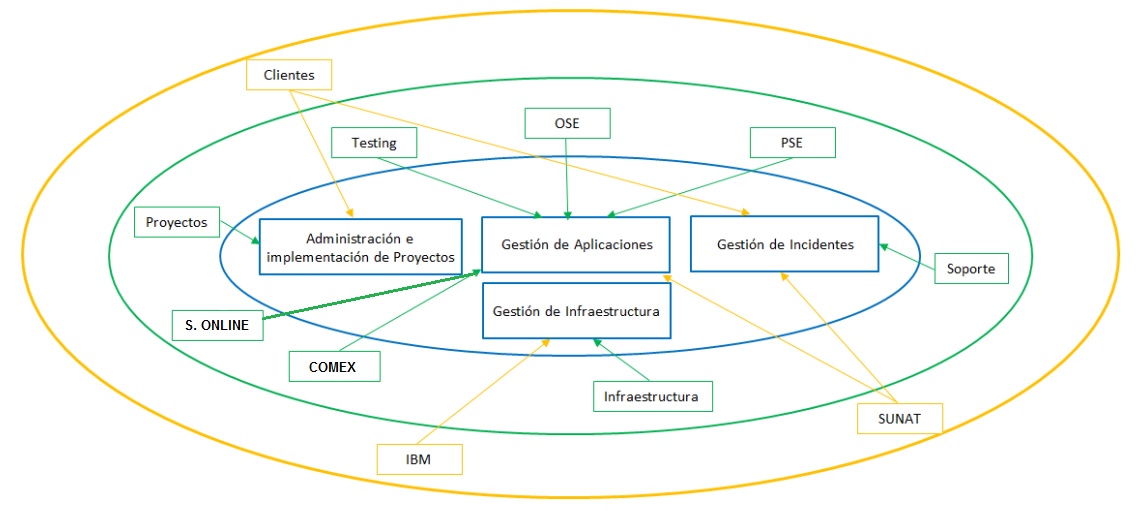
Los activos que maneja el área de TI son:

* Información Física: documentos físicos.
* Información Electrónica: documentos electrónicos.
* Software: sistemas operativos, aplicaciones.
* Hardware: servidores, dispositivos de comunicación.
* Servicios: housing.
* Medios de almacenamiento: memorias, discos duros externos, CD.
* Sitios o ambientes: data center.
* Personal.

1. **MARCO LEGAL**

|  |  |
| --- | --- |
| **Norma, Estándar, Protocolo** | **Descripción** |
| Ley de protección de datos personales, ley N° 29733 | Tiene por objeto garantizar el derecho fundamental de las personas a la protección de su privacidad, para lo cual prescribe que el tratamiento de sus datos personales sea proporcional y seguro. |
| Constitución Política del Perú | Que, el numeral 6 del artículo 2 de la Constitución Política del Perú reconoce el derecho que toda persona tiene a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar |
| ISO/IEC 13335-1:2004 | Presenta los conceptos y modelos fundamentales para una comprensión básica de la seguridad de las TIC, y aborda los problemas generales de administración que son esenciales para la planificación, implementación y operación exitosas de la seguridad de las TIC. |
| ISO/IEC 27005:2011 | Proporciona directrices para la Gestión de Riesgos en Tecnologías de la Información. La norma ISO 27005 no especifica ni recomienda ningún método específico de análisis de riesgos, aunque es cierto que especifica un proceso estructurado, sistemático y riguroso desde el análisis de riesgos hasta la creación del plan de tratamiento de riesgos |
| ISO/IEC 31000:2009 | Gestión de Riesgos |
| ISO/IEC 27001:2013 | Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. |
| ISO/IEC 27002:2005 | Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. |
| ISO/IEC 27002:2013 | Consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones. ISO/IEC 27002:2005 tenía 11 secciones principales mientras que ISO/IEC 27002:2013 ahora tiene 14. Estas nuevas secciones analizan la criptografía, la seguridad de las comunicaciones y las relaciones con los proveedores (secciones 10, 13 y 15, respectivamente). |

1. **ESTRUCTURA ORGANIZATIVA**



1. **TERMINOLOGIA BASICA**

A continuación, se definen algunos conceptos que deben estar claros para seguir abordando el presente documento sin errores de interpretación.

