ABAI CX Digital Management

Política de Seguridad Física y Lógica

22 de Abril de 2024

www.abaigroup.com

Control de cambios

Realizado	Cargo:	Responsable CTSO
	Nombre:	Samuel Payano
	Fecha:	2024-04-12
Revisado	Cargo:	Gerente de Infraestructura y TI
	Nombre:	Alexis Roman
	Fecha:	2024-04-12
Aprobado	Cargo:	Director General
	Nombre:	Juan Diego de Lavalle
	Fecha:	2024-04-22

Registro de Cambios			
Versión	**Fecha**	**Descripción del cambio**	**Autor del cambio**
1.0	2024-03-22	Primer Documento	*Samuel Payano* *Responsable CTSO*
2.0	2024-04-22	Se incluye item de ambientes con aire acondicionado y sistemas de detección y alarma contra incendios. Los cambios han sido identificados con el ícono ►	*Samuel Payano* *Responsable CTSO*

ÍNDICE

1. Objetivo

- El objetivo de la política de seguridad física y lógica es prevenir y detectar el acceso físico no autorizado, el daño, la interferencia y el robo de información y la protección de los datos, procesos y programas; así como, prevenir el acceso físico no autorizado, el daño a las instalaciones de las oficinas de ABAI Perú.
- Definir e implementar políticas, estrategias, normas y procedimientos que nos permitan asegurar, controlar y minimizar el riesgo a niveles aceptables para la organización, debiendo ser esta labor revisada y actualizada continuamente.
- Preservar la confidencialidad, integridad y disponibilidad de los activos de información.
- Proteger los activos de la información de ABAI Perú ante todas las amenazas, ya sean internas o externas, deliberadas o accidentales, con el objetivo de garantizar la continuidad del servicio ofrecido a nuestros clientes y la seguridad de la información.
- Establecer los lineamientos generales de Seguridad de la información que permitan garantizar el adecuado uso y protección de los activos de información de ABAI Perú a través de actividades preventivas de revisión, análisis y corrección.

2. Alcance y Sanción

- La presente política debe ser publicada, distribuida y puesta en práctica de manera obligatoria por todos los colaboradores de ABAI Perú y por terceros cuya relación con ABAI Perú les permita tener acceso a información y/o a servicios de tecnología de la información.
- El incumplimiento de esta política constituye una falta grave y será materia de sanción.
- ABAI Perú protegerá la información que maneja en forma adecuada a su valor y criticidad, independientemente de los medios que la contengan, y velando especialmente por su disponibilidad, confidencialidad e integridad.
- ABAI Perú establece como metodología de evaluación de riesgos de Seguridad de la información, aquella que esté alineada con la evaluación de riesgos operacionales, complementada por normativa local y corporativa sobre gestión de riesgos de Seguridad de la información y Ciberseguridad.
- Todas las áreas organizacionales de ABAI Perú tienen la obligación de coordinar y ser facilitadoras de sus procesos e información con el responsable CTSO sin restricción alguna, excepto cuando ésta sea definida por Dirección General explícitamente.
- El responsable CTSO propondrá las normas y procedimientos específicos que se requieran para la ampliación y determinación especifica de la política de Seguridad

de la información en cada ámbito especializado y según sea requerido por ABAI Perú.

- Esta política alcanza a todas las áreas de ABAI Perú, incluyendo los proveedores que tienen acceso a la información de ABAI Perú.
- Aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de recepción, oficinas de dirección, directorio y Call Center de atención de los clientes, las cuales deben contar con mecanismos de protección física y controles de acceso adecuados para la protección de los centros de trabajo además la protección del acceso a los sistemas de información de ABAI Perú.

3. Definiciones

- **Activo de información:** Conocimiento o datos que tienen valor para la organización, por lo tanto, deben ser protegidos.
- **Confidencialidad:** Característica de la información que permite que sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Disponibilidad:** Característica que permite que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.
- **Integridad:** Característica que permite salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- **Custodio de activo de información:** Persona o área que, según sus funciones, es designada por el propietario de la información para mantener y proteger la información, de acuerdo a los lineamientos, políticas y procedimientos de Seguridad de la información.
- **Propietario de información:** Persona que, según sus funciones, tiene la responsabilidad de mantener operativos sus activos de información, determinar su criticidad y clasificación, establecer los requerimientos de protección de los mismos (controles) y definir las restricciones de acceso, tomando en cuenta las políticas de control de acceso vigentes.
- **Seguridad de la información:** Preservación y protección de la confidencialidad, integridad y disponibilidad de la información, de una amplia gama de amenazas, a fin de minimizar el daño, garantizar la continuidad comercial y maximizar el retorno sobre las inversiones y las oportunidades de negocio.
- **Ciberespacio:** Entorno virtual, en donde no existe forma física, sino más bien un entorno complejo que resulta de la interacción de personas, organizaciones y actividades de todo tipo de dispositivos tecnológicos y redes que se conecten a este entorno.
- **Ciberseguridad:** Conjunto de acciones que la organización debe llevar a cabo para proteger los activos de la organización y los usuarios en él, a través de la

prevención, detección y respuesta a los ataques a los activos de la organización y los usuarios del ciberespacio.

