BIZLINKS S.A.C

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Actualización: 11/07/2022

ÍNDICE

1.- PRESENTACIÓN

1.1.- PRESENTACIÓN DE LA ORGANIZACIÓN

1.2.- CONTEXTO

1.3.- COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

2.- ALCANCE Y EXCLUSIONES

2.1.- ALCANCE

3.- GESTIÓN DEL MANUAL DEL SISTEMA

3.1.- IDENTIFICACIÓN, CODIFICACIÓN, REVISIÓN, APROBACIÓN, DIFUSIÓN Y ARCHIVO.

3.2.- ACTUALIZACIÓN.

4.- PROCESOS DEFINIDOS

4.1. INTERACCIÓN DE PROCESOS

5. LIDERAZGO Y COMPROMISO

5.1.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.2.- ROLES, RESPONSABILIDAD Y AUTORIDAD

6. PLANIFICACIÓN

6.1.- ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

6.2.- OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Jorge Sotomayor	Javier Drazl
Revisado:	**Aprobado:**
OFICIAL DE SI	**GERENTE GENERAL**
Fecha:11/07/2022	**Fecha: 11/07/2022**

7.- APOYO

7.1.- RECURSOS

7.2.- COMPETENCIA

7.3.- TOMA DE CONCIENCIA

7.4.- COMUNICACIÓN

7.5.- INFORMACIÓN DOCUMENTADA

8.- PLANIFICACIÓN

8.1.- PLANIFICACIÓN Y CONTROL OPERACIONAL

8.2.-APRECIACIÓN Y TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

8.3.- TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

9.- EVALUACIÓN DE DESEMPEÑO

9.1- SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

9.2.- AUDITORÍA INTERNA

9.3.- REVISIÓN POR LA DIRECCIÓN

10.-MEJORA

10.1.- NO CONFORMIDADES Y ACCIONES CORRECTIVAS

10.2-MEJORA CONTINUA

11.- DOCUMENTOS DE REFERENCIA

Fecha de Modificación	Versión Actual	Descripción / Modificaciones
28/08/2019	00	Edición Inicial
04/10/2019	01	Se modificó el punto 1.3. Compresión de las necesidades y expectativas de las partes interesadas. Se agregó “SUNAT” como una parte interesada
20/04/2020	02	Modificación del FODA 2020
01/05/2020	03	Revisión de las partes interesadas y modificación del alcance.
12/10/2020	04	Modificación de la interacción de procesos.
03/12/2020	05	Actualización del organigrama de la organización
27/08/2021	06	Se revisó y se determina que no se realizan cambios durante esta revisión.
11/07/2022	07	Modificación del documento

Jorge Sotomayor	Javier Drazl
Revisado:	**Aprobado:**
OFICIAL DE SI	**GERENTE GENERAL**
Fecha:11/07/2022	**Fecha: 11/07/2022**

1. Presentación

Bizlinks, es una empresa de servicios especializada en facilitar el intercambio de información entre empresas de manera electrónica.

Nuestras operaciones iniciaron hace más de 10 años con el objetivo de ser líderes en la integración entre procesos de las empresas en su camino a la transformación digital dentro del comercio electrónico.

Dentro de los beneficios que ofrece se encuentra lo siguiente:

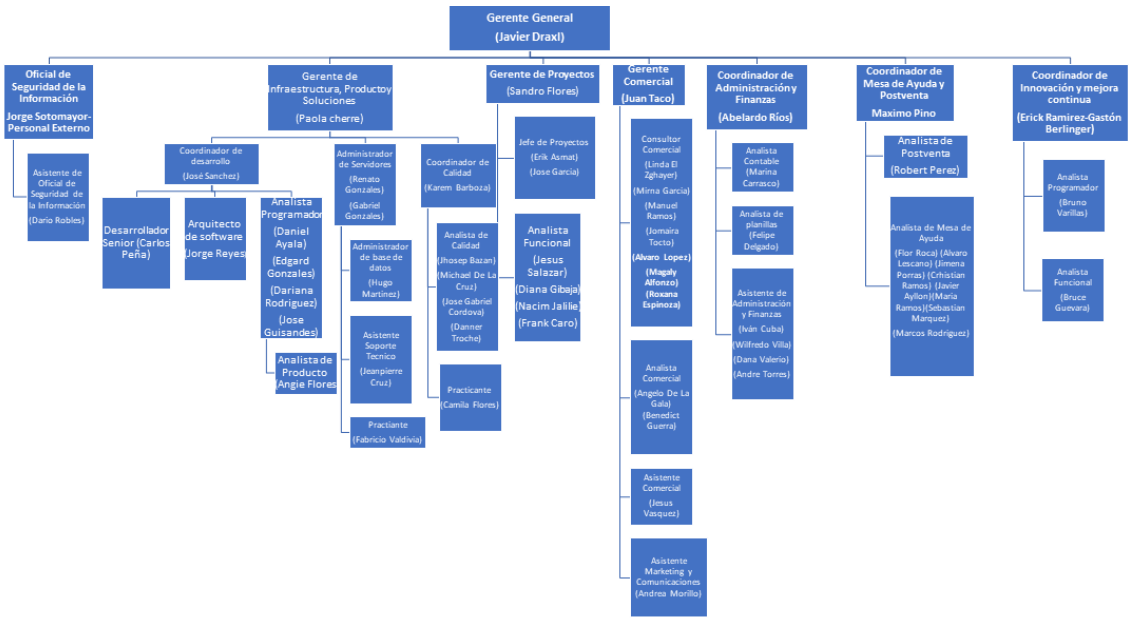
- Personal capacitado
- Disponibilidad de atención 24/7
- Atención personalizada
- Experiencia en todo tipo de negocio
- Confidencialidad e integridad
- Mejora continua de los servicios que ofrece

Además de estar certificada como Operador de servicios electrónicos OSE y Proveedor de servicios Electrónicos PSE.

