Política de Seguridad de la Información

1. Introducción

La Dirección de SONDA del Perú reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, proveedores, partner, precios, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

La información es un recurso que, como el resto de los activos que sean tangibles o intangibles, tiene valor para la institución y por consiguiente debe ser debidamente protegida.

2. Acerca de la seguridad de la información

La seguridad de la información se entiende como la preservación, aseguramiento, control y cumplimiento de las siguientes características de la información:

a) *la confidencialidad*, asegurando que sólo quienes estén autorizados puedan acceder a la información, la cual no debe ser divulgada. Las personas autorizadas no pueden revelar la información sin contar con una autorización formal.
b) *la integridad*, asegurando que la información y sus métodos de proceso son exactos y completos;
c) *la disponibilidad*, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, prácticas, procedimientos, acuerdos documentados (Reglamento interno de trabajo, contrato, siendo estos no limitativo) estructuras organizativas, funciones de software y todas las medidas que sean necesarias. Estos controles han sido establecidos para asegurar que se cumplan los objetivos específicos de seguridad de la empresa.

3. Alcance

Esta política se aplica en el conjunto de unidades, verticales de negocio y áreas de la organización, sus recursos, a la totalidad de los procesos internos o externos vinculados a la empresa a través de contratos o acuerdos con terceros y a todo el personal de SONDA del

Perú, cualquiera sea su situación contractual, la unidad de negocio a la cual se encuentre adscrito y el nivel de tareas que desempeñe.

4. Organización para la Seguridad de la Información

SONDA del Perú garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición será:

- CISO del Perú
- Oficial de Seguridad de la Información
- Oficial de Cumplimiento
- Gestor de Seguridad de la Información
- Coordinador de Seguridad de la información
- Jefe de Informática Interna

Dicha comisión deberá revisar anualmente como mínimo y actualizar cuando sea conveniente esta política, presentando las propuestas a la alta dirección.

5. Responsables

La Política de Seguridad de la Información y todos sus documentos relacionados son de aplicación obligatoria para todo el personal de SONDA del Perú, cualquiera sea su situación contractual, la unidad o vertical de negocio y áreas a la cual se encuentre adscrito y el nivel de las tareas que desempeñe:

La *Alta Dirección* es representada por la gerencia general. El rol es responsable de aprobar esta política y sus modificaciones, aprobar los recursos necesarios para el cumplimiento de la política de SI.

El *Comité de Seguridad de la Información* es responsable de revisar y proponer a la Alta Dirección, para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del SGSI de SONDA del Perú. Es responsabilidad de

dicho comité de proponer las estrategias de capacitación en materia de seguridad de la información en SONDA.

El *Oficial de Seguridad de la Información* será el responsable de alinear los objetivos de la gestión de la seguridad de la información con los objetivos del negocio, garantizando que es utilizado un enfoque coherente con la visión y la misión de la organización.

El *Oficial de Cumplimiento* será el responsable de determinar si algún incidente de la información detectado involucra también la afectación del sistema de compliance, y de ser el caso, llevará a cabo las acciones requeridas.

El *Gestor de Seguridad de la Información* será el responsable de presidir el Comité de Seguridad de la Información, diseñar y mantener los procesos para la gestión de la seguridad de la información en concordancia con las normativas vigentes. De igual manera, es responsable de diseñar políticas de seguridad específicas para los servicios y/o procesos de la organización.

El *Coordinador de Seguridad de la Información* será el responsable de coordinar las acciones del Comité de Seguridad de la Información proponer mejoras y de impulsar la implementación y el cumplimiento de la presente política.

El *Jefe de Informática Interna* será el responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la organización, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de las unidades o verticales de negocio y áreas de SONDA del Perú, de aspectos inherentes a los temas tratados en la presente política. El nivel de supervisión que pueda realizar el Jefe de Informática Interna deberá ser aprobado por la alta dirección o Informática Interna SONDA.

El *CISO* será responsable de la planificación y cumplimiento de las normativas y lineamientos de SONDA con respecto a la seguridad de la información acorde a las estrategias de la organización y el tratamiento de las acciones que podrían impactar al cliente.

El *Coordinador de Recursos Humanos* cumplirá la función de notificar a todo el personal que se vincula contractualmente con la organización, de las obligaciones respecto al cumplimiento de requisitos de confidencialidad según el contrato. En el proceso de inducción se debe asegurar que comunique la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del SGSI. De igual forma, desde la cuenta de gerencia de personas se notifica la presente política y de los cambios que en ella se produzcan, a todo el personal, a través de la seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

Los *propietarios de activos de la información* son responsables de la clasificación, mantenimiento y actualización de esta, así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo con sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Los usuarios de la información son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

6. Enfoque

El enfoque de SONDA con respecto a los riesgos de SI se basa en cumplir con el marco legal, contractual y los requisitos de seguridad de información propios y de nuestros clientes, proveedores y partners utilizando la expertise técnica del personal de la organización y de los colaboradores de SONDA en toda la región.