- **Amenaza:** Evento que puede afectar adversamente la operación del Banco y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.
- **Vulnerabilidad:** Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los activos de información.
- **Incidente:** Evento que se ha determinado que tiene un impacto adverso sobre la organización y que requiere de acciones de respuesta y recuperación.
- **Ingeniería social:** Corresponde a la práctica de obtener información confidencial, a través de técnicas o manipulación de usuarios legítimos de una organización.
- **Información confidencial**: Comprende los datos relacionados con los negocios de la empresa, los antecedentes de los clientes, así como también información de planes estratégicos, metodologías, contratos y cualquier otra información que, de ser mal utilizada, podría afectar en forma grave el prestigio de la empresa y su continuidad en el negocio.
- **Excepción:** Cualquier incumplimiento a lo que se establece a las políticas o normas de Seguridad de la Información, pero que, bajo los sustentos adecuados, niveles de aprobación correspondiente y procesos establecidos son aceptados por la organización.
- **Seguridad Física:** Conjunto de reglas, sistemas y procesos que tratan de proteger la integridad física del conjunto de elementos que forman parte de un espacio.
- **Seguridad de las Personas:** Conjunto de reglas, sistemas y procedimientos encaminados a salvaguardar la integridad de los empleados, clientes, accionistas, invitados y visitantes, incluyendo consultores o auditores que desempeñen su labor de forma ocasional o periódica, en el espacio bajo responsabilidad de seguridad física.
- **Seguridad de Edificios:** Conjunto de medios materiales, electrónicos y humanos que tratan de proteger el perímetro y el interior de una instalación, así como de los empleados, clientes o visitas que allí se encuentren.
- **Infraestructura Crítica:** Infraestructura estratégica cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
- **Servicio Esencial:** Servicio cuyo funcionamiento es imprescindible, no permite soluciones alternativas y su perturbación tendría un grave impacto.
- **Activos Clave:** Clientes, empleados, instalaciones, plataformas IT e información.
- **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Activo Físico:** Todo objeto o bien que posee una persona natural o jurídica, tales como maquinarias, equipos, edificios, muebles, vehículos, ordenadores, material de oficina, etc.
- **Áreas Seguras:** Sitio donde se maneja información sensible o valiosos equipos informáticos, es decir, refugios con los que alcanzar los objetivos de ABAI.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Hardware:** Errores intermitentes, conexión suelta, desconexión de tarjetas, etc.
- **Software:** Sustracción de programas, modificación, ejecución errónea, defectos en llamadas al sistema, etc.
- **Datos:** Alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.
- **Memoria:** Introducción de virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
- **Usuarios:** Suplantación de identidad, acceso no autorizado, visualización de datos confidenciales, etc.

4. Responsabilidades

Responsable	Funciones
Vigilancia de Seguridad Física	• Vigilar y proteger bienes muebles e inmuebles, así como a las personas que se encuentren dentro de los mismos. • Realizar controles de identidad en el acceso o en el interior de determinadas instalaciones. • Validar que el trabajador al momento de salir de las instalaciones no salga con pertenecías de la empresa. • Coordinar con los servicios externos de emergencia. • Deberá de reportar al responsable CTSO, casos o eventos de seguridad.

