POLÍTICA DE SEGURIDAD

ENTIDAD DE REGISTTO Y
SISTEMA DE INTERMEDIACIÓN DIGITAL
“FÍRMALO.PE”

Cód: POLI_SEG

Versión 1.0

Firmado digitalmente por MIGUEL ANTONIO HERNANDEZ GARCIA DNI:10218167 RUC:20554785469
DNI: IDCPE-10218167
Motivo: Responsable de la firma
Fecha: 07/09/2023 11:14:01-05
Empresa: IN SOLUTIONS S.A.C
Cargo: GERENTE GENERAL

Control de versiones

Versión	Secciones modificadas	Descripción del cambio	Fecha de aprobación	Revisado por	Aprobado por
1.0	Original	Creación del documento	26/JUL/2023	Miguel Hernández	Miguel Hernández

Contenido

POLÍTICA DE SEGURIDAD

1. Introducción

   In Solutions S.A.C, con RUC N° 20554785469 es una empresa dedicada a brindar soluciones tecnológicas, entre las que destacan los softwares y/o aplicaciones de servicios de verificación biométrica contactless, firma digital, portal de firma digital firmalo.pe, entre otros.

2. Objetivo

   Establecer el marco general y los lineamientos para la seguridad de la información relacionados al Sistema de Intermediación Digital y a la Entidad de Registro, a fin de garantizar la disponibilidad, confidencialidad e integridad de la información durante el desarrollo de las operaciones y acciones del servicio.

3. Gestión del Documento

   3.1. Organización que administra la política de Seguridad

   El presente documento es administrado por la empresa INSOLUTIONS S.A.C., con RUC N° 2055478546

   3.2. Persona de contacto

   La persona responsable del Sistema de Intermediación Digital "Fírmalo.pe", de autorizar los cambios en el documento y de asegurar la implementación de la Política de Seguridad es Miguel Hernandez, Gerente General de In Solutions S.A.C. Para cualquier consulta, pueden dirigirse a:

   - Teléfono: +51 1 3108149
   - Correo Electrónico: info@insolutions.pe
   - Dirección: Calle Enrique Palacios 360, oficina 102. Miraflores, Lima, Lima.
   - Web: http://insolutions.pe/

4. Refererencias
   - Ley N° 27269 Ley de Firmas y Certificados Digitales
   - Ley N° 27310 Ley que modifica el artículo 11° de la Ley N° 27269
   - Decreto Supremo N°052-2008-PCM. Reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias
     - Guía de Acreditación para los Prestadores de Servicios de Valor Añadido, específicamente el Anexo 3 – Modelo de Política de Seguridad del SVA
     - Lineamientos del como ISO 27001 y el estándar NTP-ISO/IEC 17799

5. Alcance de aplicación

El contenido de la presente política, así como las normas y procedimientos que deriven de ella, serán de cumplimiento obligatorio para todo el personal de In Solutions y terceros contratados que participen de manera directa o indirecta en la prestación del servicio del Sistema de Intermediación Digital "Fírmalo.pe" y en los procesos de la Entidad de Registro In Solutions.

6. Controles de seguridad

6.1. Evaluación de riesgos

Se realiza una evaluación y análisis de riesgos, tendiéndose en consideración tanto las amenazas internas como externas. De esta manera, se implementan las opciones de tratamiento de riesgos que permitan mitigar el impacto en los activos de información.

Se archivan el inventario de activos de información y la matriz de evaluación y tratamiento de riegos, tal como se indica en la sección de archivo de la Declaraciones de Prácticas.

6.2. Política de Control de Acceso

In Solutions no limita el acceso de lectura a información no confidencial y utilizada para realizar labores diarias del personal. Sin embargo, sí se establecen controles de accesos a la información confidencial generada como parte de la operación del servicio. Los controles se implementan como resultado de la evaluación de riesgos, de modo que solo personas autorizadas puedan acceder y/o realizar acciones como añadir, borrar o modificar registros.

Los ambientes en los que se encuentra la información sensible son protegidos contra acceso físico y lógico no autorizado.