1. Activo de información: Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.
2. Accesos no autorizados: consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o contraseñas, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.
3. Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
4. Análisis de riesgos: uso sistemático de la información para identificar fuentes y estimar el riesgo.
5. Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.
6. Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
7. Caballo de Troya: es un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera que permite la administración remota a un usuario no autorizado.
8. CID: Acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información
9. Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, basado en el principio de la “necesidad de conocer”.
10. Control: Acción tomada con la finalidad de reducir la frecuencia o impacto de un riesgo inherente a los procesos de la organización.
11. Correos maliciosos: La intención de estos correos es aprovecharse de nuestro desconocimiento, ingenuidad o buena voluntad para obtener información que si nos pidiesen directamente no les daríamos. Información que puede ir desde conseguir las cuentas de correo electrónico de nuestros contactos hasta nuestros datos bancarios.
12. Disponibilidad: Acceso a la información por parte de los usuarios autorizados cuando lo requieran.
13. Evaluación de riesgos: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
14. Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.
15. Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos y actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
16. Impacto: El costo para la organización de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros, por ejemplo, pérdida de reputación, implicaciones legales, entre otros.
17. Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
18. Infección de virus: es un software que tiene por objetivo de alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias o imprevistos.
19. Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
20. Inventario de activos: Lista de todos aquellos recursos (de información, software, hardware, servicios, personas, instalaciones, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
21. ISO/IEC 27001: Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).
22. Log: log, historial de log o registro, se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).
23. Nivel de Riesgo: Indicador que se obtiene de la combinación del impacto y la frecuencia.
24. Plan de tratamiento de riesgos: Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
25. Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.
26. Propietario: Identifica a la persona que tiene responsabilidad aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
27. Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
28. Riesgo Inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
29. Riesgo Residual: Nivel de riesgo que subsiste luego de evaluar controles existentes.
30. Riesgo después del tratamiento: Nivel de riesgo que subsiste luego de implementar los controles propuestos.
31. Rootkits: Es un programa que se encarga de borrar o enmascarar las huellas dejadas después de introducirse en un sistema. Estas huellas se encuentran en los ficheros guardando todas las operaciones hechas por un usuario (entrar, salir, ejecutar un programa, etc.).
32. Seguridad de la Información: Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.
33. Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
34. Sniffer: Programas encargados de interceptar la información que circula por la red. Por ejemplo: Cuando un usuario entra en un sistema, tiene que dar usuario y clave de acceso. Estos datos viajan para ser comprobados con el fichero de contraseñas y ahí es donde el sniffer actúa, intercepta estos datos y los guarda en un fichero para su utilización posterior de forma fraudulenta.
35. SGSI: Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).
36. Tratamiento de riesgos: Proceso de selección e implementación de medidas para modificar el riesgo.
37. Valoración de riesgos: Proceso completo de análisis y evaluación de riesgos.
38. Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.
39. **ROLES, RESPONSABILIDADES Y AUTORIDAD DE LA ORGANIZACIÓN**

En concordancia con la distribución de personas y actividades, a continuación, se indican los roles y responsabilidades de los involucrados en el Sistema de Gestión de Seguridad de la Organización:

* 1. Gerente General: Con respecto al sistema de Gestión de Seguridad de la Información, tiene las siguientes funciones y responsabilidades:
     1. Brindar su apoyo y compromiso con el Sistema de Gestión de Seguridad de la Información (SGSI) de TCI.
     2. Aprobar la política de seguridad de la información, así como velar por su publicación y distribución.
     3. Aprobar el alcance, los manuales, metodologías, plan de capacitación y concientización del SGSI y políticas relacionados al SGSI de TCI.
     4. Nombrar al Comité de Gestión de Seguridad de la Información (CGSI).
     5. Definir las funciones, asignar responsabilidades y la rendición de cuentas y, delegar autoridad y responsabilidad a cada una de las áreas para el cumplimiento de la política y objetivos.
     6. Asegurar la disponibilidad de los recursos (humanos, de infraestructura, financieros y tecnológicos), mediante la aprobación del presupuesto de los proyectos relacionados con el SGSI
  2. Comité de Gestión de Seguridad de la Información (CGSI): Con respecto al Sistema de Gestión de Seguridad de la Información, tiene las siguientes funciones y responsabilidades:
     1. Asegurar que los objetivos de seguridad de la información estén identificados, cumplan con los requerimientos organizacionales y estén integrados en los procesos relevantes.
     2. Asegurar que el sistema de gestión de seguridad de la información este conforme a los requisitos de la Norma Técnica Peruana.
     3. Revisar el Sistema de Gestión de Seguridad de la Información.
     4. Asegurar que la implementación de los controles de la seguridad de la información es coordinada a través de TCI.
     5. Revisar los procesos de auditoría interna y externa de forma periódica.
     6. Velar por el cumplimiento de las políticas y procedimientos de seguridad de la información.
     7. Decidir el criterio para la aceptación de riesgos y oportunidades de seguridad de la información y los niveles de riesgo aceptables.
     8. Establecer la Medición del Sistema de Gestión de Seguridad de la Información, involucrando a las partes interesadas pertinentes en las actividades de medición, aceptar los resultados de las mediciones como insumos para la revisión por la dirección y utilizar los resultados de las mediciones en actividades de mejora del SGSI.
     9. Monitorear el cumplimiento de la mejora continua del Sistema de Gestión de Seguridad de la Información.
     10. Otras que considere necesario el Gerente General.
  3. Oficial de Seguridad de la Información: Con respecto al Sistema de Gestión de Seguridad de la Información, tiene las siguientes funciones y responsabilidades:
     1. Dirigir, coordinar y controlar todas las actividades relacionadas con la Seguridad de la Información de TCI.
     2. Liderar y velar por el desarrollo, implementación, mantenimiento y cumplimiento de políticas y procedimientos para promover la seguridad de la información.
     3. Coordinar y proponer la agenda de las sesiones del Comité de Gestión de Seguridad de la Información.
     4. Registrar en actas lo actuado por el Comité de Gestión de Seguridad de la Información.
     5. Custodiar los registros de los acuerdos tomados en las sesiones del Comité de Gestión de Seguridad de Información.
     6. Liderar el proceso de gestión de incidentes de seguridad de la información.
        1. Analizar los incidentes de seguridad reportados:
        2. Registrar incidente en la Bitácora de Incidentes.
        3. Evaluar y tomar una decisión sobre los incidentes de seguridad reportados.
        4. Hacer seguimiento a los incidentes de seguridad reportados.
        5. Planificar y preparar una respuesta sobre el incidente al usuario correspondiente.
     7. Liderar la realización de actividades orientadas al análisis y evaluación de riesgos y oportunidades de seguridad de la información periódicos, a fin de mantener un conocimiento actualizado de las amenazas y vulnerabilidades.
     8. Monitorear la efectividad y eficiencia de los controles implementados para la protección de los activos de información.
     9. Promover la difusión y apoyo a la seguridad de la información dentro de TCI.
     10. Proponer planes y programas de concientización en materia de seguridad de la información y, capacitar en forma constante y continua a todo el personal de TCI.
     11. Asesorar a las distintas áreas de TCI en temas relacionados a seguridad de la información.
     12. Apoyar en la revisión gerencial del SGSI y necesidades de mejora.
     13. Promover y hacer seguimiento de la mejora continua.
     14. Realizar el seguimiento de las acciones correctivas.
     15. Apoyar en la planificación y realización de las auditorias del SGSI.
     16. Elaborar los informes de gestión del SGSI, para su revisión por el Comité de Gestión de Seguridad de la Información.
     17. Elaborar y cuando corresponda revisar, los documentos referidos a la seguridad de la información.
     18. Monitorear cambios significativos en la empresa que puedan poner en riesgo los activos de información del TCI.
     19. Informar a la gerencia y al Comité de Seguridad de Información, sobre el desempeño del SGSI
  4. Propietario de Riesgos: Con respecto al Sistema de Gestión de Seguridad de la Información, tiene las siguientes funciones y responsabilidades:
     1. Aceptar los riesgos asociados a la seguridad de la información, así como solicitar el apoyo de las áreas pertinentes para evaluar dichos riesgos y establecer medidas de mitigación.
     2. Aprobar el plan de tratamiento de riesgos y la aceptación de los riesgos residuales de la seguridad de la información.
  5. Propietario de Activos: Con respecto al Sistema de Gestión de Seguridad de la Información, tiene las siguientes funciones y responsabilidades:
     1. Participar en los procesos de identificación y clasificación de activos de información, siguiendo el procedimiento formal definido.
     2. Autorizar la asignación de accesos sobre la información.
     3. Autorizar los cambios sobre los activos de información de su propiedad.
  6. Gerentes y/o jefes: Con respecto al Sistema de Gestión de Seguridad de la Información, tienen las siguientes funciones y responsabilidades:
     1. Apoyar en la difusión de las políticas y procedimiento de seguridad de la información de TCI al personal bajo su cargo, para asegurarse que las conozcan y comprendan que el incumplimiento de las mismas podría resultar en una acción disciplinaria.
     2. Comunicar requerimientos de control y protección de la información al Oficial de Seguridad de la Información y asegurar que la información y recursos bajo su control estén debidamente protegidos por las medidas de seguridad adecuadas.
     3. Apoyar y facilitar las revisiones periódicas para la verificación del cumplimiento de las políticas y procedimientos de seguridad de la información.
     4. Determinar los criterios y niveles de acceso a la información de la cual son responsables y notificar el cambio de función/ubicación de cualquier personal de TCI sea por reasignación o retiro, con la finalidad de modificar o cancelar sus accesos.
     5. Reportar inmediatamente el incumplimiento o infracciones a las políticas y normas de seguridad.
     6. Aprobar y revisar todos los procedimientos y formatos del SGSI que le correspondan.
  7. Personal de TCI: Con respecto al Sistema de Gestión de Seguridad de la Información, tiene las siguientes funciones y responsabilidades:
     1. Conocer, comprender y cumplir las políticas y procedimientos de seguridad de la información de TCI.
     2. Identificar y notificar incidentes y riesgos de seguridad de la información al jefe inmediato superior y/o al Oficial de Seguridad de la Información.
     3. Utilizar la información, sistemas y todos los recursos de TCI únicamente para los propósitos autorizados e inherentes a la función asignada.
     4. Mantener la confidencialidad e integridad de la información que circula al interior de TCI.
     5. Reportar incumplimientos de seguridad de la información.
  8. Terceros o Proveedores:
     1. Deben cumplir las cláusulas incluidas dentro de los contratos o acuerdos de confidencialidad, que están referidas a salvaguardar la confidencialidad, integridad y disponibilidad de la información de TCI.
     2. Deben brindar todas las facilidades necesarias para que TCI revise el cumplimiento de las condiciones incluidas en los contratos de los servicios brindados; así como también aspectos de seguridad de la información de los servicios.
     3. Identificar y notificar incidentes y riesgos de seguridad de la información al Oficial de Seguridad de la Información.