Responsable CTSO	• Elaborar y actualizar la Política de Seguridad Física y Lógica, asegurando su adecuación a la legislación vigente. • Hacer cumplir los mandatos en la Política de Seguridad Física y Lógica liderando las actuaciones necesarias y facilitando la consecución de estas. • Desarrollar e implementar procesos y sistemas seguros para proteger y mitigar incidencias de seguridad física y lógica. • Garantizar el cumplimiento de la gestión de atención de las vulnerabilidades. • Garantizar que la información sensible de la empresa esté protegida contra cualquier amenaza. • Planificar y conducir las actividades de ABAI Perú relacionadas con la Seguridad de la Información. • Difundir y velar por el cumplimiento de las políticas de seguridad física y lógica. • Presentar a Comité de Gestión el estatus de la seguridad física y lógica.
Gerente de Infraestructura y TI	• Definir y administrar los niveles de servicio TI. Administrar los incidentes, los problemas, la configuración hardware y software, el ambiente físico y las operaciones. • Facilitar la operación y el uso de los servicios TI habilitando a los usuarios. • Monitorear la implementación de los controles de Seguridad de la Información para el funcionamiento efectivo de la SGSI. • Monitorear el estado de la Ciberseguridad incluyendo las principales las vulnerabilidades, amenazas emergentes e incidentes de seguridad.
Director General	• Aprobar la Política de Seguridad Física y Lógica. • Aprobar las políticas y lineamientos para la ejecución de las acciones necesarias para la implementación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad y su mejora continua. • Proveer los recursos humanos, técnicos, tecnológicos, infraestructura y financieros, necesarios para desarrollar, implementar, operar y mantener un adecuado funcionamiento de la Seguridad.
Usuarios ABAI	• Participar activamente en la consecución de los objetivos de Seguridad de la Información y Ciberseguridad, y cumplir con la presente política y las normas que de ésta se deriven. • Hacer buen uso de los activos de información asignados bajo su responsabilidad para la realización de las funciones asignadas. • Reportar a sus jefaturas o gerencias cualquier incidente o situación anómala que ponga en riesgo la confidencialidad, integridad y disponibilidad de la información. • Garantizar su propia seguridad y la de los activos que se les haya asignado, debiendo observar las recomendaciones de seguridad, los principios éticos y las normas recogidas en el código de conducta.

5. Referencias

- ISO 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad.

6. Desarrollo

6.1 Políticas de Seguridad Lógica

6.1.1 Uso Adecuado de Dispositivos Portátiles

- La política de Uso adecuado de Dispositivos Portátiles tiene como objeto el establecer los principios generales de actuación orientados a aumentar la seguridad en el uso de los dispositivos portátiles asignado al personal de

ABAI Perú, tanto en lo que se refiere a equipos que se utilicen dentro de las dependencias de ABAI Perú como fuera de ellas.

- Con el fin de facilitar el desempeño de sus funciones, ABAI Perú podrá asignar diversos dispositivos portátiles (ordenadores y teléfonos móviles), a determinados colaboradores los cuales, como depositarios de dichos equipos, serán responsables de observar la debida diligencia en su custodia y salvaguarda, dicha diligencia deberá también ser observada por el personal externo sobre sus dispositivos portátiles en caso de que contengan información de ABAI Perú.
- Se deberán de tener en cuenta, además los riesgos derivados del acceso remoto a la información cuando éste se lleva a cabo desde/hacia áreas eventualmente desprotegidas y fuera del alcance de las premisas de seguridad establecidas por ABAI Perú, con el fin de minimizar las posibilidades de acceso a dicha información por parte de terceros no autorizados.

A continuación, se facilita una serie de requisitos, reglas y consejos a poner práctica para la consecución de los fines de esta política:

6.1.2 Propietarios de los Activos

El Propietario de un activo es el empleado que decide sobre la finalidad, contenido y uso del activo. El Propietario de un activo es responsable de la seguridad del mismo y, por tanto, el propietario del riesgo asociado al activo, por lo que debe asegurarse de que se analicen y gestionen los riesgos asociados al mismo. El Propietario de un activo de información tiene que ser un empleado con cargo de director o similar, que podrá delegar las tareas operativas en uno o más colaboradores directos.

Por tanto, el Propietario de un activo de información tiene las siguientes responsabilidades:

- Asegurarse, durante todo el ciclo de vida, que se identifican los requisitos de seguridad aplicables al activo de acuerdo al marco normativo de seguridad, a las necesidades del negocio, a las leyes correspondientes en materia de seguridad y a los análisis de riesgos de seguridad que sean pertinentes, con el objetivo de reducir los riesgos a un nivel aceptable. Para ello proporcionará la información necesaria a la Organización de Seguridad, quien propondrá los requisitos y controles de seguridad aplicables.
- Clasificar el activo, como mínimo, según sus requisitos de Confidencialidad, Integridad y Disponibilidad.

6.1.3 Amenazas del Sistema

Las amenazas afectan principalmente al Hardware, al Software y a los Datos. Estas se deben a fenómenos de:

- Interrupción
- Interceptación.
- Modificación.
- Generación.

6.1.3.1 Amenaza de Interrupción

- Se daña, pierde o deja de funcionar un punto del sistema.
- Detección inmediata.

Ejemplos: Destrucción del hardware, Borrado de programas, datos, Fallos en el sistema operativo.

6.1.3.2 Amenaza de Interceptación

- Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.
- Detección difícil, no deja huellas.

Ejemplos: Copias ilícitas de programas.