Los servidores se alojan de forma virtual en el cloud Microsoft Azure, que cuenta con todas las medidas de seguridad de acceso, tanto a nivel personal como a nivel tecnológico.[1]

6.3. Seguridad del Personal

Todo el personal posee conocimiento, experiencia y calificaciones necesarias para desempeñar las funciones de acuerdo con los roles que tiene asignados dentro de los servicios acreditados. Específicamente, el personal gerencial cuenta con conocimiento y experiencia en firmas y certificados digitales, sellos de tiempo, seguridad de la información y evaluación de riesgos

[1] Mayor información sobre las medidas de seguridad Azure se encuentran en: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

El personal en roles de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada y pudieran perjudicar la imparcialidad de las operaciones del servicio.

6.3.1. Roles de Confianza

Se definen, como mínimo, los siguientes roles de confianza:

- Oficiales de seguridad: Responsables de administrar la implementación de las prácticas de seguridad
- Administradores de sistemas: Autorizados a instalar, configurar y mantener la integridad de los sistemas
- Operadores de sistemas: Responsable de operar la integridad de los sistemas en el día a día. Autorizados para ejecutar sistemas de respaldo y recuperación.
- Auditores de sistemas: Autorizados a ver archivos y logs de los sistemas

El personal es formalmente asignado a cumplir los roles de confianza, los cuales se definen los roles en los documentos Memoria Descriptiva y Organigrama del SID y ER, respectivamente.

6.3.2.Controles aplicados al personal

Para la contratación de una persona dentro de un rol de confianza, se verifica la documentación entregada por el aspirante. El área competente de la empresa In Solutions realiza, como mínimo, las siguientes verificaciones:

- Verificación de la identidad.
- Confirmación de las referencias.
- Confirmación de empleos anteriores.
- Revisión de referencias profesionales.
- Confirmación y verificación de grados académicos obtenidos.
- Verificación de antecedentes penales, policiales y crediticios
- Verificación de experiencia y calificaciones específicas para la función que desempeña cada rol.
- Constancias de conocimiento y experiencia en seguridad de la información (para el personal encargado de la Seguridad)

En ningún caso, In Solutions asigna en roles de confianza o administración a cualquier persona que es conocida por tener una participación en un crimen serio u otra ofensa la cual afecta su idoneidad para su puesto.

El personal no tiene acceso a funciones de confianza hasta completar todas las verificaciones necesarias.

6.3.3. Rechazo de un candidato

Los motivos que pueden dar lugar a rechazar al candidato a un rol de confianza son los siguientes:

- No contar con la formación y experiencia necesarias para el puesto.
- Falsedades en la solicitud de trabajo, realizadas por el aspirante.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato

6.3.4. Capacitaciones al personal

Se imparten capacitaciones periódicas para asegurar que pueda desempeñar correctamente sus funciones.

Las capacitaciones incluyen, como mínimo, los siguientes aspectos:

- Conceptos básicos de firmas y certificados digitales, en especial, los aplicables al Sistema de Intermediación Digital y los procedimientos de la Entidad de Registro.
- Formación sobre aspectos de funcionamiento del Sistema de Intermediación Digital "Fírmalo.pe" y de los procedimientos de la Entidad de Registro, de acuerdo con las funciones que realiza cada persona.

La formación del personal se actualiza de acuerdo a las necesidades, de tal manera que la frecuencia es suficiente para que cumplan sus funciones de manera competente y alineados a las políticas de la empresa.

6.3.5. Controles de personal en terceros contratistas

Corresponde a los terceros contratistas, que participan en las operaciones del Sistema de Intermediación Digital "Fírmalo.pe", evidenciar la verificación de antecedentes de su personal, de tal manera que sea equivalente a la realizada al personal del SVA.

Además, la seguridad se mantiene cuando las operaciones son tercerizadas a través de las cláusulas definidas en los contratos con los terceros.

6.4. Seguridad Física y del entorno

Para el caso del data center del SID "Fírmalo.pe", los controles de seguridad física son implementados por el contratista Microsoft Azure y verificados por IN SOLUTIONS.

