POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	REPOSI01
Versión:	05
Creado por:	Johanna Viveros - Jefe del Sistema Integrado de Gestión
Revisado por:	Jaime Vélez – Director Corporativo de Administración y Finanzas
Aprobado por:	Comité de TI
Fecha de la versión:	04-02-2024

Historial de modificaciones

Fecha	Versión	Creado / Modificador por	Descripción de la modificación
01-04-2021	0	Gustavo Sanchez - Coordinador de SI	Documento creado.
29-07-2021	1	Gustavo Sanchez - Coordinador de SI	Aprobación de la política por la alta dirección.
19-01-2023	2	Johanna Viveros - Coordinador del Sistema Integrado de Gestión	Eliminación del índice. Cambios en la estructura del documento: Se reemplazan los numerales de "Finalidad, Ámbito de la aplicación, Objetivos, Principios generales, Responsabilidades, Implementación, Control y Auditoría, Comunicación de la política y Alta Dirección" por: "Objetivo, Alcance, Terminología, Documentos de referencia, Consideraciones generales, Control y seguimiento, Comunicación de la política, Actualización y revisión. Definición del objetivo de la política, según el alcance del SGSI y la certificación bajo la norma 27001:2013. Especificación del alcance del SGSI, de manera resumida y aplicable. Se crea numeral con la declaración de la política. Se replantean los objetivos del SGSI. Se reemplaza numeral Principios y por Lineamientos Generales. Se replantean roles y responsabilidades: Colaboradores, Área de TI, Área de SIG, Terceros y Alta Dirección. Control y seguimiento, Comunicación de la política, Actualización y revisión: Se resume y mejora la redacción. Firma: Se elimina firma de responsable de TI y del SIG.
15/11/2023	3	Johanna Viveros – Jefe del Sistema Integrado de Gestión	Consolidación de políticas de cada país a una regional. Mejora en la redacción y ampliación del alcance, incluyendo aplicación completa a Perú. Ajuste a nuevo formato de políticas y procedimientos del SIG. Cambio de código, por categoría regional.
28/10/2024	4	Johanna Viveros – Jefe del Sistema Integrado de Gestión	Ampliación del alcance: Inclusión de Argentina. Actualización general de lineamientos, según nueva versión ISO27001:2022
16/01/2025	5	Johanna Viveros – Jefe del Sistema Integrado de Gestión	Ampliación del alcance: Inclusión de Ecuador. Mejoras en la redacción de los objetivos del SGSI.

1. OBJETIVO

Establecer los lineamientos de seguridad de la información y ciberseguridad que deben cumplir los procesos de Belltech.

2. ALCANCE

Aplica a todos los procesos de Belltech Argentina, Chile, Colombia, Ecuador, Perú y sus aliados que participan en la provisión de soluciones digitales y servicios tecnológicos en comunicaciones unificadas, sistemas de autoservicios y puntos de venta.

Esta política podrá hacerse extensiva a los procesos de Belltech de toda la región, cuando sea aplicable, total o parcialmente.

3. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2022
- REMNSI01 Manual de Seguridad de la Información

4. DEFINICIONES

Activo de Información	Elemento o medio que almacena o procesa información.
Auditoría	Análisis de procesos y activos de información, para identificar los fallos, incumplimiento y oportunidades de mejora.
Cifrado	Proceso que garantiza la confidencialidad de la información. Los datos se codifican y sólo se pueden acceder con clave y algoritmo acordado entre las partes.
Confidencialidad	Propiedad de la información, que garantiza que sea accedida únicamente por el personal autorizado.
Disponibilidad	Propiedad de la información, que garantiza que esté disponible cuando se requiera.
Evento	Cualquier ocurrencia sobre activos o entorno, que indique un posible compromiso de las políticas o controles, que pueda afectar a la seguridad.
Incidente	Evento que compromete las operaciones de la compañía. Puede ser un incumplimiento de las políticas del SGSI o un riesgo materializado.
Integridad	Propiedad de la información que garantiza la exactitud de los datos, sin alteración, pérdida o destrucción.
SGSI	Sistema de Gestión de Seguridad de la Información.
SIG	Sistema Integrado de Gestión.
Tercero	Persona natural o jurídica que no es parte directa de la compañía, pero mantiene una relación con ésta. Por ejemplo, clientes, proveedores, entes de control.
Vulnerabilidad	Debilidad de seguridad en los activos de información.