6.1.3.3 Amenaza de Modificación

- Acceso no autorizado que cambia el entorno para su beneficio.
- Detección difícil según circunstancias.

Ejemplos: Modificación de bases de datos, Modificación de elementos del HW.

6.1.3.4 Amenaza de Generación

- Creación de nuevos objetos dentro del sistema.
- Detección difícil. Delitos de falsificación.

Ejemplos: Añadir transacciones en red, Añadir registros en base de datos

6.1.4 Control de Acceso

- Todo acceso lógico a los activos de información de ABAI Perú es solicitado por el área de administración de personal, conforme al procedimiento PS-RH-SEC-PRO-001S_PER Selección e Incorporación Overhead y PS-RH-SEC-PRO-002S_PER Selección e Incorporación Operaciones, o solicitado por un jefe inmediato, conforme al procedimiento PS-IT-GIF-PRO-002S_PER_Incidentes y Solicitudes TI.
- Todo acceso lógico deberá cumplir lo establecido en el procedimiento PS-SI-GSI-PRO-004S_PER Gestión Roles y Privilegios.
- Las autorizaciones de acceso deben habilitar el acceso a la información mínima necesaria para el cumplimiento de las tareas asignadas
- No se podrá otorgar derechos de acceso sin haberse completado el proceso de autorización
- Queda prohibido el uso de códigos de usuarios o contraseñas embebidas, o cualquier otro mecanismo que permita el acceso omitiendo/evadiendo/saltando las reglas de seguridad establecidas por el organismo.

6.1.5 Identificación y Autentificación

La asignación de información confidencial, como parte de la autenticación del usuario, debe cumplir con lo establecido en el PS-IT-GIF-MAN-001S_PER_Manual de SI y Otros TI PER.

6.1.6 Roles

Los derechos de acceso se agrupan de acuerdo con un rol determinado y el uso de los recursos se restringe a las personas autorizadas a asumir dicho rol, en cumplimiento del procedimiento PS-SI-GSI-PRO-004S_PER Gestión Roles y Privilegios.

6.1.7 Transacciones

Toda transacción en línea en ABAI Perú, se efectuará validando previamente las credenciales de acceso (usuario y contraseña) otorgadas a los usuarios, de ser el caso.

6.1.8 Modalidad de Acceso

Se debe tener en cuenta también que tipo de acceso o modo de acceso se permitirá., los modos de acceso que pueden ser usados son: Lectura, Escritura, Ejecución, Borrado, y deben gestionarse de acuerdo con el procedimiento PS-SI-GSI-PRO-004S_PER Gestión Roles y Privilegios.

6.2 Política de Seguridad Física

Las medidas de seguridad física deben prevenir en lo posible el hurto o extravío de los equipos portátiles, y permitir la recuperación de estos en el mayor número de casos posible. Los equipos portátiles deberán estar registrados con la identificación del número de serie y los datos del propietario.

Todo personal deberá:

- Guardar el ordenador portátil, incluyendo los componentes móviles asociados al mismo, así como cualquier otro dispositivo portátil asignado en un lugar seguro cuando no esté siendo utilizado.
- No dejar abandonado en un lugar público, en ningún momento, ninguno de los dispositivos portátiles asignados.
- Durante la realización de viajes, mantener el equipo bajo control en todo momento.
- En caso de robo o perdida del equipo, el usuario debe de notificarlo al responsable CTSO, utilizando para ello el canal de comunicación al correo seguridadperu@abaigroup.com.
- Todo colaborador deberá responder por el cuidado de su integridad física no exponiéndose a los peligros generados por su actividad laboral o ajena a esta.
- Ningún colaborador de ABAI Perú debe de estar al margen de la ley.
- Está prohibido el porte de armas de fuego y/o armas blancas dentro de las instalaciones de la compañía o en instalaciones.
- Todos los colaboradores se comprometen a respetar y cumplir las normas de convivencia al interior de la compañía o en instalaciones donde se encuentre operando la empresa; los horarios establecidos para el ingreso y salida del lugar y el cumplimiento de las normas internas tales como: la prohibición de visitantes sin autorización, la toma de fotografías y video sin autorización, y las demás que sean informadas oportunamente por parte del coordinador de seguridad y de los clientes.
- El colaborador que tenga alguna sospecha o sea víctima de alguna de las formas de violencia o extorsión, se compromete a dar aviso de forma inmediata al responsable CTSO a través del correo seguridadperu@abaigroup.com o jefe inmediato y por intermedio de este a los órganos de seguridad del gobierno.
- Cualquier participación de un colaborador en actos de violencia o contra la ley será causal de terminación de su contrato laboral.
- Ningún colaborador podrá divulgar a terceros se manera formal o informal, cualquier información sobre movimientos y/o ubicación del personal de la compañía.