7. Objetivo

Proteger, preservar y administrar objetivamente la información de SONDA del Perú, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas externas o internas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de SONDA del Perú para asegurar su nivel de eficacia.

Definir las directrices de SONDA del Perú para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

7.1. Objetivos y metas del SGSI

Los objetivos y metas del SGSI se encuentran en el Manual del SGSI.

8. Acerca de los activos de información

Cada unidad o vertical de negocio y área, bajo la supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de la información físicos o digital que poseen. Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, deberán ser especificadas por el Comité de Seguridad de la Información.

La información de nuestros clientes que sea procesada en nuestras instalaciones será tratada conforme a lo indicado en esta política. La información de los clientes tratada en las ubicaciones de estos será atendida según las políticas de seguridad de la información de estos, caso contrario -o de no existir tales políticas- está política y sus políticas asociadas serán utilizadas.

El Jefe de Informática Interna deberá proporcionar herramientas que permitan la administración del inventario, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

La información deberá ser clasificada en base a su confidencialidad. La información deberá ser etiquetada según su nivel de clasificación. Los activos de soporte deberán ser etiquetados según el nivel más alto de información que soporten, en base a la clasificación de esta última. Los activos de información serán valorizados considerando su nivel de confidencialidad, integridad y disponibilidad como mínimo.

El personal que tiene contacto directo con la información o sus medios de soporte debe asegurarse que el etiquetado o rotulado es realizado.

La clasificación y etiquetado de información se realizará cumpliendo el proceso de gestión de información documentada, basándose en los niveles de confidencialidad: Público, Interno, Restringido y Confidencial con el documento de Clasificación de información.

9. Seguridad de la información en el recurso humano

Todo el personal de SONDA del Perú, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. Este perfil puede ser determinado, o estar asociado, al puesto que desempeñe. Es responsabilidad del

Coordinador de Recursos Humanos en coordinación con el Jefe de Informática Interna mantener un directorio completo y actualizado de tales perfiles.

Los atributos en materia de seguridad de la información de tales perfiles serán definidos según la división, gerencia, jefatura, o función específica a la que se deba tener acceso, acompañada del nivel de confidencialidad del acceso.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el gerente de la unidad o vertical o área o el administrador del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

Todo personal que incumpla la presente política y alguno de los acuerdos suscritos, ya sea de manera dolosa o por negligencia, deberá afrontar un proceso disciplinario según el Reglamento interno de trabajo (RIT).

9.1. Acuerdos de confidencialidad

El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el *acuerdo de seguridad de la información* y manuales que sean necesarios.

Toda persona que represente al proveedor, clientes y trabajadores, que acceda a los sistemas de información de la organización deberá firmar un *acuerdo de seguridad de la información*. Quedan excluidas las personas que únicamente accederán a sistemas públicos o redes aisladas exclusivamente para invitados, y partners.

9.2. Responsabilidades generales y manejo de activos asignados

Toda persona que utilice los activos de la información físicos o digitales –ya sea como intermediario o como directamente responsable– debe asegurar mantener su confidencialidad, integridad y disponibilidad. Esto también es aplicable a los activos que soportan dicha información.

Los activos de soporte que requieran tengan, usen o necesiten algún tipo de protección adicional deberán contar con unos *términos de uso* que deberán ser informados.

Velar en todo momento el cumplimiento de las normas de acceso, operación y protección de los activos de información entregados para el desarrollo de sus funciones.

9.3. Responsabilidades del personal de la organización

Todo el personal de SONDA del Perú debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información Institucional.

El Reglamento interno de trabajo debe contemplar procesos y sanciones disciplinarias para los casos en que se presenten usos de información que violen los términos y condiciones estipulados, los acuerdos establecidos o la presente política.

El Comité de Seguridad de la Información se encargará de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

Todo el personal de la organización tiene la obligación de proteger la información que tiene en su poder, ya sea de manera física o digital. La organización proveerá información de apoyo para cumplir esta política.

Todo el personal es responsable de la impresión, fotocopiado o cualquier otro método de copiado de información. La organización deberá determinar las medidas de seguridad que se utilizará para proteger la información que sea sometida a duplicación.