5. CONDICIONES GENERALES

Los controles implementados en el SGSI, beneficia a todos los clientes internos y externos; proyectando sus acciones en la conservación de los recursos tecnológicos, infraestructura y de información, diseñando e implementando planes de acción de seguridad de la información y mejora continua, enfocados en minimizar los incidentes de seguridad de la información y ciberseguridad.

Belltech desarrolla procedimientos para adoptar buenas prácticas de seguridad de la información, implementar y dar cumplimiento a las obligaciones legales, normativas y contractuales, incluyendo prácticas ambientales responsables, en cada actividad de los procesos.

Se documenta la Declaración de Aplicabilidad, correspondiente al diseño, implementación, mantenimiento y mejora del SGSI de Belltech.

5.1. Alcance del SGSI.

"Provisión de soluciones digitales y servicios tecnológicos en: comunicaciones unificadas, sistemas de autoservicios y puntos de venta en Belltech Argentina, Chile, Colombia, Ecuador y Perú".

5.2. Declaración de la política.

Belltech declara la siguiente Política de Seguridad de la Información, como eje principal del SGSI, para la definición de otras políticas, manuales, procedimientos e instructivos.

"Belltech está comprometida con la protección de la confidencialidad, integridad y disponibilidad de la información propia y de sus aliados, en sus procesos para proveer soluciones digitales y servicios tecnológicos en comunicaciones unificadas, sistemas de autoservicios y puntos de venta; mediante la gestión de riesgos, el cumplimiento de requisitos legales y otros relacionados con la seguridad de la información y comprometiéndose con la mejora continua de su sistema de gestión de seguridad de la información".

5.3. Objetivos del SGSI.

A continuación, se enuncian los objetivos de seguridad de la información, que se buscan alcanzar, mediante la implementación del SGSI.

- Velar por que los colaboradores y procesos garanticen la confidencialidad, integridad y disponibilidad de la información y servicios de Belltech y sus aliados.
- Definir, implementar y mantener controles y buenas prácticas de seguridad de la información, aplicable al negocio.
- Identificar, valorar y gestionar los riesgos asociados a la seguridad de la información.
- Promover el cumplimiento del 100% de los requisitos legales, normativos y contractuales aplicables, referentes a la seguridad de la información.

5.4. Lineamientos generales.

5.4.1. Requisitos de la norma.

Se presentan las definiciones generales, para la implementación del SGSI de Belltech, relacionados con la ISO/IEC 27001:2022.

Contexto de la organización	Entender la organización y su contexto. Comprender las necesidades y expectativas de las partes interesadas. Determinar el alcance del sistema de gestión de seguridad de la información. Implementar y mantener el Sistema de gestión de seguridad de la información.
Liderazgo	Demostrar el liderazgo y compromiso de la Alta Dirección. Disponer y comunicar la política de seguridad de la información. Asignar funciones, responsabilidades y autoridades de la organización.
Planificación	Gestionar Riesgos y oportunidades de seguridad de la información. Gestionar los objetivos de seguridad de la información. Planificar cambios del sistema de gestión.
Soporte	Proporcionar recursos para el SGSI. Determinar competencias para el SGSI. Generar conciencia sobre seguridad de la información. Determinar las comunicaciones internas y externas.
Información documentada	Crear documentos del SGSI. Mantener los documentos actualizados.
Operación	Planificar y controlar los procesos operativos. Evaluar los riesgos de seguridad de la información Tratar los riesgos de seguridad de la información.
Evaluación del desempeño	Hacer seguimiento, medición, análisis y evaluación. Ejecutar auditorías internas. Realizar revisiones por la Dirección.
Mejora	Mejorar continuamente el SGSI.

5.4.2. Requisitos del Anexo.

Se deben implementar los siguientes controles, de acuerdo con su correspondiente justificación y documentar detalladamente en las políticas, manuales, procedimientos e instructivos.

- Controles organizacionales:

Políticas de seguridad de la información	La definición, aprobación y seguimiento por la Alta Dirección garantiza que las directrices en seguridad de la información estén alineadas con los objetivos estratégicos de Belltech y apoye los proyectos requeridos.
Roles y responsabilidades de seguridad de la información	Cada colaborador debe conocer las funciones y capacidades para desempeñar sus funciones, dentro del marco de seguridad de la información.
Segregación de deberes	El personal encargado de la gestión de la seguridad de la información no cuenta con permisos de administración en la plataforma tecnológica y es independiente de las áreas de operación y apoyo.
Responsabilidades de gestión	La participación de la Alta Dirección en las definiciones, divulgación y exigencia de cumplimiento apalanca la sensibilización y aumenta el grado de compromiso en todos los niveles.

