



Código	POL.GPD.003
Versión	1.0
Fecha de aprobación	08/03/2023
Número de páginas	1 de 8

**POLÍTICA DE SEGURIDAD DE SERVICIO DE VALOR AÑADIDO**

**SELLO DE TIEMPO**



**Historial de Versiones**

Versión	Fecha	Autor	Resumen de Cambios
1.0	8/03/2023	Juan Carlos Dávila F.	Documento inicial.

<b>Firma:</b>	<b>Firma:</b>	<b>Firma:</b>
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General

## INTRODUCCIÓN

BIGDAVI S.A.C., es una sociedad anónima cerrada, constituida en el Perú, que tiene por objeto social entre otras actividades, la comercialización de productos y la prestación de servicios en Certificación Digital (certificados digitales, sellos de tiempo, software de firma digital, dispositivos criptográficos, entre otros), identificación y consultoría en tecnologías de la información, centrándose especialmente en la TRANSFORMACIÓN DIGITAL, bajo la filosofía de CERO PAPEL, permitiendo de esta manera simplificar los procesos comerciales y proporcionar seguridad a través del uso de herramientas de certificación digital, a nivel nacional e internacional. BIGDAVI S.A.C., es una empresa peruana orientada a la cobertura de necesidades de protección documentaria y de marca al servicio de las organizaciones privadas y públicas, mediante la elaboración y comercialización de elementos con tecnología de punta que brindan altos niveles de seguridad contra su duplicación y su falsificación. Actúa también en el campo de la identificación, validación y trazabilidad de personas y documentos digitales.

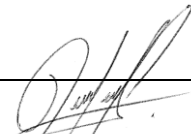
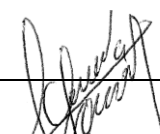
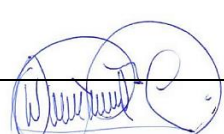
BIGDAVI S.A.C., brinda el servicios de certificación digital con la finalidad de garantizar al usuario la legalidad en el manejo de su información, así como también en el manejo de sus documentos digitales conforme a la regulación peruana establecida por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). Actualmente los servicios de certificación digital involucra los siguientes servicios:

- Firma Digital a documentos digitales.
- Sello de Tiempo.
- Trazabilidad de Documentos.
- Notificación y envío de Correos Electrónicos.
- Transferencia de Archivos digitales de forma segura.
- Almacenamiento y custodia de Archivos Digitales.

Para obtener la acreditación de SERVICIO DE VALOR AÑADIDO SELLO DE TIEMPO es necesario realizar una política de seguridad que vaya acorde a lo estipulado en el Anexo 3. De la Guía de Acreditación, para efectos de la reglamentación que solicita INDECOPI, existe un oficial de seguridad encargado de velar por los controles de seguridad puestos en la plataforma.

Entre las guías de buenas prácticas utilizadas son las siguientes:

- ITIL, ciclo de vida de un servicio.
- ISO 27001 para el uso de herramientas de seguridad que garanticen la validez en seguridad de la información.
- NTP-ISO/IEC 17799:2007

<b>Firma:</b> 	<b>Firma:</b> 	<b>Firma:</b> 
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General

**POLÍTICA DE SEGURIDAD DE SERVICIO DE VALOR AÑADIDO**

**SELLO DE TIEMPO**


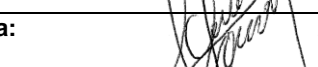

**1. OBJETIVOS**

- Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Garantizar la continuidad de las operaciones de los principales elementos que componen el SERVICIOS DE VAÑOR AÑADIDO SELLO DE TIEMPO.
- Establecer actividades que permitan evaluar los resultados y retroalimentación de la política de seguridad de la información.
- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información ante la eventual presencia de siniestros que los paralicen parcial o totalmente.
- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de BIGDAVI S.A.C. en la administración del riesgo.