9.4. Responsabilidades de usuarios externos

Todos los usuarios externos y el personal de empresas externas deben estar autorizados por un miembro del personal de la organización quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de Tl institucionales. Los procedimientos para el registro de tales usuarios deben ser creados y mantenidos por el Jefe de Informática Interna.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de Tl institucionales (*Acuerdo de Seguridad de la Información*). Las cuentas de usuarios externos no deben ser genéricas.

9.5. Usuarios invitados y servicios de acceso público

El acceso de usuarios no registrados solo debe ser permitido a la red de datos de invitados. Esta red deberá estar separada de la red corporativa. El acceso y uso a cualquier otro tipo de recurso de información y Tl no es permitido a usuarios invitados o no registrados.

10. Teletrabajo

Los usuarios de los activos de la información deben:

Velar en todo momento el cumplimiento de las normas de acceso, operación y protección de los activos de información entregados para el desarrollo de sus funciones.

Utilizar sólo los dispositivos, configuraciones y elementos autorizados por la organización para el desarrollo de las funciones de teletrabajo.

Mantener operativos los agentes y elementos de seguridad instalados por la organización, tales como filtros de navegación, antivirus, VPN, y otros; e informar si detectan errores en su comportamiento al Comité de seguridad de la información.

Cumplir con la Política de gestión de activos y de software y la Política de Tecnología y Ciberseguridad en Teletrabajo.

11. Seguridad física y del entorno

11.1. Acceso

Se debe tener acceso controlado y restringido a las instalaciones donde se encuentren los servidores principales y sus dispositivos de comunicaciones. El Jefe de Informática Interna en conjunto con el Coordinador de Seguridad de la Información elaborarán y mantendrán las normas, controles y registros de acceso a dichas áreas

La organización asegurará el perímetro de las instalaciones que procesen información, acorde al nivel de información procesada. Los centros de datos centrales serán accesibles solo por personas autorizadas y se llevará un registro de tales accesos.

11.2. Seguridad en los equipos

Los servidores que contengan información y servicios organizacionales deben ser mantenidos en un ambiente seguro y protegido por lo menos con controles de acceso y seguridad física, controles de humedad y temperatura, y sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional vigente en formato digital debe ser mantenida en servidores o servicios aprobados por el Comité de Seguridad de la Información o el Jefe de Informática Interna. El Jefe de Informática Interna define el límite de responsabilidades de las unidades de

negocio. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información.

Los equipos claves de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS. El Jefe de Informática Interna debe asegurar que la infraestructura de servicio de Tl está cubierta por mantenimiento y soporte adecuados de hardware y software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por el personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información organizacional. Las estaciones de trabajo usadas para pruebas o desarrollo deben encontrarse fuera de la red de datos de SONDA del Perú, pudiendo brindársele acceso a una red separada de esta.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo con las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad de la Información o el Jefe de Informática Interna.

Los equipos que cambian de responsable o propietario deben ser objeto de un borrado seguro de información y custodiados con controles de acceso hasta una próxima asignación.

11.3. Seguridad en el cliente

El personal de SONDA que tenga acceso a las oficinas del cliente debe cumplir las políticas de estos, respetando el acceso áreas restringidas, quedando prohibido la toma de fotos y/o videos de sus ambientes e información confidencial, mal uso del área de trabajo, divulgación de información, así como la divulgación de la exposición de la marca.

12. Administración de las comunicaciones y operaciones

12.1. Incidentes de seguridad de la información

El personal de la organización debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad de la información, de la presente política, de los acuerdos suscritos, u otras actividades sospechosas a través de su jefe inmediato al Jefe de Informática Interna. Estos reportes también podrán realizarse directamente a cualquier miembro del Comité de Seguridad de la Información o al Service Desk.

El Comité de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad. En conformidad con la ley, SONDASONDA del Perú podrá acceder o realizar seguimiento a las comunicaciones efectuadas mediante las herramientas corporativas, previa autorización del usuario, el responsable legal y del Comité de Seguridad de la Información.

El Gestor de Disponibilidad y Continuidad en conjunto con el CISO, el Jefe de Informática Interna y el Coordinador de Seguridad de la Información mantendrá documentación para el tratamiento de fallas en sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo habitual de actividades. Dichos documentos serán definidos por el proceso de Gestión de la Disponibilidad y Continuidad.

12.2. Datos personales

La organización está comprometida con la privacidad y el manejo adecuado de los datos personales de sus empleados. Todo dato personal será tratado respetando las leyes y normativas que los regulen, incluyendo los datos sensibles que puedan ser gestionados por la organización.

El personal que haga tratamiento de datos personales deberá tener conocimiento de la importancia de estos. La asignación de roles y responsabilidades para el tratamiento de datos personales deberá realizarse en base criterios definidos.