Contacto con autoridades	Apoya la mitigación de riesgo legal y contractual, comunicar a partes interesadas.
Contacto con grupos de interés especial	Apoya la mitigación de riesgos, relacionada con incumplimiento normativo y buenas prácticas, en seguridad de la información.
Inteligencia de amenazas	La gestión de amenazas operativa y automatizada permite actuar adecuadamente, de manera preventiva y reactiva.
Seguridad de la información en la gestión de proyectos	Durante las etapas de los proyectos, se deben contemplar los criterios de seguridad de la información, para minimizar riesgos en la operación.
Inventario de información y otros activos asociados	El inventario actualizado permite identificar y gestionar riesgos relacionados, para cada proceso.
Uso aceptable de la información y otros activos asociados	La entrega formal de responsabilidades sobre los activos de activos de información genera conciencia y mejor uso.
Devolución de activos	Permite controlar los accesos e información corporativa, durante su uso.
Clasificación de la información	Permite identificar riesgos y controles que se deben implementar, en función de los requisitos legales, valor, criticidad y vulnerabilidades.
Etiquetado de información	Permite que las partes interesadas conozcan la clasificación y traten la información correctamente.
Transferencia de información	Agiliza los procesos, protege los datos en tránsito y designa responsabilidades por las partes.
Control de acceso	La gestión de riesgos se simplifica, al permitir acceso a instalaciones, activos, información y servicios, de acuerdo con la necesidad de cada rol.
Gestión de identidad	Los procedimientos para asignar, modificar y eliminar permisos de usuario, según rol y responsabilidades, mitiga riesgos de seguridad de la información.
Información de autenticación	La protección de datos de autenticación protege sistemas, datos, redes y aplicaciones, frente a acceso no autorizado y garantizar el no repudio.
Derechos de acceso	La modificación y cancelación de permisos, garantiza que la información y servicios sólo sean accedidos por personal autorizado.
Seguridad de la información en las relaciones con los proveedores	La información debe ser protegida en todos los ambientes en donde sea tratada. La gestión de riesgos debe contemplar activos internos y externos.
Seguridad de la información en los acuerdos con los proveedores	Las cláusulas de seguridad de la información en los acuerdos con terceros permiten conocer el grado de responsabilidad de las partes, implementar y hacer seguimiento a su cumplimiento.
Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación	La seguridad de la cadena de suministro protege la integridad física, protege ante amenazas cibernéticas, controla amenazas relacionadas con disponibilidad, capacidad, integridad y confidencialidad.
Seguimiento, revisión y gestión de cambios de servicios de proveedores	El control de cambios ayuda a adaptarse constantemente al mercado, sin dejar de implementar controles eficaces de seguridad de la información.
Seguridad de la información para el uso de servicios en la nube	La información debe ser protegida en todos los ambientes en donde sea tratada. La gestión de riesgos debe contemplar activos internos y externos.
Planificación y preparación de la gestión de incidentes de seguridad de la información	Entrega una guía a partes interesadas de las acciones a tomar, canales y escalas de comunicación.
Evaluación y decisión sobre eventos de seguridad de la información	La correcta clasificación y valoración de eventos ayuda a reconocer y abordar posibles amenazas y vulnerabilidades de seguridad, anticipadamente.
Respuesta a incidentes de seguridad de la información	La reacción oportuna y adecuada ofrece una recuperación en tiempo aceptable, minimiza impactos y puede prevenir que ocurran nuevamente.
Aprender de los incidentes de seguridad de la información	Las lecciones aprendidas permiten conocer cómo abordar situaciones, activar planes exitosos, evitar acciones ineficaces y apoyar la mejora continua.