**2. ALCANCE**

El alcance de este plan se sitúa en los diferentes daños o perjuicios que afectan interna o externamente con los activos de la información más importantes, debido a esto se define el alcance que tendrá este plan:

- El plan solo es aplicable a los procesos que tenga control por nuestra organización, cualquier caída fuera de nuestra infraestructura, no forma parte de las características del servicio o producto.
- El plan atiende una cantidad de procesos que hayan sufrido daño o perjuicio en la información que manejan, pero no garantiza la información externa que no haya sido generada o gestionada por nuestra organización.
- El alcance del plan de contingencia incluye los elementos básicos y esenciales, componentes y recursos informáticos que conforman los sistemas de información que maneja nuestra organización, que se relacionan a continuación:
  - **Datos:** En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (Bases de Datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes (TIF) u otro archivo o colecciones de bits.
  - **Aplicaciones:** Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la entidad.
  - **Tecnología:** Incluye los recursos en la nube como nodos o servidores, servicios de base de datos en general denominados software para el procesamiento de información.
- Independientemente de la cobertura y medidas de seguridad que se hallen implantadas, puede ocurrir un desastre, por tanto, es necesario que el Plan de Contingencia cuente también con un Plan de Recuperación en caso de desastres, el cual tendrá como objetivo restaurar los servicios de los sistemas de información de forma rápida, eficiente y con el menor costo y pérdidas de tiempo posible con la finalidad de cumplir con el Acuerdo de Nivel de Servicio (SLA) que tenemos suscrito con nuestros clientes.
- Como mínimo, los diferentes planes de contingencia que hacen parte del presente documento han sido construidos considerando que el BIGDAVI S.A.C., tenga

<b>Firma:</b> 	<b>Firma:</b> 	<b>Firma:</b> 
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General

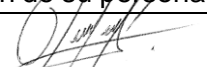


**POLÍTICA DE SEGURIDAD DE SERVICIO DE VALOR AÑADIDO**

**SELLO DE TIEMPO**

soluciones de continuidad en su operación diaria, aunque ello implique una posible reducción en su capacidad de proceso.

### 3. DEFINICIONES

- **Acceso:** Es la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una Base de Datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.
- **Amenaza:** Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a un computador. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario.
- **Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.
- **Base de Datos:** Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.
- **Datos:** Los datos son hechos y/o valores que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos en el presente documento. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y Bases de Datos, textos (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), videos (secuencia de tramas), etc.
- **Golpe (Breach):** Es la violación exitosa de las medidas de seguridad, como el robo de información, la eliminación de archivos de datos valiosos, el robo de equipos, PC, etc.
- **Incidente:** Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.
- **Integridad:** Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.
- **Privacidad:** Se define como el derecho que tiene BIGDAVI S.A.C., para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros.
- **Seguridad:** Se refiere a las medidas que toma BIGDAVI S.A.C., con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizada o intencional. En el caso de los datos e información contenidos en los sistemas de información de BIGDAVI S.A.C., la privacidad y seguridad guardan estrecha relación entre sí, aunque la diferencia entre ellas radica en que la primera se refiere a la distribución autorizada de información y la segunda al acceso no autorizado.
- **Sistemas de Información:** Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel,

<b>Firma:</b> 	<b>Firma:</b> 	<b>Firma:</b> 
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General

**POLÍTICA DE SEGURIDAD DE SERVICIO DE VALOR AÑADIDO**

**SELLO DE TIEMPO**

o pueden ser complejos como una aplicación de software con base de datos.

- **Cortafuegos (Firewall):** Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios.
- **Plan de Contingencia:** Son procedimientos que definen cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
- **Riesgo:** Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o daño.

#### 4. EVALUACION DE RIESGOS Y ESTRATEGIAS

Para la clasificación de los activos de las Tecnologías de Información de BIGDAVI S.A.C., se han considerado lo siguiente:

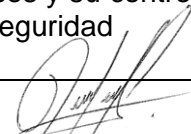
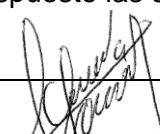

- Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).
- Frecuencia del Evento: Puede ser (Nunca, aleatoria, Periódico y continuo)
- Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Debido a que la tecnología es muy volátil, es posible que algunos sistemas de información dejen de operar por encontrarse deprecados o al ser reemplazados por unos más modernos. De acuerdo con lo anterior, los sistemas que dejen de operar por ser reemplazados por otros o por estar deprecados o a inicios de estarlo, deben permanecer instalados durante los tres (3) meses siguientes en forma simultánea para emplearlos en caso de contingencia y una vez concluido este período el responsable debe realizar una copia de seguridad completa de la información de las BDs y enviarla al área de Proyectos y Desarrollo para su verificación y custodia en diferentes almacenamientos de Objetos y/o datos en frío.