12.3. Protección contra el software malicioso y hacking

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos, técnicos y administrativos. El Comité de Seguridad de la Información elaborará y mantendrá una o más políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso, y como control mínimo, las estaciones de trabajo de SONDA del Perú deben estar protegidas utilizando un software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control. Las estaciones de trabajo de desarrollo o pruebas, debido a su condición, podrán poseer un software antivirus no estándar, siempre y cuando sea con la finalidad de hacer pruebas de este.

SONDA del Perú, a través del Jefe de Informática Interna, podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

Cuando se realice dicho seguimiento se deberá informar al Comité de Seguridad de la Información de la ejecución de dicha tarea.

El CISO o el Jefe de Informática interna deben mantener actualizada una lista con las alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

12.4. Copias de seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo con los procedimientos documentados por el Comité de Seguridad de la Información o el Jefe de Informática Interna. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

El Jefe de Informática Interna debe asegurarse que se realizan pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas. Dichas pruebas deben ser realizadas en intervalos de tiempos definidos que, en todo caso, no deben exceder los doce (12) meses entre pruebas. Los registros de las copias de seguridad deben ser guardados durante al menos tres (3) meses según corresponda. El Comité de Seguridad de la Información puede realizar auditorías inopinadas que permitan determinar el correcto funcionamiento de los procesos de copias de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar a su jefe inmediato las copias de seguridad para su registro y custodia.

12.5. Administración de configuraciones de red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red, debe ser documentada y mantenida. Es responsabilidad del Jefe de Informática Interna el aseguramiento de dicha documentación.

Todo equipo de Tl debe ser revisado, registrado y aprobado por el Jefe de Informática Interna, antes de conectarse a cualquier nodo de la red de comunicaciones y datos de SONDA del Perú. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

12.6. Transacciones de datos e intercambio de información

Todas las transacciones de datos deberán ser protegidas para asegurar su continuidad, disponibilidad e integridad. Las formas de proteger estas transacciones podrán variar dependiendo de la aplicación y del tipo de información de traten.

Todas las aplicaciones de la organización que puedan operar sobre redes públicas deberán ser identificadas. Un análisis de riesgos deberá ser realizado para prevenir la materialización de amenazas sobre este tipo de uso.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Gerencia de Administración y Finanzas y/o un representante legal autorizado. El Comité de Seguridad de la Información debe brindar asesoría para tal fin. Toda la información de la organización debe ser manejada de acuerdo con la legislación vigente.

12.7. Internet, correo electrónico y mensajería instantánea

Las normas de uso de internet, de los servicios de correo electrónico y de la mensajería instantánea serán elaboradas por el Jefe de Informática Interna. Este debe velar por el cumplimiento de la ética institucional y el manejo responsable de los recursos de Tl.

No se permite el uso del internet, correo electrónico o mensajería instantánea para fines personales, o laborales externos a la función o funciones específicamente asignadas a su puesto.

12.8. Pantalla y escritorio limpio

Los lugares de trabajo que se encuentran dentro del alcance de la presente política deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas.

Los equipos que queden ubicados en zonas de atención al público deben situarse de forma en que las pantallas no puedan ser visualizadas por personas externas.

Cada vez que un colaborador se vaya a ausentar de su lugar de trabajo debe guardar los documentos y medios que contengan información confidencial o restringida.

Al finalizar la jornada de trabajo, el colaborador debe guardar en un lugar seguro los documentos y medios que contengan información confidencial, restringida o de uso interno.

Cuando un colaborador realice la impresión de información clasificada como confidencial o restringida deberá retirarla inmediatamente de la impresora.

Las estaciones de trabajo deben tener aplicado el estándar de bloqueo automático tras -como máximo- cinco (5) minutos de inactividad.

La pantalla de bloqueo debe mostrar solo 1) información pública, 2) las cuentas de usuario que han iniciado sesión en el equipo, 3) el dominio al que está inscrito el equipo.

Cada vez que un colaborador se ausente de su lugar de trabajo debe bloquear su estación de trabajo.

Toda pizarra después de ser usada en una reunión, planeamiento, charla, audiencia, conferencia, inducción, comité, etc. que contenga información se deberá o debe ser limpiada con una mota.

Los equipos de copias o impresión deben estar ubicados en lugares con acceso controlado y cualquier documentación confidencial o restringida se debe retirar inmediatamente del equipo.