El incumplimiento de esta política por parte de algún colaborador de la compañía será considerado como falta grave.

6.3 Criterios

La actividad de la seguridad física debe contemplar y salvaguardar los siguientes criterios:

6.3.1 Control y Registro de Ingreso de Personas Externas

Para las personas que van a visitar el site de ABAI Perú, se define lo siguiente:

El solicitante comunicará vía correo electrónico al personal a cargo del grupo que asiste a la oficina, sobre el ingreso de personas externas.

Los datos que se envía son:

- Nombre del personal externo.
- D.N.I del personal externo.
- Hora aproximada del ingreso.
- Motivo de visita.

Nota: Si el personal externo viene con su vehículo se solicitará la placa de la unidad.

El personal a cargo deberá gestionar los accesos al edificio donde se encuentra la oficina de ABAI Perú, para el caso de la sede Chorrillos, se enviará mediante correo electrónico a la Jefatura de Administración de Personal.

El personal de vigilancia de Perú debe registrar en el cuaderno de novedades todas las visitas y los datos del personal externo y equipos registrados (marca, serie, modelo, etc.).

6.4 Aspectos Generales

La política de Seguridad Física pretende atender las amenazas potenciales desde un punto de prevención, detección, retardo y, en su caso, comunicación con la Seguridad Pública. Estas conformarán el Sistema de Seguridad de ABAI y de sus diferentes instalaciones, dentro del cual se pueden diferenciar los siguientes subsistemas de Seguridad:

- Subsistema de Protección ante Intrusión, incluyendo sensores de intrusión (contactos magnéticos, detectores volumétricos, etc.) y sus interfaces y controles, y las barreras físicas que dificulten dicha acción.
- Subsistema de Control de Accesos, incluyendo todos los sistemas on-line, lectoras, controladores, tarjetas, software de acreditación y gestión de accesos, etc., más las puertas, cerraderos eléctricos, tornos, que controlan el paso de personas y vehículos.
- Subsistema de Vigilancia por Televisión (CCTV), incluyendo cámaras, grabadores, aplicaciones específicas, monitores, etc.

- Subsistema de Centralización e Integración, incluyendo redes de datos, hardware específico, aplicaciones y servicios de parametrización.

Como norma general, los medios técnicos a instalar deberán cumplir con los siguientes requisitos:

- Proporcionar el nivel de seguridad requerido para la instalación donde se implanten, cumpliendo con los objetivos para los que se instalan.
- No interferir en el normal funcionamiento de la instalación.
- Estar en concordancia con la legislación y normativa vigente.
- No producir daños ni a las personas ni a las instalaciones.
- Cumplir con los mínimos de calidad exigidos.

Su descripción es genérica, debiendo determinarse la intensidad de dichas medidas al nivel de amenazas existente en el entorno del activo y a los condicionantes de importancia de los éstos, relación con las Fuerzas y Cuerpos de Seguridad, etc.

6.4.1 Protección ante Intrusión

La Protección ante Intrusión tiene como objetivo impedir el ingreso de personas ajenas a los edificios por cualquier vía, incluso mediante destrucción de puertas, ventanas o muros.

La intrusión puede darse desde el exterior al interior de las oficinas, o desde el interior de estas a áreas de acceso no permitido (por ejemplo, cuartos técnicos).

La Protección de Intrusión lógicamente se da cuando en el interior de las áreas a proteger no hay personal, típicamente cuando las oficinas están cerradas (excepto en el caso de determinados cuartos técnicos).

Como mínimo las vías lógicas de intrusión desde el exterior han de estar afectadas de la Protección, incluyendo entre estas:

- Puertas de acceso, puertas de emergencia, ventanas y terrazas alcanzables desde el exterior, accesos desde tejados susceptibles de ser accesibles desde otros edificios.
- En el caso de oficinas incluidas en el interior de edificios que alberguen otras actividades, se debe considerar como exterior las áreas de las oficinas externas a la propia oficina de ABAI, como halls de ascensores, escaleras de emergencia, etc.
- En el caso de cuartos técnicos internos, centros de proceso de datos, almacenes o, en general, cualquier recinto interior en el que los robos o sabotajes puedan causar un daño importante, sus vías de acceso desde las oficinas deben ser también objeto de Protección de Intrusión.

La Protección de Intrusión cumple las siguientes misiones:

- Disuadir al posible intruso.

- Detectar el intento de intrusión.
- Retardar la acción de intrusión.
- Comunicar a la policía o a la Seguridad Privada la intrusión o su intento.