#### 5. CONTROL DE ACCESO

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la Plataforma y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y accesos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.
- Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Para los accesos y su control del mismo se ha dispuesto las siguientes normas dentro de la política de seguridad

<b>Firma:</b> 	<b>Firma:</b> 	<b>Firma:</b> 
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General

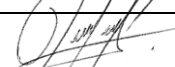


**POLÍTICA DE SEGURIDAD DE SERVICIO DE VALOR AÑADIDO**

**SELLO DE TIEMPO**

- Debe establecerse reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.
- Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente y tenga una autorización de su superior.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información. Para este fin existe un panel de administración que brinda estos accesos.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- El cambio obligatorio de contraseñas será cada 30 días calendario, después de su inicio de sesión, continuando sucesivamente.
- Se realizará un control con los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- Bloqueo de cuenta en 3 intentos de 5 min. Si vuelve a ocurrir será notificado al cliente como a la empresa.
- Todas las plataformas cuentan con un código Captcha que se encarga de evitar cualquier intromisión de un robot o algún actor intruso.
- Se mantendrá un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Se debe cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la plataforma o sufrieron la pérdida/robo de sus credenciales de acceso.
- Se debe entregar a los usuarios un detalle escrito de sus derechos de acceso.

**6. SEGURIDAD DEL PERSONAL:**

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los

<b>Firma:</b> 	<b>Firma:</b> 	<b>Firma:</b> 
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General

**POLÍTICA DE SEGURIDAD DE SERVICIO DE VALOR AÑADIDO**

**SELLO DE TIEMPO**

incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal de la organización, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito de la organización.

Para su control del mismo se ha dispuesto las siguientes normas dentro de la política de seguridad




- Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo y roles dentro de la organización.
- Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto.
- Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información que la organización maneje de acuerdo a los servicios que preste a sus clientes. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente.
- Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.
- Todos los empleados que tengan acceso como usuarios de la plataforma y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la organización, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la organización. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de los ambientes de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.
- Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como sea posible.
- Todos los empleados y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.
- Los usuarios de la plataforma, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Oficial de Seguridad.
- Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:
  - Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
  - Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
  - Alertar inmediatamente al Oficial de Seguridad.

**7. SEGURIDAD FÍSICA**

No aplica.

**8. SEGURIDAD DE COMUNICACIONES Y REDES**

Las conexiones no seguras a los servicios de red pueden afectar a toda la organización, por

<b>Firma:</b> 	<b>Firma:</b> 	<b>Firma:</b> 
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General

**POLÍTICA DE SEGURIDAD DE SERVICIO DE VALOR AÑADIDO**

**SELLO DE TIEMPO**

lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Oficial de Seguridad en coordinación con el área de Proyectos y Desarrollo tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo a un pedido formal y debidamente registrado y autorizado.

Este control es particularmente importante para las conexiones de red a instancias y aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la organización.

**9. CONTROL DE CAMBIOS Y CONFIGURACIÓN**

Proporcionar el Procedimiento de control de versiones y gestión de cambios de software, con el objetivo de tener un inventario de los mismos y mantener una trazabilidad de cambios y mejoras.

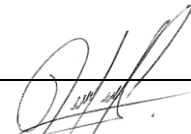
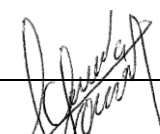
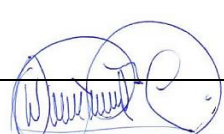
El alcance de esta política es está relacionada con productos y servicios que han sido puestos en producción en alguna o para una empresa o para alguna funcionalidad específica. No debe incluirse en este procedimiento lo siguiente:

- Código Fuente que no haya probado previamente.
- Código Fuente que provenga de un externo.

**10. REFERENCIA**

Para la elaboración de este documento, se consideró las disposiciones y normativas que se detallan a continuación:

- Norma ISO 9001:2015.
- Norma ISO/IEC 27001:2013
- Guía de Buenas Prácticas ITIL
- Metodología ágil SCRUM.

<b>Firma:</b> 	<b>Firma:</b> 	<b>Firma:</b> 
<b>Elaborado por:</b> Juan Carlos Dávila F. <b>Cargo:</b> Gerente de Proyectos y Desarrollo	<b>Revisado por:</b> Jesús Ojeda Angles <b>Cargo:</b> Gerente de Operaciones	<b>Visado por:</b> Wilfredo Dávila F. <b>Cargo:</b> Gerente General