Asimismo, se establece y documenta el **Sistema de Gestión de Seguridad de la Información** en adelante SGSI, conforme a la norma de referencia UNE-ISO/IEC 27001:2013, identificando para ello los activos a proteger, el enfoque de la gestión del riesgo adoptado por la organización, los objetivos y controles, así como el grado de protección requerido para los mismos.

1.1. Presentación de la organización.

El Organigrama de la organización es el siguiente:



1.2. Contexto.

Bizlinks determina las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la Seguridad de la información.

Para ello se lleva a cabo un análisis, permanente, de su entorno:

- Externo: Relacionado con aspectos de tipo:
    - Legales. Identificando y analizando los principales cambios legales que puedan afectar a la empresa en materia de seguridad de la información.
    - Tecnológicos. Identificando y analizando los principales aspectos tecnológicos presentes y futuros que puedan afectar a la empresa.
    - Competitivos. Identificando y analizando los principales competidores presentes y futuros, sin menosprecio alguno.

- Mercado. Identificando, analizando y anteponiéndonos a los principales cambios y variaciones en el mercado, asociados a variaciones en los gustos de los clientes, cambios en la tecnología.
- Cultural. Identificando y analizando los principales aspectos culturales que puedan afectar que puedan afectar a la empresa.
- Social. Identificando y analizando los principales aspectos sociales que puedan afectar que puedan afectar a la empresa.
- Económico. Identificando y analizando los principales aspectos económicos presentes y futuros que puedan afectar a la empresa.

- Interno. Relacionado con cuestiones de tipo:

  - Valores. Que rigen a la organización.
  - Conocimientos. Que atesoran su personal, y que existe la posibilidad de que no esté siendo utilizado al 100%.
  - Desempeño. Desarrollo de sistemáticas, respeto de las mismas y trabajo respecto a los requisitos de seguridad establecidos; por otro lado, objeto de la norma ISO 27001.

A continuación, se adjuntará el análisis FODA:

		OPORTUNIDADES		AMENAZAS
CUESTIONES EXTERNAS	O1	Mejora en los procesos de Sistema de Gestión de Seguridad de la Información con el objetivo de obtener la re-certificación ISO 27001	A1	Inestabilidad política en el ejecutivo y legistativo a causa de un posible cambio de la constitución política, generando desconfianza en futuras inversiones. Además de la incertidumbre económica del país por la inestabilidad política y enfermedades catalogadas como pandemía por el MINSA.
	O2	La apertura de nuevos mercados e-commerce en un 50%, aumentando el uso de pasarelas de pagos. (Nuibiz, Pagoefectivo, SafetyPay, etc)	A2	Dependencia de resoluciones de SUNAT para OSE y PSE. Amenaza constante a la creación de un nuevo modelo de facturación o indisponibilidad del portal y web service.
	O3	Aumento de demanda del mercado de soluciones provistas por FINTECHs, con crecimiento en los últimos 5 años del 21%	A3	Incremento de la competencia dentro del rubro de la Facturación Electrónica debido a la publicación de la resolución SUNAT N°155-2017, que obliga a las Mypes a facturar de forma electrónica.
	O4	La *Resolución SUNAT N°155-2017* obliga a las Mypes a facturar de forma electrónica, generando una mayor demanda de los servicios prestados por Bizlinks.	A4	Como consecuencia la pandemia, se notó como estrategia ejecutar trabajo de forma remota saturando las redes de internet hogar, perjudicando las labores diarias del trabajo remoto.
	O5	Las empresas que cuentan actualmente con verificación PSE tendrán que contar con la certificación ISO 27001 para el año 2021. A través de la Resolución Nº 105-2020/SUNAT	A5	Ataques por ciberdelicuentes en busca de vulnerabilidades que comprometan la seguridad de la información
		FORTALEZAS		**DEBILIDADES**
CUESTIONES INTERNAS	F1	Contamos con un proveedor que aplica controles de seguridad física dentro de su Datacenter, brindando protección a la confidencialidad, integridad y disponibilidad de nuestros servidores. Para nuestros servidores en la nube contamos con seguridad de accesos a servidores mediante la plataforma de IBM Perú.	D1	Los sistemas para portales de productos no se encuentran sistematizados e integrados y esto trae consigo muchos inconvenientes con respecto al tiempo de respuestas.
	F2	Contamos con la certificación ISO 27001 , que exige la implementación y mantenimiento de controles de seguridad para los procesos que son parte del "alcance" de Bizlinks.	D2	No se cuenta con procesos y/o plan enfocados a ethical hacking para encontrar y solucionar fallos de seguridad.
	F3	Experiencia en el rubro más de 7 años, permitiéndonos manejar una base de datos enriquecida.	D3	Falta implementar la gestión de proceso perjudicando en la carga laboral.
	F4	Somos parte del grupo Alignet, líder en soluciones tecnológicas en el mercado de comercio electrónico.	D4	No se cuenta con un SLA al interno en Bizlinks, por lo cual podría perjudicar a las áreas internas en capacidad, disponibilidad y seguridad.
	F5	Facilidad de la empresa para adaptarse al trabajo remoto y fácil uso de herramientas que permiten lograr el trabajo remoto, como por ejemplo Teams, Onedrive y uso de VPN.	D5	Falta implementar planes enfocados al capital humano, generando un desconocimiento de habilidades en los colaboradores y una baja sinergía laboral entre las áreas.
	F6	Cartera de productos diversos e innovadores, personalizados según el tipo y tamaño de empresa (apoyándonos en más de 90 Business Partners).	D6	No se tiene un plan de fidelización de clientes (postventa), las reuniones con clientes son escazas (kickoff) y hay poca información de la competencia por lo que esto implica a un bajo resultado en satisfacción al cliente.

Con carácter anual, se lleva a cabo la determinación de cuestiones internas y externas pertinentes a nuestro SGSI, durante la revisión por la dirección, quedando evidenciado en el **SI-FR-01 Informe de Revisión por la dirección ISO 27001**.