6.4.2 Cierre de Instalaciones

El cierre de las instalaciones tiene especial importancia, pues además de sellar los accesos convenientemente (puertas y ventanas) implica la conexión (y desconexión en su apertura) de la detección de intrusión.

6.4.3 Control de Accesos

El Control de Accesos tiene por misión la de restringir el acceso a las instalaciones y a determinadas zonas, de manera que accedan a ellas exclusivamente los usuarios y vehículos que estén acreditados para ello. Este el control de acceso a cada recinto y la detección de posibles vulneraciones de Seguridad, contribuyendo simultáneamente a la protección de la integridad y Seguridad de las personas y objetos que se encuentran en el interior del edificio.

El Control de Accesos físico ha de ser coherente con los criterios de accesibilidad a los sistemas de información, y en un futuro se podrán extraer datos conjuntos de la doble accesibilidad física y lógica, a los sistemas de información.

Con este fin se dispone de diversas medidas que se disponen para controlar cada uno de los tráficos antes mencionados:

Personas:

- Barreras físicas que impiden el acceso no autorizado (puertas, tornos).
- Elementos de bloqueo de las barreras físicas, como cerraderos eléctricos, cerraduras y cerraderos mecánicos, hojas deslizantes, etc.
- Elementos que permiten verificar los permisos de acceso, como lectores de tarjetas (verificación automática mediante consulta a base de datos) o bombillos amaestrados (verificación mediante accionamiento mecánico con llave).

6.4.4 ►Ambientes con Aire Acondicionados

En los data center de ABAI Perú, de la ciudad de Lima y Piura, se usa el instrumento Termohigrómetro que mide y muestra la temperatura (T°) y humedad relativa (HR%) del medio. Se realiza el control diario del monitoreo a cargo del personal de Infraestructura y es registrado en el formato PS-IT-GIF-PLL-005S_PER Registro T(°C) y HR(%).

6.4.5 ►Sistemas de Detección y Alarma Contra Incendios

En los locales de ABAI Perú, se cuenta con los sistemas contra incendios que son los detectores de humo, que se activan ante una presencia de partícula de humo y humedad sobre una rejilla con puente electrónico. Estos detectores reaccionan con cualquier gas o humo. Está a cargo del mantenimiento y supervisión el arrendador de los locales.

6.4.6 Vehículos

- Barreras físicas que impiden el acceso no autorizado, como portones motorizados y barreras de vehículos.
- Elementos de bloqueo de las barreras físicas y retienen en su posición.
- Elementos que permiten verificar los permisos de acceso, como los lectores de matrículas (verificación automática mediante consulta a base de datos).

A continuación, se describen los criterios a tener en cuenta en la implementación del subsistema de control de accesos en los activos.

Para aquellos activos cuya propiedad es compartida con terceros, cabe destacar que los criterios descritos a continuación no hacen referencia a las zonas y accesos comunes, sino únicamente a las zonas y accesos propios del activo.

6.4.7 Medios de Identificación

- La gestión de los derechos de accesibilidad, mediante el cuaderno de ocurrencias que tiene el vigilante ubicado al ingreso de las oficinas de ABAI Perú.
- Las altas y bajas de los permisos de acceso, los permisos a las visitas deben estar controlado directamente por personal de ABAI.
- Se entregará a los trabajadores el fotocheck para el acceso de los centros de trabajo.

6.4.8 Circuito Cerrado de Televisión (CCTV)

El subsistema de CCTV tiene como misión la captura y almacenamiento de imágenes de TV, permitiendo su visionado en directo y revisión de grabaciones.

Las funciones que debe cumplir este sistema tienen que ser múltiples:

- Revisión forense de incidencias.
- Para llevar a cabo estas funciones, dispondrá de equipos para la captación, digitalización, compresión, transmisión, almacenamiento, tratamiento y visualización de imágenes de TV.

6.5 Áreas Seguras

6.5.1 Perímetro de Seguridad Física

Las instalaciones de ABAI cuentan con diferentes medidas de seguridad física perimetral, identificadas para cada sede.

6.5.2 Controles Físicos de Entrada

Los visitantes que acudan a las oficinas de ABAI estarán siempre acompañados por un empleado y no se permitirá el acceso, salvo autorización expresa de la Dirección, a ningún empleado ni visitante fuera del horario laboral o sin que alguien de la ABAI esté presente.

Dentro de las instalaciones de ABAI, los sistemas sensibles (servidor, router, equipos de comunicaciones) están situados en las salas técnicas dentro de una sala separada y con medidas de seguridad para su acceso, de forma que ninguna persona no autorizada tiene acceso a ellos.