Recolección de evidencia	La custodia permite evidenciar activos afectados, personas que participan, tiempos de acción y cumplimiento de procesos.
Seguridad de la información durante la interrupción	Un Análisis de Impacto al Negocio identifica escenarios de discontinuidad, predecir consecuencias, comprender y definir alternativas.
Preparación de las TIC para la continuidad del negocio	Los planes de contingencia deben ser reales, aplicables al negocio y eficaces, para cumplir con los niveles de riesgos aceptables.
Requisitos legales, estatutarios, reglamentarios y contractuales	Conocer y compilar los requisitos aplicables ayuda en la identificación de necesidades, asignación de responsables, seguimiento y escalamiento.
Derechos de propiedad intelectual	Garantiza las creaciones intelectuales, favorece la competencia leal, fomenta el intercambio de conocimientos y mitiga riesgos de incumplimiento legal.
Protección de registros	Se deben implementar medidas de protección que mitiguen riesgos sobre datos propios y de terceros.
Privacidad y protección de la información de identificación personal (PII)	La implementación de controles tecnológicos, programas de concienciación e inclusión de cláusulas obligatorias en contratos laborales y comerciales promueven el cumplimiento de la reglamentación vigente relacionada.
Revisión independiente de la seguridad de la información	Para una validación objetiva sobre la aplicación de medidas, se ejecutan auditorías internas y externas sobre los procesos, por personal independiente de las áreas de operación y apoyo.
Cumplimiento de políticas, normas y estándares de seguridad de la información	El monitoreo y revisión constante permiten realizar un seguimiento al sistema de gestión, para actuar adecuadamente y apoyar el cumplimiento de lineamientos, requisitos legales, normativos y contractuales.
Procedimientos operativos documentados	La formalización de procedimientos escritos facilita la capacitación de personal nuevo, consulta y seguimiento a los procesos establecidos.

- Controles de personas:

Selección	La verificación de antecedentes ayuda a determinar si los colaboradores pueden desempeñar un cargo y mitiga riesgos de afectación de la imagen de Belltech, costos por mala contratación, inseguridad y fraude.
Términos y condiciones de empleo	La documentación formal permite comprender y garantizar el cumplimiento de las condiciones de las partes.
Concientización, educación y capacitación en seguridad de la información	Los programas de capacitación y concienciación promueven la cultura de comprensión de riesgos y prácticas de seguridad de la información.
Proceso disciplinario	Un proceso formal facilita el análisis y toma de decisiones, ante faltas de responsabilidad de los colaboradores.
Responsabilidades después de la terminación o cambio de empleo	Cada colaborador debe conocer las responsabilidades, para evitar conflictos y proteger los intereses de Belltech al finalizar la relación laboral.
Acuerdos de confidencialidad o no divulgación	Los acuerdos firmados impiden que los secretos comerciales y patentes sean divulgados o tratados con un fin que favorezca a terceros no autorizados.
Trabajo remoto	Se requiere proteger la información y activos, cuando los colaboradores se encuentran fuera de las instalaciones físicas.
Informes de eventos de seguridad de la información	Los canales de comunicación conocidos y disponibles permiten atender por personal responsable y llevar registros reales de eventos o incidentes.

- Controles físicos:

Perímetros físicos de seguridad	Los perímetros restringidos y vigilados hacen parte de la seguridad en profundidad, definida en Belltech, para proteger los activos de información.
Entrada física	La protección física proporciona un nivel de seguridad, para minimizar los riesgos de acceso no autorizado en las instalaciones de Belltech.

Asegurar oficinas, salas e instalaciones	La protección física proporciona un nivel de seguridad, para minimizar los riesgos sobre los activos de información en las instalaciones de Belltech.
Monitoreo de seguridad física	El registro y revisión de elementos de control de acceso permite detectar y analizar situaciones no deseadas en las instalaciones de la compañía.
Protección contra amenazas físicas y ambientales	La ubicación geográfica de las oficinas y el uso de infraestructura tecnológica requiere de controles frente a amenazas físicas y ambientales que puedan poner en riesgo la integridad de los activos y continuidad del negocio.
Trabajar en áreas seguras	Belltech identifica áreas en donde se almacena y procesa activos de información que requieren estrategias de seguridad física.
Escritorio despejado y pantalla despejada	Por la distribución física de las oficinas y forma de trabajo, se requiere proteger la información, para evitar acceso por personal no autorizado.
Emplazamiento y protección de equipos	Según la distribución física de las oficinas y forma de trabajo, se requiere proteger los equipos, para evitar manipulación por personal no autorizado.
Seguridad de los activos fuera de las instalaciones	De acuerdo con las necesidades comerciales y forma de trabajo, se requiere proteger los activos cuando se encuentran fuera de las instalaciones físicas.
Medios de almacenamiento	La compañía utiliza dispositivos tecnológicos susceptibles a fallas, cambios y obsolescencia, que deben ser tratados, para proteger la información.
Utilidades de apoyo	La compañía utiliza dispositivos tecnológicos que dependen del insumo eléctrico para su funcionamiento, necesarias para la operación de Belltech, las cuales requieren ser protegidas y respaldadas.
Seguridad del cableado	La compañía utiliza dispositivos tecnológicos que dependen de conexiones físicas para su funcionamiento, que requieren ser protegidas y respaldadas.
Mantenimiento de equipo	El mantenimiento programado y adecuado asegurar el funcionamiento y disponibilidad de equipos, al minimizar fallas y averías.
Eliminación segura o reutilización de equipos	Los colaboradores de Belltech reutilizan dispositivos tecnológicos en buena condición. Por lo tanto, se deben proteger los activos lógicos asociados.