1. **LINEAMIENTOS**
   1. Existe un oficial de seguridad en la empresa que se encargará de controlar y proponer acciones de mejora en el SGSI.
   2. En caso de incurrir en una falta que sea adverso a las políticas, la empresa podrá tomarse la libertad de acudir a los acuerdos que fueron firmados en su momento por el personal en falta, estos documentos podrían tener hasta cargos de denuncia; estos documentos dependiendo el área podrían ser entre:
      1. Documento de Acuerdo de Confidencialidad
      2. Documento de Acuerdo de Cumplimiento.
   3. Las políticas deben ser difundidas y aplicadas entre el personal con el fin de transformarlos en hábitos y buenas prácticas.
   4. Todos los equipos y documentos a los cuales un personal acceda deben estar debidamente documentados con cargos; las mismas podrán ser objeto de control y monitoreo.
   5. Las propuestas de mejoras se presentan al Oficial de Seguridad de la Información para su evaluación. De ser viable, designa al jefe e integrantes del proyecto, solo en caso de que se requiera una inversión de recursos y/o adquisición de TI, el Oficial de Seguridad de la Información solicitará al Comité de Gestión de Seguridad de la Información su aprobación. El proyecto deberá indicar el responsable y fecha de cumplimiento de cada actividad, así como los recursos necesarios, de ser el caso.
2. **DECLARACION DE POLITICAS**
   1. Política de Seguridad de la Información

La empresa TCI S.A se encuentra comprometida con:

1. Proteger los activos de información frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar su confidencialidad, integridad, disponibilidad de la misma.
2. Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control necesarias para evitar que los riesgos de la seguridad de la información se materialicen.
3. Mejorar continuamente la eficacia del sistema de gestión de seguridad de la información a fin de minimizar constantemente los riesgos de la seguridad de la información.
4. Cumplir los requisitos legales y regulatorios que afectan a la organización respecto a la seguridad de la información.
   1. Política Dispositivos Móviles

Se aplica para todos los dispositivos móviles permitidos en la organización como, por ejemplo, celulares o laptops:

1. TCI establece medidas de seguridad adicional para los riesgos ocasionados por dispositivos móviles, los tipos de dispositivos móviles pueden ser:

* Teléfono móvil
* Laptop
* USB
* Tablet
* Dispositivos con tecnología Bluetooth.

1. Las configuraciones aceptables para los dispositivos móviles que hagan uso de los servicios de TCI deben considerar lo siguiente:

* Contar con Software antivirus y Software antimalware (P.ej. Mcaffe, ESET)
* Dispositivos no rooteados (Hacer root o rootear un dispositivo móvil es el proceso de modificar el sistema operativo que viene en el dispositivo para conseguir el control total sobre él).
  1. Política de Desarrollo Seguro de Software

La empresa TCI velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de sistemas de información, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por TCI.