En el caso de las oficinas de captura de datos de la Entidad de Registros, se implementan controles de acceso mediante la huella dactilar al momento de ingresar y/o recibir visitas de terceros, clientes o aspirantes a clientes.

Además, los ambientes cuentan con ventilación y condiciones ambientales óptimas para el personal.

6.5. Seguridad de comunicaciones y redes

Se protege el acceso físico y lógico a los dispositivos de gestión de red, con el objetivo de garantizar la seguridad de los datos y servicios utilizados a través de la red interna y del internet.

La red tiene las siguientes características:

- Se controla el acceso de los usuarios y administradores, a través de políticas de red
- Se cuenta con sistemas de detección de intrusos para prevenir accesos de código malicioso o no autorizado (antivirus, detección de malware, troyanos, etc.)
- Se cuenta con protección a nivel de capa de aplicación a través de un Web Application Firewall.
- Se cuenta con protección a nivel de capa de red a través de un DDoS.

- Se separa la zona de constante acceso con la red interna de procesamiento y almacenamiento de información crítica. De acuerdo a los diferentes niveles de seguridad, deben separarse las redes de datos de los sistemas de procesamiento centra.
- El acceso a dominios de redes internases protegido contra acceso no autorizado, incluyendo a suscriptores y terceros que confían. Los firewalls deben ser configurados para prevenir todos los protocolos y accesos no requeridos para la operación.

6.6. Mantenimiento de equipos y su desecho

Se asegura el buen funcionamiento de los equipos a través del mantenimiento preventivo, especialmente para equipos críticos. El mantenimiento se realizará bajo las estrictas instrucciones de cada fabricante, pudiendo incluir limpieza externa para evitar la acumulación de polvo, parches o actualizaciones de firmware, reemplazo de un componente de hardware que se encuentre dañado, entre otros.

Según la designación de roles de confianza de la sección **6.3.1 Roles de Confianza,** los "Operadores de sistemas" serán los encargados de gestionar el mantenimiento preventivo de los equipos. De ser necesario, se contratarán terceros para ejecución de dicha tarea.

Antes del reemplazo o desecho de un equipo, se revisará que toda la información sensible haya sido borrada de tal forma que no pueda ser recuperada.

6.7. Control de Cambios y Configuración

Según la designación de roles de confianza de la sección **6.3.1 Roles de Confianza,** los "Administradores de sistemas" serán los encargados de analizar y aprobar los cambios que se requieran realizar en los sistemas, a fin de evitar posteriores fallas o incompatibilidades con otros sistemas. Se ha dispuesto que todo cambio en la configuración de producción o parches de emergencia para aplicaciones críticas sean

efectuados, de preferencia, fuera del horario de atención a los clientes y que sean documentados.

Todas las actualizaciones siguen un protocolo estricto, que va desde las validaciones en el ambiente de calidad, pasando por certificación y finalmente pase a producción.

6.8. Planificación de Contingencias

Se toman medidas preventivas que permitan reaccionar ante una posible interrupción del servicio, de tal manera que se pueda mantener la continuidad de las operaciones críticas.

Las medidas de contingencia están relacionadas a los riesgos identificados como parte de la **Evaluación de riesgos.**

6.9. Auditorías y Detección de Intrusiones

In Solutions se somete a auditorías internas de seguridad periódicamente. De esta manera, se pueden encontrar vulnerabilidades y mantener los controles indicados en el presente documento. Se cuenta con protección en tiempo real, por medio de Security Center de Azure, además de las capas de seguridad, indicadas en la sección 6.5

Además, se realizan pruebas periódicas de detección de intrusiones que permiten alertar de intentos no autorizados a los sistemas críticos.

6.10. Medios de Almacenamiento

Con el fin de proteger la información sensible, se establecen controles sobre los medios de almacenamiento permitidos. Únicamente personal autorizado tiene acceso a los medios de almacenamiento necesarios para proteger la información.

Los medios de almacenamiento que contienen datos sensibles, como copias de respaldo, son protegidos contra acceso no autorizado y, una vez que ya no son requeridos, se realiza un borrado de información antes de ser eliminados