1.3. Comprensión de las necesidades y expectativas de las partes interesadas.

Parte Interesada	Necesidades/Requisitos	Expectativas	Requisitos en el Sistema de Gestión de Seguridad de Información
Trabajadores	Pagos puntuales, experiencia en el rubro, capacitaciones, seguridad de la información. Recursos para el desempeño de sus funciones.	Mejora continua salarial, beneficios. Posibilidad de crecimiento y desarrollo del personal. Estabilidad y Buen clima laboral.	Recursos Humanos
Clientes	Seguridad de la información, precios accesibles, capacitaciones en los servicios adquiridos, cumplir con los lineamientos de SUNAT, soporte tecnológico y flexibilidad en la integración.	Solución rápida de requerimientos e incidentes. Comunicación Oportuna. Proactividad en el seguimiento posventa del servicio.	Gestión Comercial/ Contratos
Usuarios	Sistema confiable (sin errores), rapidez del sistema, seguridad de la información, accesibilidad y disponibilidad al sistema, sistema amigable, flexibilidad y soporte continuo.	Servicio sin interrupciones, capacitación y manuales de los servicios brindados, atención por personal con conocimiento multidisciplinario.	Gestión comercial/ mesa de ayuda
Proveedores	Cláusulas de seguridad definidas. Cumplimiento del pago de los productos y/o servicios contratados.	Contratos claros y legibles. Continuidad en las negociaciones que disponen. Competencia leal entre proveedores de la organización.	Área Administrativa y gerencial/ Contratos con cláusulas
Aliados estratégicos/ Partners	Alianzas continuas, soporte rápido, compatibilidad con sus soluciones, comunicación, cláusulas definidas dentro de los contratos y seguridad de información.	Comunicación de nuevas resoluciones de SUNAT.	Gestión Comercial/ Comunicación/ Contratos
SUNAT	Certificación ISO 27001, validación correcta de los comprobantes electrónicos, etc.	Seguir cumpliendo con los requisitos que le autorizaron para ser un OSE y PSE.	Cumplimiento

Entes gubernamentales	Cumplimiento legal, tributario y normativo.	Integración de medidas medioambientales.	Cumplimiento
MINSA	Cumplir con las resoluciones ministeriales y medidas adoptadas para el trabajo	Cumplimiento del plan para la vigilancia, prevención y control de covid-19 en el trabajo	Cumplimiento
Competidores	Evitar competencia desleal y evitar guerras de precios.	Veracidad en la información.	Gestión Comercial/ Estratégica
Accionistas	Rentabilidad, cumplimiento de las políticas y objetivos de la entidad.	Continuidad de la empresa, consolidación del grupo, etc.	Gestión estratégica
Alta dirección/Gerencia General	Rentabilidad, cumplimiento de las metas, productividad y maximizar beneficios.	La calidad del servicio, mejora continua de la empresa, etc.	Gestión estratégica

Bizlinks determina las partes interesadas que son pertinentes al sistema de gestión de seguridad de la información, además de los requisitos de estas partes interesadas, identificando a todas las personas u organizaciones que pueden afectar o ser afectadas por la gestión de la seguridad de la información o de la continuidad del negocio y todos los requisitos legales, normativos, contractuales y de otra índole que correspondan.

Para ello, con carácter anual, lleva a cabo el seguimiento y la revisión de la información sobre las partes interesadas durante la Revisión del Sistema por la Dirección.

2. Alcance

2.1. Alcance.

El propósito de la Gestión de Seguridad de la Información es alinear la seguridad con los objetivos del negocio y garantizar la gestión efectiva en todas las actividades de los servicios suministrados por la empresa.

El cumplimiento de los requisitos de esta norma para nuestro Sistema de Gestión de la Seguridad de la Información recoge en el presente Documento, al que denominamos **SI-MA-01 MANUAL DEL SGSI** y todos aquellos que se derivan de éste y que se citan en cada uno de los requisitos desarrollados.

El alcance de esta implementación y su posterior certificación comprende:

"Servicios especializados de facturación electrónica y comprobantes electrónicos PSE y OSE a nivel nacional"

N°	Procesos	Procesos Relacionados
1	Gestión de Emisión PSE	Comercial
		Implementación (Desarrollo, Proyectos y Producto)
		Post-Venta
2	Gestión de Validación OSE	Comercial
		Implementación (Desarrollo, Proyectos y Producto)
		Post-Venta

Se cuenta con el documento **SI-FR-28 Declaración de aplicabilidad**, donde se tiene desarrollado el anexo A de la norma ISO 27001, con la justificación de aplicabilidad y los documentos o registros correspondientes.

3. Gestión del Manual del Sistema de gestión de seguridad de la información

El **SI-MA-01 Manual del sistema de gestión de seguridad de la información** y los documentos que del mismo se derivan son de obligado cumplimiento para todos los trabajadores de la organización que deben velar por su confidencialidad y control, por lo cual se dispone del sistema documental original y completo, en los repositorios de la organización, adicionalmente, y si así lo considera oportuno el Responsable del Sistema y Gerencia General, se podrá realizar la distribución de la documentación a la parte interesada que lo solicite.