* + 1. *Evaluación de riesgos para el proceso de desarrollo*

El oficial de seguridad de información debe realizar periódicamente la evaluación de lo siguiente:

* Los riesgos relacionados con el acceso no autorizado al ambiente de desarrollo.
* Los riesgos relacionados con los cambios no autorizados sobre el ambiente de desarrollo.
* Las vulnerabilidades técnicas de los sistemas utilizados en la organización.
* Los riesgos que puede traer una nueva tecnología si se utiliza en la organización.
  + 1. *Asegurar el ambiente de desarrollo*

Se debe asegurar el ambiente de desarrollo, identificando lo siguiente:

* Accesos lógicos al ambiente de desarrollo para personal de la organización.
* Separación lógica de los ambientes de desarrollo, prueba y producción.
* Realización de copias de respaldo de los ambientes de desarrollo.
  + 1. *Principios de ingeniería segura*

La organización debe contar con metodologías de referencia para ingeniería segura de sistemas de información, tanto para el desarrollo de nuevos sistemas como para el mantenimiento de los sistemas existentes:

* Para desarrollo web: Metodología OWASP / Metodología de Ciclo de vida del software – ISO 12207
* Para desarrollo Cliente/servidor: Metodología de Ciclo de vida del software – ISO 12207

Principios

1. Partir siempre de un modelo de permisos mínimos, es mejor ir escalando privilegios por demanda de acuerdo a los perfiles establecidos en el ciclo de vida del software.
2. Asegurar de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
3. Nunca confiar en los datos que ingresan a la aplicación, todo debe ser verificado para garantizar que lo que está ingresando a los sistemas es lo esperado y además para evitar inyecciones externas de código.
4. Hacer un seguimiento de las tecnologías utilizadas para el desarrollo. Estas van evolucionando y cualquier mejora que se haga puede dejar obsoleta o inseguras versiones anteriores.
5. Todos los accesos exitosos y/o fallidos que se hagan a los sistemas deben ser registrados en los logs de auditoría
6. Se debe evaluar las transacciones sensibles en los sistemas de información para considerar que se incluyan dichas transacciones en los logs de auditoría.
7. Para intercambiar información sensible utilizar protocolos para cifrar las comunicaciones, y en el caso de almacenamiento la información confidencial debería estar cifrada utilizando algoritmos fuertes y claves robustas.
8. Cualquier funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo a los requerimientos. De esta forma se evita generar código que resulte siendo innecesario.
9. La información almacenada en dispositivos móviles debería ser la mínima, y más si se trata de contraseñas o datos de sesión. Este tipo de dispositivos son los más propensos a ser que se pierdan y por lo tanto su información puede ser expuestas más fácilmente.
10. Cualquier cambio que se haga debería quedar documentado, esto facilitará modificaciones futuras.

Normas dirigidas

1. Normas dirigidas a: Gerencia de TI
   1. Debe proporcionar los recursos necesarios a nivel de infraestructura requeridos por la Gerencia de desarrollo.
2. Normas dirigidas a: Gerencia de desarrollo
   1. Debe implantar los controles necesarios para asegurar que las instalaciones y/o actualizaciones al ambiente de producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
   2. Debe asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
   3. Debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de TCI.
   4. Debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
   5. Deberá asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
   6. Debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de TCI.
3. Normas dirigidas a: desarrolladores
   1. Deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el análisis hasta la puesta en marcha.
   2. Deben construir los sistemas de información de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación estandarizadas.
   3. Deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
   4. Deben suministrar opciones de desconexión o cierre de sesión de los sistemas de información (logout) que permitan terminar completamente con la sesión o conexión asociada, pudiendo ser un cierre de la aplicación, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
   5. Deben evitar incluir las cadenas de conexión a las bases de datos en el código de los sistemas de información. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales deberán estar cifrados.
   6. Deben certificar el cierre de la conexión a las bases de datos desde los sistemas de información tan pronto como estas no sean requeridas.
   7. Deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.
   8. Deben proteger el código fuente de los sistemas de información construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
      1. *Requerimientos de seguridad de información*

Dirigidas a propietarios de los sistemas de información, gerencia de desarrollo y oficial de seguridad de información:

* Todos los sistemas de información o desarrollos de software deberán tener un propietario dentro de la empresa.
* La gerencia de desarrollo debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
* El oficial de seguridad de información debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.
  + 1. *Requerimientos solicitados a los desarrolladores*
* Deben documentar los requerimientos establecidos y en coordinación con arquitectura de software definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
* Deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
* Deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
* Deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
* Deben utilizar los protocolos sugeridos por la gerencia de desarrollo e innovación y el oficial de seguridad de información en los sistemas de información desarrollados.
* Deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros
  + 1. *Requerimientos de seguridad relacionados con redes públicas*
* Todos lo servicio accedidos desde redes públicas como sistemas de información y web Services debe contar con autenticación para el acceso o procesamiento de información.
* Todos lo servicio accedidos desde redes públicas deben hacer uso de protocolo HTTPS para sus sistemas web.
  + 1. *Repositorio*
* La organización establece que todo el código fuente de las aplicaciones de la organización se encuentra en el servidor de archivos en las carpetas definidas para tal fin. El acceso lógico a estas unidades es aprobado por la gerencia de TI y es revisado periódicamente por el oficial de seguridad de información.
* El acceso a los programas fuente debe estar limitado solamente a personal de desarrollo.
* Estos accesos deben ser revisados con frecuencia con la finalidad de identificar posibles accesos no autorizados.
  + 1. *Control de versión*

El control del versionamiento de software en la organización se realiza a través de la herramienta SVN, dependiendo si el software desarrollado puede ser administrado por dicha herramienta.

* + 1. *Control de cambios*

Los cambios en el desarrollo y durante el mantenimiento de los sistemas deben ser realizados de acuerdo a un documento de especificaciones o alcance.

* + 1. *Protección de datos de prueba*

Los datos sensibles, como también los datos que pueden estar relacionados a personas, no son utilizados como datos de prueba.

* 1. Política de control de accesos

El objetivo es definir las consideraciones que se deben de tener en cuenta para los accesos a la infraestructura tecnológica de TCI.

1. El control de acceso a la infraestructura tecnológica de TCI se debe realizar por medio de cuentas de usuario y contraseñas. Las cuentas de usuario deben ser únicas para cada empleado y éste será responsable por toda actividad que sea realizada con dicho usuario.
2. Está prohibido intentar ingresar a la infraestructura tecnológica con la cuenta de usuario de otro empleado.
3. La creación, modificación y eliminación de accesos a la infraestructura tecnológica debe hacerse a través de un procedimiento formal y con las autorizaciones correspondientes en formatos de acceso.
4. Los accesos con altos privilegios (usuarios administradores) deben ser controlados igualmente mediante formatos y no deben exceder un número razonable.
5. Periódicamente se debe revisar que los accesos de las cuentas de usuario de personal cesado hayan sido eliminados y/o deshabilitados.
6. Periódicamente se debe revisar que los accesos concedidos a los usuarios sean los que les corresponde de acuerdo a las funciones que desempeñan.
7. El acceso a repositorios con código fuente debe ser controlado.
   1. Política de uso de controles criptográficos

Las claves criptográficas deben de estar disponibles operativamente tanto tiempo como lo requiera el servicio que lo solicite. Las claves pueden mantenerse en un equipamiento criptográfico mientras se utilizan, o pueden almacenarse de manera externa – con las medidas de seguridad adecuadas – y recuperarlas cuando sea necesario.

De manera general, una clave se utilizará durante un plazo concreto, o período criptográfico, por los motivos siguientes:

1. Se limita la exposición en caso de compromiso de una clave.
2. Se limita el tiempo disponible para intentar penetrar los mecanismos de acceso lógico, físico y de procedimiento que protegen una clave de su divulgación no autorizada.
3. Se limita el período durante el cual la información puede comprometerse por divulgación accidental de claves o material criptográfico a entidades no autorizadas.
   1. Política de puesto de trabajo despejado

El objetivo de este punto es definir las consideraciones que se deben de tener en cuenta en el espacio de trabajo del colaborador, así como las consideraciones para el bloqueo de la pantalla de una computadora cuando no se usa.

1. Política de Escritorio Limpio
   1. Cuando un colaborador se ausenta de su sitio de trabajo debe bloquear su computadora.
   2. Al finalizar la jornada de trabajo o durante ausencias largas como la hora de almuerzo,
   3. El colaborador debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o uso interno y apagar o bloquear su computador.
   4. La información confidencial, cuando se imprima se debe retirar inmediatamente de la impresora.
2. Política de Pantalla limpia
   1. Cada vez que el colaborador se ausente de su sitio, debe bloquear su computadora con el objetivo de proteger la información y el acceso a las aplicaciones.
   2. Las computadoras deben tener aplicado un protector de pantalla definido por el equipo de Infraestructura, de forma que se active cuando la computadora no esté en uso. Cuando esto ocurra, la pantalla de autenticación solicita el usuario y la clave de red del colaborador para desbloquearse.
   3. Política de respaldo de la información

El objetivo de este punto es definir las reglas básicas para la ejecución de copias de respaldo de la información; se aplica para todas las copias de respaldo que se realizan tanto de la información, del software y de las imágenes del sistema.

