POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión:	1.0	
Código:	ENRV-0004	
Fecha de creación:	14/05/2019	
Creado por:	Javier Delgado	Cargo: Oficial de Privacidad de Datos
Aprobado por:	Rocío Huamán	Cargo: Responsable de la Entidad de Registro
Nivel de confidencialidad:	Restringido	

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación

1. Introducción

Para Innova Digital Solutions en adelante INDIGITAL, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones, por lo cual existe un compromiso expreso de protección como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

La información debe ser protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada, puede existir en diversas formas: impresa, escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones.

La Seguridad de la Información es la protección de la información contra una amplia gama de amenazas con el fin de garantizar la continuidad del negocio, minimizar los riesgos que la acarrean y maximizar el retorno de las inversiones y oportunidades de negocio.

2. Objetivo

El objetivo de este documento es establecer y determinar los lineamientos que permitan proteger la información de la Entidad de Registro alineado a la Política de Seguridad de la Información de INDIGITAL.

3. Alcance

Esta política aplica a toda la Entidad de Registro de INDIGITAL y es de consideración por parte de los colaboradores involucrados.

4. Gestión de la seguridad de la información

4.1. Objetivos de la seguridad de la información

1. Mantener y custodiar la información generada por los procesos del servicio de Entidad de Registro.
2. Realizar el tratamiento de los riesgos asociados a los activos de información de la Entidad de Registro.
3. Aplicar controles de seguridad a los activos de información de la Entidad de Registro.
4. Conservar la integridad de la información de todos los datos procesados por la Entidad de Registro.
5. Asegurar la continuidad del servicio de la Entidad de Registro.

4.2. Principios de seguridad de la información

Los principios de Seguridad de la Información están basados en la Política de Seguridad de la Información de INDIGITAL.

5. Requisitos para la seguridad de la información

5.1. Evaluación del riesgo

La Entidad de Registro cuenta con una metodología de Análisis y Gestión del Riesgo que permite analizar regularmente el grado de exposición de nuestros activos de información frente a aquellas amenazas que puedan aprovechar ciertas vulnerabilidades e introduzcan impactos adversos a las actividades o procesos de nuestra organización, así como definir los criterios de clasificación y aceptación del riesgo.

5.2. Política de control de acceso

La Entidad de Registro cuenta con una Política de Control de Acceso que especifica los controles implementados para la protección de la información recopilada.

5.3. Política de seguridad del personal

La Entidad de Registro cuenta con una Política de Seguridad del Personal que establece los controles y requisitos que los colaboradores que participan en las operaciones de la Entidad de Registro deben cumplir.

5.4. Seguridad física

La Entidad de Registro cuenta con los siguientes elementos que permiten asegurar la seguridad física y ambiental:

- El edificio donde se encuentra la Entidad de Registro tiene control de acceso (recepción) en el primer piso y una cámara de video vigilancia por piso.
- Cámaras de video vigilancia internas.
- Aire acondicionado.
- INDIGITAL cuenta con certificado de Defensa Civil que regula el uso de luces de emergencia, extintores, detectores de humo y señales de emergencia.
- Sistema Biométrico para acceder a la Oficina de INDIGITAL.
- Cerraduras mecánicas para el acceso a los distintos ambientes de la Entidad de Registro.

5.5. Comunicaciones y redes

La Entidad de Registro cuenta el servicio de correo electrónico para la comunicación, el cual es gestionado mediante herramientas que permiten su administración.

La comunicación de la Entidad de Registro con la Entidad de Certificación se realiza mediante canales seguros SSL y la autorización del acceso a la plataforma mediante certificados digitales de los Operadores de Registro.

5.6. Mantenimiento de equipos y desechos

La Entidad de Registro cuenta con un Plan de Mantenimiento de Equipos para asegurar el correcto funcionamiento de los equipos utilizados. La destrucción de la documentación física se realizará utilizando un triturador de papeles, en caso de la documentación digital se realizará de acuerdo al procedimiento de formateo del equipo.

5.7. Cambios y configuraciones

La administración de los cambios y configuración está gestionada por la EC vinculada.

5.8. Plan de contingencias

La Entidad de Registro cuenta con un Plan de Contingencias que define las acciones para atender de forma oportuna, eficiente y eficaz los incidentes o desastres que afecten la continuidad de las actividades de Emisión, Reemisión, Revocación o Suspensión de Certificados Digitales.

5.9. Auditorias y detección de intrusiones

La Entidad de Registro se someterá a auditorías internas para verificar sus operaciones al menos una vez al año.

La Entidad de Registro se someterá a auditorias por parte de la Autoridad Administrativa Competente (AAC) cada vez que ésta lo requiera, respecto a las operaciones realizadas. El auditor debe ser autorizado por la AAC.

5.10. Medios de almacenamiento

Los archivos digitales serán almacenados en un gestor documental de INDIGITAL, el almacenamiento de los archivos gestionados por la plataforma son administrados por la Entidad de Certificación.

6. Vigencia

Esta Política y todo su contenido tendrán vigencia a contar de su fecha de aprobación y puesta en marcha, y tendrá duración indefinida en tanto la Alta Dirección de INDIGITAL no adopte otra resolución al respecto.

El Oficial de Privacidad de Datos es el propietario de este documento y el responsable de verificar y actualizar el mismo cuando sea necesario.

7. Aprobación y modificaciones

El presente documento fue aprobado por la Alta Dirección de INDIGITAL el 31 de mayo de 2019. Para que este documento sea considerado válido debe contar como mínimo con la Firma Digital del Responsable de la Entidad de Registro de INDIGITAL. En caso de realizarse modificaciones, deberá consignarse el registro de cambios en el historial de modificaciones del documento.

8. Mecanismo de divulgación

El texto íntegro y actualizado de la presente Política se pondrá y mantendrá a disposición de los interesados en la página web de INDIGITAL (www.indigitalsolutions.com) y en el repositorio de la Entidad de Registro de la organización.

9. Definiciones

9.1. Activo de Información

Todo aquello que tenga valor y es importante para INDIGITAL, sean documentos, sistemas o personas. Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización.

9.2. Riesgo

Es la posibilidad de que ocurra un evento que afecte adversamente el logro de los objetivos de INDIGITAL. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.

9.3. Amenaza

Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.

9.4. Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.

9.5. Confidencialidad

Propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados.

9.6. Integridad

Propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, permitiendo salvaguardar la exactitud y completitud de los activos de información.

9.7. Disponibilidad

Propiedad de la información según la cual es accesible y utilizable oportunamente por las personas, sistemas o procesos autorizados, en el formato requerido para su procesamiento.

9.8. Evento de Seguridad de la Información

Actividad o serie de actividades sospechosas que amerita ser analizada desde la perspectiva de la Seguridad de la Información.

9.9. Incidente de Seguridad de la Información

Evento o serie de eventos de Seguridad de la Información, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.

10. Documentos de referencia

a) SGSI-0003-Política General del Sistema de Gestión de Seguridad de la Información
b) SGSI-0004-Política de Seguridad de la Información

En caso de duda, aclaración o para más información sobre el uso de esta Política y la aplicación de su contenido, por favor consulte vía correo electrónico al Oficial de Privacidad de Datos.