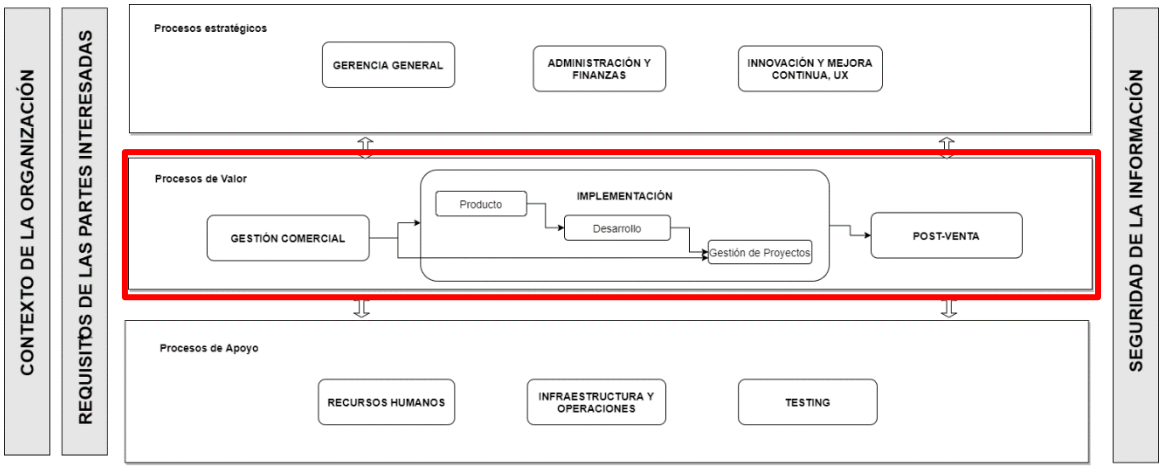
La redacción, control y emisión del Manual es competencia del responsable SGSI de la organización, así como de su revisión, difusión y archivo. La aprobación del **SI-MA-01 Manual del sistema de gestión de seguridad de la información** es responsabilidad del Gerente General.

4. Procesos definidos

Con el objetivo de dar cumplimiento a la política de seguridad, se han desarrollado los siguientes procesos:

4.1. Interacción de Procesos

Se tiene el presente mapa de procesos. Asimismo, se cuenta con fichas de caracterización por clausula y anexo A, en donde se mencionan las entradas ,salidas, registros, recursos, indicadores, entre otros.



5. Liderazgo y compromiso

5.1. Liderazgo y compromiso de la dirección

La alta dirección es la máxima responsable en el desarrollo e implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) y de que éste mejore continuamente. Para asegurar esto:

- La Dirección comunica a todos los trabajadores, mediante unos canales establecidos, la necesidad de satisfacer, determinar y cumplir los requisitos de seguridad de la información.
- Desarrolla una **POLÍTICA** y unos **OBJETIVOS** reales, medibles y coherentes con la realidad de la organización y las necesidades de seguridad.
- **POLÍTICA y OBJETIVOS** que son comunicados, entendidos y aplicados dentro de la empresa.

- Asegura la integración de los requisitos del sistema de gestión de seguridad de la información por procesos de negocio de la organización.
- Es responsable de asignar los recursos necesarios para implantar este SGSI y revisarlo periódicamente para verificar si se están alcanzando los objetivos y el buen funcionamiento del sistema.
- Promueve la toma de conciencia del enfoque basado en procesos.
- Comunica a la organización su compromiso con el presente SGSI, la importancia de una gestión eficaz y conforme con los requisitos SGSI.
- Asegura que el SGSI logre los resultados previstos.
- Involucra, dirige y apoya a las personas, para contribuir a la eficacia del sistema de gestión.
- Promueve la mejora continua.
- Apoya otros roles pertinentes de la Dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.
- Participación de la Dirección en foros, asociaciones profesionales especializadas en seguridad de la información y encuentros relativos a la seguridad de la información.

5.2. Política de Seguridad de la Información

La **SI-FR-02 Política del sistema de gestión de seguridad de la información** está expresada por la Dirección y archivada en los Documentos del Sistema de Seguridad de la Información para asegurar que es adecuada a la organización, al contexto de la organización, e incluye el compromiso de mejora continua.

Esta **POLÍTICA** es la base para establecer los **OBJETIVOS** de Seguridad de la Información, es entendida y comunicada a toda la organización y se revisa periódicamente.

La **POLÍTICA** está disponible para todas las partes pertinentes y ha sido comunicada, para su entendimiento y aplicación en la organización.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por la autoridad competente y son aprobados por la Dirección, el establecimiento de objetivos de seguridad se realizará atendiendo la ficha de proceso de **SI-FP-11 Seguimiento y medición de procesos** y se registrarán en el registro de objetivos.

Todos los objetivos deben ser revisados al menos una vez al año.

5.3. Funciones, responsabilidades y autoridad de la organización

Las autoridades en seguridad de la información quedan definidas por la Dirección, por medio del **AF-OT-01 Organigrama**.

Los roles y responsabilidades en seguridad de la información quedan definidos por la Dirección en el **Manual de Organización y Funciones MOF**, comunicados y archivados.

Así tiene definidas responsabilidades y competencias para todo el personal que dirige, realiza y verifica cualquier trabajo que incide sobre la seguridad de la información del servicio prestado, como se explica en el documento **AF-FP-01 Gestión de Recursos Humanos**.

La Dirección designa al puesto de Jefe Oficial de Seguridad de la información como responsable del Sistema de Gestión de Seguridad de la información, para asumir la responsabilidad y autoridad, con el objetivo de:

- Asegurarse que se establecen, implementan y mantienen los procesos necesarios para el Sistema de Gestión de la Seguridad de la Información.
- Informar a la alta dirección sobre el desempeño del Sistema de la Seguridad de la Información y de cualquier necesidad de mejora.
- Hay que asegurar que se promueva la toma de conciencia de los requisitos del cliente en todos los niveles de la organización.

6. Planificación

Bizlinks lleva la planificación del sistema de gestión de la seguridad de la información considerando el contexto y las expectativas de las partes interesadas de la organización, continuamente.

6.1. Acciones para tratar riesgos y oportunidades

Bizlinks considera esencial, identificar los posibles riesgos y elaborar una estrategia adecuada que le permita conocer el estado del sistema y adoptar las medidas necesarias para tratar los riesgos que pudieran derivarse. Por ello, identifica los riesgos y oportunidades que son necesarios tratar con el fin de:

- Asegurar que el Sistema de Gestión de la Seguridad de la Información, pueda lograr sus resultados previstos.
- Prevenir o reducir efectos indeseados.
- Lograr la mejora continua.