1. Se establece que todos los días se debe ejecutar obligatoriamente una copia de respaldo de la información en producción.
2. Quincenalmente se debe mantener una copia de respaldo off-site.
3. Periódicamente, las copias de respaldo off-site deben ser probadas con la finalidad de identificar que contengan la información con la cual han sido etiquetadas.

**Programación**

1. Todos los días se debe generar una copia de respaldo (backup) de la información en producción.
2. El etiquetado del backup debe indicar el día, mes y año de la ejecución del backup.
3. Se debe de utilizar una herramienta para la ejecución de los backup.
4. Con una periodicidad semestral se deben realizar pruebas de restauración sobre las copias de respaldo. Las pruebas de restauración consistirán en elegir archivos aleatorios y verificar que puedan ser restaurados.

**Verificación**

1. Todos los días, una persona del área de infraestructura debe verificar la ejecución exitosa de los backups a través de los logs de auditoría o correos electrónicos enviados por la herramienta.

**Copias Off-site**

1. Con una periodicidad quincenal, el Jefe de Plataforma de TI de realizar una copia del último día hábil de la semana (por lo general sábado) del dispositivo donde se encuentre el backup de la empresa.
2. Esta copia debe ser realizada de preferencia en un medio preparado para almacenar información.
3. La copia debe ser etiquetada con la fecha original en la que fue hecho el backup.
4. La copia debe ser entregada al proveedor y se debe llevar registro de estas copias.

**Tiempos de retención**

1. Las copias de respaldo se deben mantener por un mínimo de 3 meses.
   1. Política de intercambio de información

El objetivo de este punto es definir las consideraciones que se deben de tener en cuenta para transferir información dentro de TCI y con cualquier entidad externa, se aplica para la información que se usa y es transferida o intercambiada con las partes interesadas.

Se asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades, a través de:

1. Acuerdos de Confidencialidad.
2. Acuerdos de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio.
3. Acuerdos de Cumplimiento de requerimientos de la entidad con la que se comparte información.
   1. Política de seguridad de la información para proveedores

El objetivo de este punto es definir las consideraciones a tener en cuenta cuando se tenga algún tipo de relación con algún tercero para proteger a los activos, se aplica para todas las relaciones que se tengan con proveedores que accedan a información en la empresa:

1. Todo proveedor que acceda a información de la organización deberá firmar un “Acuerdo de cumplimiento” como constancia de recepción y aceptación, el cual es parte del contrato de servicio.
2. El proveedor proporcionará los datos completos de la persona de contacto, quien será el encargado de recibir todo tipo de directivas de seguridad de la información.
3. Todo proveedor de servicios deberá velar porque su personal que presta los servicios directamente a la organización cumpla con las políticas de seguridad de la información. En caso de incumplimiento, la organización se reserva el derecho de solicitar al Proveedor el cambio de personal, sin perjuicio del derecho de la organización de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.
4. El Proveedor deberá garantizar que todo su personal que realiza servicios para la organización cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondiente a la actividad asociada, como de manera transversal en materia de seguridad de la información.
5. Cualquier tipo de intercambio de información que se produzca entre la organización y el Proveedor se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.
6. **CONTROLES**
   1. Marco General de Riesgo y Control

|  |  |
| --- | --- |
| **Principios de Control** | **Riesgos Relacionados** |
| Gestión de Activos | No contar con procedimientos de gestión de activos de información incrementa el riesgo de no poder controlar dichos activos y no poder asignar responsabilidad de darse el caso de un incidente. |

* 1. Controles

|  |  |  |  |
| --- | --- | --- | --- |
| **Control** | **Evidencia** | **Frecuencia** | **Responsable** |
| **Inventario de activos**  Periódicamente se deben realizar inventarios de los activos de información de la empresa, valorándolos de acuerdo a la confidencialidad, integridad y disponibilidad. | Inventario de Activos de Información clasificados | Anual / en demanda | Oficial de Seguridad de la Información |
| **Propiedad de los activos**  Todos los activos de información deberán tener asignado un propietario el cual será responsable del mantenimiento de los controles adecuados. | Inventario de Activos de Información clasificados | Anual / en demanda | Oficial de Seguridad de la Información |
| **Uso aceptable de los activos**  Todo personal (externo o interno) debe firmar el acuerdo de cumplimiento de las Políticas de Seguridad de Información de TCI. | Acuerdo de Cumplimiento de personal interno / personal externo | En demanda | Coordinador de RR.HH. |
| **Devolución de activos**  El personal de la empresa debe completar un formato de salida (Check-out) cuando son desvinculados. Este formato debe incluir la validación de la devolución de activos asignados. | Formato de Check out | En demanda | Coordinador de RR.HH. |
| **Directrices de clasificación de la información**  La clasificación de la información debe estar documentada de manera detalla y formal. | Inventario de Activos de Información clasificados | Anual / en demanda | Oficial de Seguridad de la Información |
| **Etiquetado de la información**  La información debe estar etiquetada de acuerdo a su clasificación. | Información etiquetada | En demanda | Gerencias |
| **Manejo de los activos**  TCI establece los mecanismos de manejo de los activos de la información para su transporte y almacenamiento. | Procedimiento de manejo de activos | Continuo | Oficial de Seguridad de la Información |
| **Gestión de soportes extraíbles**  TCI establece que todos los computadores de los colaboradores tengan bloqueado los puertos USB. Se habilitara un puerto por área con su respectivo encargado. | Computadores de los colaborados con puertos USB bloqueados | En demanda | Gerencias |
| **Disposición de medios**  Los medios que contengan información secreta o confidencial tal como discos duros, dispositivos móviles, etc, son destruidos o reutilizados una vez finalizada su vida útil. | Formato de disposición o reutilización de medios | En demanda | Jefe de Plataforma TI |