No se permite acceder ni almacenar en las salas de servidores, líquidos, bebidas o cualquier objeto o elemento que pueda suponer o incrementar los riesgos de seguridad (incendio, cortocircuito, avería, etc.).

El detalle de los controles físicos de entrada está identificado para cada sede.

6.5.3 Aseguramiento de Oficinas, Despachos e Instalaciones

La descripción de cada sede incluye el aseguramiento de oficinas, despachos e instalaciones.

6.5.4 Protección contra Amenazas Externas

Anualmente y cuando se hayan producido incidentes o contingencias de seguridad física que así lo aconsejen (incendios, inundaciones, etc.) se revisarán los planes de emergencias de la empresa.

Los planes de continuidad y Emergencias de la empresa serán comunicados a todos los empleados y partes interesadas.

- No se permite el almacenamiento de materiales peligrosos o combustibles cerca de las áreas seguras (salas técnicas). Los suministros a granel como por ejemplo los de papelería no deberán almacenarse en las áreas seguras.
- La documentación almacenada en formato impreso estará alejada de las áreas seguras.

- Cuando existan equipos o medios de reemplazo o respaldo, éstos deberán ubicarse a una distancia prudencialmente segura, para evitar que dichos equipos puedan ser dañados por el mismo desastre que afecte a los equipos que estén en producción.
- Se revisarán con la periodicidad adecuada los sistemas de seguridad disponibles: extintores, sistemas de detección de incendios, equipos de emergencia / respaldo, etc. Cuando la revisión o tareas de mantenimiento no sean responsabilidad de ABAI, se exigirá un informe que indique el correcto estado de revisión y/o funcionamiento de los sistemas.

6.5.5 Trabajo en Áreas Seguras

El personal de ABAI desempeña su empleo en la zona de oficinas.

Se consideran áreas seguras las salas técnicas, cuyo acceso está restringido. El acceso a estas salas se realizará según el Protocolo de Control de Acceso a Salas Técnicas (ver Anexo I)

6.5.6 Áreas de Acceso Público y de Carga y Descarga

En determinadas sedes existe zona de almacén.

El único personal que pueda acceder (servicios de mensajería o paquetería, suministros, publicidad, etc.), serán siempre recibidos en la recepción de la oficina.

Si por algún motivo algún visitante debiera acceder a las instalaciones, éste estará siempre acompañado por personal de ABAI.

6.5.7 Colaboradores - Sucursal Piura

- La empresa ha implementado un Control de Ingreso y acceso a nuestras instalaciones para todos nuestros colaboradores, el cual se detalla a continuación
- Todos los colaboradores deberán presentar diariamente al ingreso su fotocheck o en su defecto su identificación correspondiente (DNI o CE) según corresponda.
- Todos los lunes a su ingreso los colaboradores deberán presentar al vigilante la evidencia de la encuesta sintomatológica llena, para que puedan ingresar.
- El Personal de Seguridad revisará las mochilas, bolsos, etc., para evitar que ingrese algún tipo de paquete, objeto extraño o prohibido en el reglamento interno de trabajo, que pueda afectar la integridad de la empresa o de algún miembro de ella.
- El personal de vigilancia realizará la revisión corporal del personal mediante el uso del Garret.

- En caso de que el Personal ingrese en bicicleta, moto o auto, estas se dejarán en la zona de parqueo ordenadas sin que obstruya el paso peatonal.
- No se permitirá el ingreso de licores u algún tipo de sustancias químicas a las instalaciones, en caso de suceder, se informará directamente a la responsable Administrativa y al supervisor.
- Todo el personal tendrá libre acceso a sus respectivas áreas de trabajo y espacios comunes, estando prohibida la circulación de personal por áreas restringidas identificadas con un cartel/Aviso correspondiente (sala de máquinas, cuarto de bombas, Data) caso contrario se procederá a la sanción disciplinaria correspondiente.
- A la salida, todo el Personal deberá permitir la revisión de sus pertenecías (bolsos y mochilas).