Adicionalmente, planifica:

- Las acciones para tratar estos riesgos y oportunidades.
- La manera de:
    - Integrar e implementar las acciones en sus procesos del Sistema de Gestión de la Seguridad de la información.
    - Evaluar la eficacia de estas acciones.

Para ello, dispone del **SI-FP-04 Apreciación de Riesgos**, por medio del cual se define y aplica un proceso de apreciación de riesgos de seguridad de la información en el cuál:

- Se establecen los criterios sobre los riesgos de seguridad de la información, en el que se incluyen los criterios de aceptación de riesgos y los establecidos para llevar a cabo las apreciaciones de riesgos.
- Se asegura que las sucesivas apreciaciones generan resultados consistentes, válidos y comparables.
- Se identifican los riesgos de seguridad de la información asociados a la pérdida de confidencialidad, integridad y disponibilidad, e identificando los dueños de los riesgos.
- Analizando las posibles consecuencias de la materialización de los riesgos, valorando la probabilidad y determinando los niveles de riesgos
- Valoración de riesgos considerando los criterios establecidos y la priorización en el tratamiento.

Así mismo, en la ficha de proceso se define el proceso de tratamiento de riesgos de seguridad de la información, en el cual:

- Se seleccionan las opciones adecuadas para el tratamiento de riesgos de seguridad de la información, y se determinan todos los controles necesarios para llevar a cabo dicho tratamiento.
- Se elabora la **SI-FR-28 Declaración de aplicabilidad** que contengan los controles necesarios y la justificación de la inclusión, estén implantados o no, además contienen la justificación de las exclusiones de los controles correspondientes al anexo A.
- Se formula el plan de tratamiento de riesgos de seguridad de la información.
- Se aprueba el plan de tratamiento de riesgos de seguridad de la información y se aceptan los riesgos de residuales por parte de los dueños de los riesgos.

El análisis de dicha apreciación y tratamiento de riesgos genera los siguientes registros: **SI-FR-12 Matriz de evaluación de riesgos y oportunidades, SI-FR-18 Matriz de apreciación de Riesgos de SI**

6.2. Objetivos de seguridad de la información y planificación para su consecución

Los objetivos generales de la empresa son:

- Garantizar que la información esté disponible y se puede utilizar cuando sea necesario.
- Garantizar que la información esté disponible exclusivamente para personas autorizadas.
- Garantizar que la información sea completa, precisa y esté protegida contra cambios no autorizados.
- Garantizar la confiabilidad de las transacciones y el intercambio de información entre empresas y asociados.
- Garantizar que el tratamiento de la información cumpla con las leyes y normativa sectorial que apliquen.

Bizlinks establece los **OBJETIVOS** de seguridad de la información en las funciones, niveles y procesos pertinentes. Estos objetivos:

- Son coherentes con la Política de Seguridad de la Información.
- Son medibles.
- Tienen en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y tratamiento de los riesgos.
- Son objeto de seguimiento.
- Son comunicados.
- Son actualizados, cuando es apropiado.

Asimismo, planifica los **OBJETIVOS,** determinando:

- Lo que se va a hacer.
- Los recursos que se necesitan.
- Los responsables.
- Plazos de finalización.
- Mecanismos de evaluación de los resultados.

7. Soporte

7.1. Recursos

La empresa tiene identificados y proporciona los recursos suficientes para garantizar el correcto funcionamiento del Sistema de Gestión de la Seguridad de la Información y mejorarlo, y para asegurar la Confidencialidad, Integridad y Disponibilidad de la información que soporta los servicios, actividades objeto de este sistema.

7.1.1. Personas

Para el desarrollo de la **POLÍTICA** de Seguridad de la Información y de las funciones y responsabilidades definidas, Bizlinks identifica las necesidades de recursos, de acuerdo con la planificación. Esto incluye la asignación de personal calificado para la realización de toda actividad recogida en el Sistema de Gestión de la Seguridad de la Información. Uno de los aspectos analizados durante la Revisión del Sistema por la Dirección, está relacionado con el contexto interno, más en concreto con el conocimiento. La organización muestra evidencia de la evaluación interna del conocimiento que atesora su personal, por medio del **SI-FR-01 Informe de Revisión por la dirección ISO 27001**.

La empresa, mediante la ficha de proceso de **AF-FP-01 Gestión de recursos humanos**:

- Tiene identificadas a aquellas personas que realizan trabajos que inciden sobre la Seguridad de la información.
- Ha determinado unos requisitos mínimos de formación, habilidades y experiencia apropiadas para asegurar la competencia de todos sus empleados, que afecta a su desempeño en seguridad de la información.

- La organización garantiza la satisfacción de las necesidades de cualificación del personal, proporcionando formación, y concientización de la importancia de las actividades que realizan y su relación con la seguridad de la información.
- Evalúa la eficacia de las acciones tomadas.
- Mantiene los registros adecuados de la educación, formación, habilidades y experiencia.

La sensibilización del personal en materia de seguridad de la información es un complemento indispensable a la hora de realizar actividades de formación. Las tareas de sensibilización tienen por objeto concientizar a todo el personal implicado en actividades que afecten a la seguridad de la importancia de su trabajo dentro del Sistema de Gestión de la Seguridad de la Información.

7.2. Competencia

La organización de Bizlinks:

- Determina la competencia necesaria, de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño de la Seguridad de la información.
- Determina la competencia real que atesora el personal tanto en los procesos de selección, como cuando se asignan otras responsabilidades diferentes al personal. Se considera la formación, experiencia y habilidades en el puesto a ocupar.
- Se toman las acciones necesarias para adquirir y desarrollar la competencia necesaria del personal, mediante el plan de formación.
- Se asegura de que estas personas sean competentes, llevando un seguimiento y evaluación mediante entrevistas personales, de cómo se ponen en práctica dichas competencias y registrando las incidencias observadas para adecuar mejor los medios a las necesidades de competencia detectadas.
- Se conserva la información documentada necesaria, como evidencia de dicha competencia.