* 1. Clasificación de la Información.

|  |  |
| --- | --- |
| **Tipo de Clasificación** | **Descripción** |
| Secreta | Es información sensible de alta importancia para TCI que solo puede ser accedida por el Directorio, Gerencia General y por las personas que estos designen. El uso incorrecto de esta puede ir en contra de los intereses de TCI.  Su divulgación, transporte y almacenamiento deberá estar autorizada expresamente mediante correo o documento administrativo por el Gerente General. |
| Confidencial | Es información crítica y solamente podrá ser conocida al interior de TCI por un grupo reducido de personas que requieran del conocimiento de esta información para estricto cumplimiento de sus funciones. Su divulgación, transporte y almacenamiento deberá estar autorizada expresamente mediante correo o documento administrativo por el propietario de la información. |
| Uso Interno | Se espera que la revelación de esta información no cause daños serios a TCI, y su acceso es libre para los empleados de la organización a través de la intranet, servidores de archivos u otros medios de almacenamiento, publicación y acceso. |
| Pública | Esta información ha sido explícitamente aprobada por TCI para conocimiento público. Los ejemplos incluyen, boletines de noticias, comunicados internos, presupuestos, memorandos, informes de prensa, entre otros. |

* 1. Manejo de los activos.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo** | **Información Física o digital** | **Transporte** | **Almacenamiento** |
| Información Secreta | Digital | Utilizar medios de almacenamiento con cifrado | La información tendrá que ser cifrada y se mantendrá dentro de la Organización de manera lógica. |
| Física | Utilizar sobre cerrado etiquetado como secreta | La información tendrá que ser almacenada en un lugar seguro dentro de la Organización. |
| Información Confidencial | Digital | Utilizar medios de almacenamiento con control de accesos | La información deberá ser almacenada en medios de almacenamiento con controles de acceso dentro de la Organización. |
| Física | Utilizar sobre cerrado etiquetado como confidencial | La información deberá ser almacenada en un lugar seguro dentro de la Organización. |
| Información Uso interno | Digital | Utilizar cualquier medio que forme parte de la infraestructura tecnológica interna de TCI y por los custodios de dicha información | Se mantendrá dentro de la Organización, física o lógicamente |
| Física |
| Información Pública | Digital | Utilizar cualquier medio | Utilizar cualquier medio |
| Física |

1. **CONCLUSIONES**

Una adecuada implementación de un SGSI trae resultados positivos tanto en procesos como en prestigio ante los clientes. Pero para cumplirlos se debe de concientizar al personal sobre los riesgos y amenazas que puedan incurrir en las áreas.

Una adecuada capacitación y estandarización en los procesos generara reducción de errores en el producto final ya que para que un producto salga a producción deberá cumplir con N validaciones previas y cada validación contara con formatos estandarizados.

Por manejar información sensible de contribuyentes, cada acceso a los distintos recursos deberá estar bloqueado con credenciales y posteriormente ir habilitando según la necesidad, una vez culminado las tareas deberá volver a bloquearse con el fin de resguardar la confidencialidad.

1. **RECOMENDACIONES**

Realizar capacitación al personal para que se cree conciencia de seguridad, la documentación debe ser agradable para que pueda ser captado incluso por personas renuentes por medio de documentos multimedia.

No brindar las políticas como una opción, deber ser expuestas de manera exhortativa con el fin de que las áreas mantengan procesos uniformes y estandarizados. Esto traerá como beneficio la rápida adecuación de personal nuevo o cambios de área.