6.5.8 Personal Contratista y Tercero - Sucursal Piura

- Deberá presentar su DNI las personas peruanas y/o Carné de extranjería si es persona extranjera. Esta acción se llevará a cabo diariamente e incluye a toda la persona contratista, subcontratado y terceros vinculados que presté algún tipo de servicio a la empresa y por el tiempo que duré su labor.
- El acceso de este personal debe ser verificado por personal de seguridad previa autorización solicitada y comunicada por responsable Administrativa y/o algún responsable quien disponga del control de los servicios. A su vez los responsables de estos servicios a ejecutar deben monitorear, acompañar y controlar las mismas.
- El control de contratistas y proveedores se registrará en un Cuaderno de Control que mantiene el personal de vigilancia, y enviarlo vía grupo de Whatsapp.
- El Personal de Seguridad revisará las mochilas, y reportará cualquier ingreso de documentos o equipos de trabajo para evitar que ingrese algún objeto extraño.
- El personal contratista se limitará a realizar sus labores en el área asignada evitando estar desplazándose por las áreas no relacionadas a su labor.
- El personal contratista al iniciar labores por primera vez en la empresa deberá presentar su SCTR, para lo cual el personal de seguridad deberá verificar que este se encuentra debidamente registrado en la misma
- El personal contratista deberá llenar la Declaración Jurada sintomatológica de Salud proporcionada por la empresa, antes de iniciar las labores por primera vez en la Sede. (Vigente ante alguna emergencia sanitaria en el País)

6.5.9 Visitas - Sucursal Piura

- El responsable que recibirá la visita debe enviar el comunicado mediante correo electrónico a vigilancia con copia a la Responsable Administrativa para la autorización de ingreso respectivo.
- El personal de vigilancia notificará sobre la llegada de la visita al Responsable que envió la solicitud para coordinar el ingreso y atención respectiva, así mismo deberá registrarlo en el cuaderno de ocurrencias y enviarlo vía WhatsApp de reportes.
- A su ingreso la visita deberá presentar su DNI o cualquier otro documento de identificación oficial vigente con fotografía al personal de seguridad. Se le entregará un fotocheck de visita el cual deberá portarlo durante su permanencia en las instalaciones.
- El Personal de Seguridad revisará las mochilas y bolsos de la visita y reportará cualquier ingreso de documentos o equipos de trabajo. En caso del ingreso de equipos tecnológicos (Laptop, Tablets, etc.) se procederá a registrarlos en el formato respectivo.
- Las Visitas tienen acceso a las instalaciones en compañía de algún colaborador de la empresa, responsable de área o a quien se designe.
- El visitante a su salida deberá entregar el fotocheck provisto por la empresa al momento de su llegada.
- Está prohibido el ingreso de personas con signos de estado etílico.
- Está prohibido el ingreso de personas con armas de fuego a excepción de personal de PNP o Fuerzas Armadas.
- En caso de visitas de inspectores de entidades gubernamentales se debe solicitar que exhiba su identificación en un lugar visible y se de aviso inmediatamente a la Responsable Administrativa.

6.5.10 Monitoreo Control Operacional de Acceso - Sucursal Piura

- El personal de seguridad brindará pautas a personal que tiene acceso a instalaciones indicando que deberán exhibir el fotocheck (carnet de visita) en un lugar visible.
- Los agentes de Vigilancia verificaran la seguridad a través de las rondas en todas las instalaciones de la empresa.
- Se realiza el control de CCTV para supervisar y monitorear las instalaciones e impedir el acceso no autorizado a las áreas sensibles de la sede, comprendiendo las áreas de data, cuarto de bombas, grupo electrógeno y puertas de ingreso y salida.

6.5.11 Control de Salidas del Personal - Sucursal Piura

- En los casos que el personal se retire por temas de salud de las instalaciones deberá presentar a su salida la papeleta autorizada y firmada por la médico o enfermera de turno, jefe inmediato y trabajador, la misma que deberá mantenerse en su archivo correspondiente.
- En los casos donde exista la necesidad de trasladar al colaborador a un centro de urgencia deberá realizarse el llamado a la ambulancia SEMID puesta a disposición las 24 horas del día (Cel. 947589017)
- Para los casos de permisos personales o comisiones de trabajo el colaborador deberá presentar a vigilancia la papeleta firmada por el trabajador y jefatura inmediata.
- Para los casos en que no se encuentre dentro de las instalaciones, el personal médico, Administración, ADP, jefe de operaciones, podrá firmar y autorizar la papeleta el coordinador que se encuentre a cargo, siendo esta firma suficiente para permitir la salida al colaborador.
- Sin embargo, en caso el colaborador manifieste su voluntad de salir sin cumplir los procedimientos, no se le retendrá por ninguna razón, respetando su libre voluntad de salir y no siendo necesario detallar el “motivo”. Esto porque a pesar de nuestros procesos no podemos obligar a las personas a permanecer dentro del lugar.
- Las papeletas de salida para permisos y comisiones que se encuentran a disposición del colaborador solicitante se mantendrán en la oficina de Administración y recepción.
- Si algún trabajador llegara a sustraer algún bien de la empresa, se retiene al personal en la recepción luego tiene que reportar al Supervisor de turno y se concluye elaborando el informe correspondiente