Todo ello de acuerdo con lo documentado en la **AF-FP-01 Gestión de Recursos Humanos** y los formatos correspondientes.

7.3. Toma de conciencia

La empresa procura acciones de toma de conciencia, para el personal (propio y subcontratado) con la intención de sensibilizarlos en materia de:

- **POLÍTICA** de Seguridad de la Información.
- **OBJETIVOS** de Seguridad de la Información, pertinentes.
- Su contribución a la eficacia del Sistema de Gestión de la Seguridad de la Información, incluyendo los beneficios de una mejora del desempeño de la Seguridad.
- Las implicaciones de no cumplir los requisitos del Sistema de Gestión de la Seguridad de la Información.

7.4. Comunicación

Bizlinks determina las comunicaciones internas y externas pertinentes al sistema de gestión de Seguridad de la Información, que incluyen:

- El contenido de la comunicación.
- Cuando comunicar.
- A quien comunicar.
- Cómo comunicar.

Dentro de la comunicación interna, se considera fundamental que se trasmita a todo el personal el compromiso de la Alta Dirección con el sistema, la implantación de los controles de seguridad, definición de los niveles de riesgos, resultados de las auditorías, y que se creen las condiciones necesarias para una comunicación fluida y eficaz entre los distintos responsables que intervienen en un proceso.

Todo ello de acuerdo con lo documentado en la **SI-FP-05 Ficha de proceso de Gestión de la Comunicación.**

7.5. Información documentada

La información documentada para el sistema de gestión comprende, la requerida como tal por la propia Norma ISO 27001:2013 y la considerada como necesaria por Bizlinks, para asegurar la eficacia del sistema.

La documentación del sistema de gestión de Seguridad de la Información incluye:

- Una declaración documentada de la **SI-FR-02 POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** y de los **OBJETIVOS**.
- Un **SI-MA-01 MANUAL DEL SISTEMA**.
- Proceso de **SI-FP-04 APRECIACION DE RIESGOS.**
- Las **FICHA DE PROCESOS** necesarios.
- Otros documentos necesarios que garantizan el correcto funcionamiento del sistema.
- Los registros necesarios para demostrar la conformidad.

7.5.1. Control de la documentación

Bizlinks controla todos los documentos necesarios para el Sistema, detallado en la ficha de proceso **SI-FP-01 Gestión de la Información documentada.**

En esta ficha de proceso se definen los controles necesarios para:

- Aprobar los documentos antes de su emisión.
- Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
- Asegurarse de que se identifican los cambios y el estado de revisión actual de los documentos.

- Asegurarse de que las versiones pertinentes de los documentos aplicables se encuentran disponibles en los puntos de uso y que se defina el acceso adecuado.
- Asegurarse de que los documentos permanecen legibles y fácilmente identificables.
- Asegurarse de que se identifican los documentos de origen externo y se controla su distribución.
- Prevenir el uso no intencionado de documentos obsoletos y aplicarles una identificación adecuada en el caso de que se mantengan por cualquier razón.
- Identificar, almacenar, proteger, recuperar, retener y disponer de los registros.

7.5.2. Control de los registros

Se establece y mantiene los registros necesarios para proporcionar la evidencia de la conformidad con los requisitos.

Estos registros son legibles, están identificados, son recuperables, se protegen, se define el tiempo de conservación, lugar de conservación y se controlan. Son mantenidos en soporte papel e informático.

8. Operación

8.1. Planificación y control operacional

Bizlinks tiene planificados y desarrollados los procesos necesarios para cumplir con los requisitos necesarios para la **seguridad de la información** y para implementar las acciones derivadas del proceso de apreciación de riesgos. Esta planificación es coherente con los demás procesos del Sistema de Gestión de la seguridad de la información.

Durante esta planificación se ha tenido en cuenta:

- La **POLÍTICA** y los **OBJETIVOS de seguridad de la información.**
- Las apreciaciones de riesgos realizadas.
- Los cambios planificados y las consecuencias de los cambios no previstos.
- La necesidad de establecer procesos y documentos, así como los recursos humanos y materiales necesarios.
- Las etapas y actividades de control, verificación y seguimiento, así como los criterios de aceptación de riesgos y los responsables de llevarlas a cabo.
- Los registros necesarios para proporcionar evidencia de que los servicios cumplen los requisitos establecidos.
- Los procesos contratados externamente garantizando que estén controlados.

Para ello, se mantendrá la información documentada para garantizar que los procesos se han desarrollado según como estaba planificado. Además, se controlará cualquier cambio que se pudiera producir en la organización, así como se revisará las consecuencias de aquellos cambios

no previstos y se llevará a cabo las medidas oportunas para mitigar los efectos adversos en el caso de ser necesario.

Así mismo, la empresa controlará todos aquellos procesos que son contratados externamente.

Se dispone de una sistemática para la gestión de los cambios, de manera que éstos se realicen de forma planificada y sistemática. Para ello, se tiene en consideración:

- El propósito del cambio y cualquiera de sus potenciales consecuencias.
- La integridad del sistema de gestión.
- La disponibilidad de recursos.
- La asignación o reasignación de responsabilidades y autoridades.

Esta planificación de los cambios queda registrada en el formato **SI-FR-24 Informe de Cambio Mejora.**

8.2. Apreciación de riesgos de seguridad de información

La empresa efectuará las apreciaciones de riesgos de seguridad de la información a intervalos planificados y cuando se produzcan cambios o modificaciones importantes.

Para ello se ha establecido en la **SI-FP-04 Apreciación de Riesgos**, el análisis y el tratamiento de los riesgos de seguridad. Esta ficha de proceso establece los criterios y los pasos necesarios, desde la identificación de riesgos de seguridad de la información, hasta la implantación y seguimiento de los controles; permitiendo establecer el nivel de riesgo de cada uno de los servicios suministrados por la organización.