12.9. Software

Todas las instalaciones de software que se realicen sobre sistemas de SONDA del Perú deben ser aprobadas por el Jefe de Informática Interna, de acuerdo con los procedimientos elaborados para tales fines.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor. El Jefe de Informática Interna tiene la responsabilidad de desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Es responsabilidad del Jefe de Informática Interna mantener una base de datos que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

El software utilizado para laboratorio, en equipos fuera de la red de datos de SONDA del Perú y que no accede directamente a algún servicio de SONDA deberá corresponder con la unidad de negocio.

El Comité de Seguridad de la Información deberá autorizar cualquier uso de software que explote alguna vulnerabilidad de los sistemas de la información, ya sea para el uso de una auditoría externa o para pruebas de seguridad internas.

El software adquirido a terceros deberá estar alineado a las políticas de seguridad de la información y a las leyes que sean aplicables.

12.9.1. Desarrollo seguro

Todo de desarrollo de software para los sistemas o como integración de los sistemas, debe ser protegido de alteraciones externas para todo el ciclo de vida del desarrollo.

Todo proyecto de desarrollo de software interno debe contar con un análisis de riesgos. No se emprenderá desarrollo alguno de software que presente riesgos altos no mitigados o aceptados.

12.10. Servicios en la nube

Todo servicio contratado en la nube deberá cumplir con un estándar mínimo de seguridad, que incluya HTTPS, autenticación de doble factor, políticas de seguridad y privacidad, así como políticas de respaldo, medidas de redundancia o planes de continuidad. Además, podrán requerirse medidas de seguridad adicionales en función de la especialización del servicio o los requerimientos de la organización y sus clientes.

13. Control de acceso

13.1. Categorías de acceso

El acceso a los recursos organizacionales debe estar restringido según los perfiles de usuarios definidos. Los usuarios con acceso privilegiado deben ser reducidos, validados por la gerencia respectiva y autorizados por el Jefe de Informática Interna.

13.2. Control de claves y nombres de usuario

El acceso a la información restringida debe estar controlado. Se usarán sistemas automatizados de autenticación que manejen credenciales. Todo acceso debe darse con un identificador único, que permita identificar el usuario de dicho acceso.

El Jefe de Informática Interna en conjunto con el Coordinador de Seguridad de la Información debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a los sistemas de cómputo y los datos que contiene es responsabilidad exclusiva del personal encargado de tales sistemas. La organización debe propender por mantener al

mínimo la cantidad de cuentas de usuario que el personal o los terceros deben poseer para poder acceder a los servicios de red.

El control de las contraseñas de red y el uso de equipos es responsabilidad del Jefe de Informática Interna. Dichas contraseñas deben ser almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por el Jefe de Informática Interna y deben ser cambiadas en intervalos regulares de tiempo. Cuando el personal adscrito cambie, las contraseñas deberán ser cambiadas.

Es un requisito para la terminación de una relación contractual o laboral del personal de SONDA del Perú que el Jefe de Informática Interna expida un mensaje de cancelación o deshabilitación de las cuentas de usuario asignadas para el uso de recursos o tecnologías de la institución.

Las contraseñas de cuentas personales no deberán ser compartidas. La organización debe proporcionar recomendaciones para la construcción de una contraseña segura.

13.3. Dispositivos móviles o portátiles

La organización reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles. Corresponde al Comité de Seguridad de la Información elaborar, mantener e implementar planes de capacitación que promuevan la concienciación en cuestión de seguridad de la información.

Las redes inalámbricas –que suelen ser utilizadas por estos equipos– introducen potencialmente nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo con el proceso de gestión de riesgos de la organización.

Todo tipo de dispositivo móvil que será utilizado de manera estándar en la organización debe contar con un análisis de riesgos respectivo. Un procedimiento para el uso de dispositivos móviles distintos a portátiles (laptops) y smartphones debe ser definido.

El tratamiento y la protección de los dispositivos o medios móviles, portátiles o removibles estará autorizado para aquellos colaboradores que para el cumplimiento de sus funciones así lo requieran. La pérdida debe ser reportada inmediatamente usando el proceso de reporte de incidentes.

13.4. Acceso remoto

El acceso remoto a los servicios ofrecidos por la organización debe estar sujeto a medidas de control definidas por Seguridad corporativa, las cuales deben incluir acuerdos escritos de seguridad de la información.

13.5. Auditoría y seguimiento

Todo uso que se haga de los recursos de tecnologías de la información en la organización debe ser seguido y auditado de acuerdo con esta política y a el "Acuerdo de Seguridad de la Información".

Las auditorías internas que verifiquen el cumplimiento de esta política o del SGSI deben contar con la participación del Comité de Seguridad de la Información o ser realizadas por este mismo.

Hugo González Castañeda
Gerente General