Se conserva los resultados de las apreciaciones de riesgos realizadas, en la **SI-FR-18 Matriz de apreciación de riesgos de SI**.

8.3. Tratamiento de los riesgos de seguridad de la información

La empresa implementará el plan de tratamiento de riesgos de seguridad de la información, guardando información documentada del mismo. El registro generado es el **SI-PL-04 Plan de Tratamiento de riesgos de SI**

9. Evaluación del desempeño

9.1. Seguimiento, medición, análisis y evaluación.

Se han aprobado una serie de documentos que pretenden garantizar la homogeneización y normalización de las actividades de seguimiento, medición, análisis y evaluación de los procesos de Bizlinks, con el fin de asegurar a la organización, que:

- Los controles de seguridad establecidos son implantados, y son eficaces.
- Las apreciaciones de riesgos realizadas.
- La gestión de incidentes de seguridad.
- Los procesos establecidos en la organización.
- El cumplimiento con las políticas de seguridad establecidas en la empresa.
- El Sistema de Gestión de Seguridad de la Información es conforme y se mantiene en constante evolución.

Gracias al funcionamiento dinámico del Sistema de Gestión de la Información se está mejorando de forma continua la organización.

La empresa determina:

- A que es necesario hacer seguimiento y que es necesario medir.
- Los métodos de seguimiento, medición, análisis y evaluación, según aplique, para asegurar resultados válidos.
- Cuando se deben llevar a cabo el seguimiento y la medición.
- Cuando se deben analizar y evaluar los resultados del seguimiento y la medición.

Para asegurar que los procesos permiten alcanzar los requisitos que los clientes exigen, y los **OBJETIVOS** de seguridad de la información que la organización se ha marcado, se lleva a cabo el seguimiento y medición de los procesos, demostrando de este modo la capacidad para alcanzar los resultados planificados. Estas actividades permiten evaluar los procesos de forma continua tomando las medidas oportunas, y, en caso de necesidad, corregir las no conformidades que se detecten, antes de que éstas puedan influir de algún modo a las actividades de la empresa.

Para medir los principales procesos de la organización se emplea una sistemática basada en unos indicadores que se gestionan de acuerdo con la ficha de proceso de **SI-FP-11 Seguimiento y medición de procesos.**

Cuando no se alcanzan los resultados esperados se aplica la ficha de proceso de **SI-FP-02 Gestión de No Conformidades.**

Todos los datos obtenidos como consecuencia de la implantación del Sistema de Gestión de Seguridad de la Información dan una información relevante sobre el funcionamiento de este y sobre el estado general de la organización. Para ello la organización determinará:

- La gestión de riesgos de seguridad de la información y controles aplicados.
- A qué se necesita hacerle seguimiento, qué es necesario medir, sin olvidar incluir procesos y controles de la seguridad de la información.
- Las técnicas de seguimiento, medición, análisis y evaluación requeridas para garantizar que los resultados son válidos.

- Cuando se ha de ejecutar tanto el seguimiento como la medición.
- Quién es el responsable de la ejecución del seguimiento y medición.
- Cuando es necesario analizar y evaluar los resultados de seguimiento y medición.
- Quién será el responsable de analizar y evaluar dichos resultados.

Existe una ficha de proceso documentado para la gestión de los indicadores llamado **SI-PR-01 SEGUIMIENTO DE INDICADORES**. Dichos indicadores son analizados en el preciso instante en el que son completados, tomando las acciones oportunas, aunque también son analizados durante la Revisión de Sistema por la Dirección.

9.2. Auditoría Interna

Para evitar en lo posible que los clientes de la organización lleguen a estar insatisfechos, se ha establecido una ficha de proceso documentado **de SI-FP-06 Gestión Auditoría Interna**, por el que se regula el modo de evaluar a la organización para poder detectar sus puntos débiles que se deben evitar, y los puntos fuertes que se deben potenciar. Para ello son auditados los departamentos implicados en el Sistema de Gestión de Seguridad de la Información, asegurando que:

- Está conforme con los requisitos propios de la organización para su sistema de seguridad de la información, con las actividades planificadas y con los requisitos de la Norma Internacional ISO 27001 tomada como referencia.
- Está implantado, actualizado y funciona de forma eficiente.

La Ficha de proceso de **SI-FP-06 Gestión Auditoría Interna** asegura la planificación, el alcance, plazo e imparcialidad de las auditorías. Se identifican los responsables y se garantiza la puesta en marcha de acciones para eliminar las no conformidades.

9.3. Revisión por la Dirección

Las Revisiones del Sistema de Gestión de la Seguridad de la Información son realizadas por la Dirección al menos una vez al año y siempre después de haber realizado, mínimo una auditoría interna a cada uno de los departamentos de la organización, según lo previsto en el **SI-FR-01 Informe de Revisión por la dirección ISO 27001**, de acuerdo con lo descrito en este manual.

Los asistentes a estas Revisiones del Sistema por la Dirección son:

- Alta Dirección.
- Oficial de SI o responsable del Sistema de Gestión de Seguridad de la información.
- Personal de otras áreas que gerencia general estime oportuno en función de los temas a tratar (dueños de procesos).

Durante la Revisión por la Dirección, se analiza el estado de ejecución de las auditorías planificadas para el año en curso y se planifica el programa de auditorías para el siguiente año dejando

evidencia de ello en el **SI-FR-01 Informe de Revisión por la dirección ISO 27001**, teniendo en cuenta todas las actividades incluidas en dichos sistemas.

En el caso de que se produzcan cambios importantes en la organización, los procesos, en la **POLÍTICA** de la empresa, se realizarán Revisiones del Sistema extraordinarias, sobre todo en aquellos casos en los que se detecte un descenso del nivel de seguridad ofrecido a los clientes.

9.3.1. Información de entrada para la revisión

La Gerencia general, para llevar a cabo la Revisión del Sistema, recopila toda la información necesaria que le facilita el Responsable de Seguridad de la información. La información que se utiliza es la que se ha generado a partir de la última Revisión del Sistema.

En la revisión se realiza el análisis de:

- **POLÍTICA** y **OBJETIVOS** de la Seguridad vigentes.
- Resultados y seguimiento de las Revisiones anteriores del Sistema por la Dirección.
- Los cambios en las cuestiones internas y externas que sean pertinentes al Sistema de Gestión.
- La información sobre el desempeño y la eficacia del sistema de gestión de seguridad de la información, relacionadas con:
    - Informes de auditorías internas y externas.
    - No conformidades y acciones correctivas.
    - Incidentes de seguridad.
    - Indicadores del Sistema de Gestión.
    - Cumplimiento de los objetivos de seguridad de la información.
- Cometarios provenientes de las partes interesadas.
- La adecuación de los recursos.
- Resultados de la apreciación al riesgo: Análisis de riesgos, el plan de tratamiento de riesgos, y las métricas de seguridad.
- Las oportunidades de mejora.
- Verificación del cumplimiento de control y supervisión previstos en los activos de información con revisión expresa en: Copias de Seguridad, Accesos e Intrusiones, uso de la red y cumplimiento de políticas por parte de los trabajadores.
- Previsión de necesidades y objetivos futuros.
- Otros factores que puedan afectar al funcionamiento de la empresa y al Sistema de Gestión de la Seguridad de la Información.
- Cambios internos y/o externos que afecten al SGSI.

A partir de los datos anteriores, la Dirección verifica que el Sistema de Seguridad de la Información es eficaz y que se están obteniendo resultados que confirman el cumplimiento de la **POLÍTICA** y **OBJETIVOS** planteados. Así mismo, se determina que el Sistema está de acuerdo con los requisitos de la Norma ISO 27001.

9.3.2. Resultados de la revisión

Los resultados obtenidos en la Revisión del Sistema por la Dirección deben incluir las decisiones tomadas referidas a:

- La mejora de la eficacia del Sistema de Gestión de Seguridad de la Información y de los controles y procesos de seguridad de la información.
- Las oportunidades de mejora continua.
- Las necesidades de cambio en la gestión del SGSI.
- Las necesidades de recursos.

Estos resultados se reflejan en el registro **SI-FR-01 Informe de Revisión por la dirección ISO 27001**, y si procede, éstos serán comunicados por el Responsable de Seguridad de la información, al resto del personal de la organización.

10. Mejora

10.1. No Conformidades y acción correctiva

Conscientes de que, pese a todos los controles realizados sobre los activos de información de la empresa, es fácil que aparezcan no conformidades asociadas al sistema de gestión, por ello se ha desarrollado la ficha de proceso documentada de **SI-FP-02 Gestión de No Conformidades,** por el que se definen las acciones que se adoptan para:

- Eliminar las causas que originan las no conformidades detectadas.
- Identificar las posibles modificaciones en los riesgos y conferirles acciones necesarias para su tratamiento.
- Tomar las acciones encaminadas a prevenir su empleo en las aplicaciones inicialmente pensadas.
- La verificación de los que hayan sido corregidos.
- La adopción de medidas de control cuando se ha detectado su presencia tras la entrega de este.
- El registro de todos los datos relacionados con lo anterior.

Las no conformidades, incluidas las acciones correctivas con las operaciones establecidas por la organización, y el proceso de gestión, incluso las quejas que provienen de las partes interesadas.

10.2. Mejora

Bizlinks pretende la mejora continua, a través del empleo de su **POLÍTICA** de Seguridad de la Información, **OBJETIVOS** de Seguridad de la Información, resultados de Auditorías y el análisis de todos los datos, que permiten la adopción de Acciones Correctivas y Planes de Mejora.

La organización tiene en consideración los elementos de salida del análisis, la evaluación, y los elementos de salida de la revisión por la dirección para confirmar si hay tareas de bajo desempeño, u oportunidades que deban tratarse como parte de la mejora continua. Toda actividad de mejora queda plasmada en el **SI-FR-24 Informe de Cambio Mejora.**

11. Documentos de referencia

Todos los documentos necesarios en esta ficha de proceso se relacionan a continuación:

- **SI-MA-01** Manual del SGSSI
- **SI-FR-02** Política de Seguridad de la información
- **SI-FR-28** Declaración de aplicabilidad
- **SI-FP-01** Gestión de la Información documentada
- **AF-FP-02** Relación con proveedores
- **SI-FP-03** Gestión de activos
- **SI-FP-10** Organización SI
- **SI-FP-12** Control de acceso
- **SI-FP-07** Áreas Seguras
- **SI-FP-13** Seguridad de los equipos
- **SI-FP-15** Seguridad Operativa
- **SI-FP-17** Seguridad de las comunicaciones
- **SI-FP-18** Requisitos de seguridad
- **SI-FP-19** Seguridad en el desarrollo y procesos de soporte
- **SI-FP-02** Gestión de No conformidades
- **SI-FP-05** Ficha de proceso de Gestión de la comunicación
- **AF-FP-01** Gestión de Recursos Humanos
- Perfiles de puestos
- **SI-FP-04** Apreciación de riesgos
- **SI-FR-01** Informe de Revisión por la dirección ISO 27001.
- **SI-FP-20** Continuidad del negocio
- **SI-FP-08** Gestión de incidentes
- **SI-FP-09** Cumplimiento de requisitos legales
- **SI-FR-17** Metodología de evaluación de riesgos y oportunidades
- **SI-FP-16** Gestión de Cambio Mejora
- **SI-FR-24** Informe de Cambio Mejora
- **SI-FP-06** Gestión de Auditoría Interna
- **SI-FP-11** Seguimiento y medición de procesos