- Controles tecnológicos:

Dispositivos de punto final de usuario	Los controles evitan que la información clasificada de Belltech y terceros, sea alcanzada por usuarios no autorizados y reducen el riesgo de ciber amenazas.
Derechos de acceso privilegiado	Se requiere proteger el escalamiento de privilegios, ante amenazas internas y externas, mediante el aseguramiento de cuentas del personal que administra la infraestructura tecnológica y garantizando que sólo ingresan a los activos que se requieren, con los permisos mínimos requeridos.
Restricción de acceso a la información	Para proteger la información de Belltech y terceros, asegurando cuentas de usuario, para que sólo ingresen a activos requeridos, con mínimos privilegios.
Acceso al código fuente	Se requiere proteger el código fuente de productos desarrollados, para que sólo sea accedido por el personal autorizado y se controlen sus cambios.
Autenticación segura	Es necesario probar la identidad de los usuarios, antes de obtener acceso a sistemas, minimizando riesgos relacionados con acceso no autorizado.
Gestión de capacidad	El constante crecimiento y mejora de la plataforma tecnológica requiere planificar la ocupación de activos de información.
Protección contra malware	Constituye una capa de protección fundamental para personas y dispositivos vulnerables que hacen parte de la arquitectura empresarial.
Gestión de vulnerabilidades técnicas	Facilita la identificación, priorización y reacción, ante riesgos de convertirse en objetivos de ataques que ponen en riesgo la información o servicio.
Gestión de la configuración	La revisión adecuada de las configuraciones de activos de información minimiza riesgos sobre la información y el servicio.
Eliminación de información	El proceso de sanitización minimiza riesgos de seguridad de la información que ya no se encuentra en uso y control, y respalda el cumplimiento de contratos y regulaciones de protección de datos.

Enmascaramiento de datos	El enmascaramiento, en Ciclo de Desarrollo, permite trabajar con datos de prueba realistas, sin exponer información confidencial.
Prevención de fuga de datos	Los controles minimizan riesgos sobre envío de información clasificada a personas no autorizadas, garantizando el cumplimiento de requisitos.
Copia de seguridad de la información	Ofrece la capacidad de restaurar datos y sistemas a un estado deseado, reduciendo el riesgo de pérdida, en caso de eventos inesperados.
Redundancia de las instalaciones de procesamiento de información	Las redundancias definidas por Belltech evitan pérdida de datos e interrupción de procesos críticos, ante daños o ciberataques.
Inicio de sesión	El resguardo y verificación del historial de inicios de sesión de sistemas de información permite tener alertas tempranas e información para realizar análisis eficaz, ante posibles eventos o incidentes de seguridad.
Actividades de seguimiento	El resguardo y verificación de registro de eventos en sistemas de información permite tener alertas tempranas e información para realizar análisis eficaz, ante posibles eventos o incidentes de seguridad.
Sincronización de reloj	Garantiza que los procesos se ejecuten de forma cronológica, asegura que los registros reflejen el tiempo real de ejecución y facilita el análisis de información para diagnósticos o monitoreos.
Uso de programas de utilidad privilegiados	La administración de plataforma tecnológica puede ser compartida por varias personas habilitadas, para de garantizar la administración y funcionamiento.
Instalación de software en sistemas operativos	El control facilita a los administradores de TI: el versionamiento de aplicaciones, distribución de licencias, consumo de recursos, gestión de vulnerabilidades, cumplimiento legal y control de acceso.
Seguridad en redes	Los controles preventivos y reactivos sobre el acceso no autorizado, uso indebido, alteración o denegación de la red y sus recursos, brindan protección sobre el acceso, uso e integridad de la red y los datos.
Seguridad de los servicios de red	La completa identificación de servicios y requisitos promueve la gestión adecuada de sus riesgos asociados.
Segregación de redes	La segmentación ayuda a impedir el acceso a usuarios no autorizados, ejerce un control granular sobre el tráfico de la red y mejora su rendimiento.
Filtrado web	El control del contenido minimiza los riesgos de ciberseguridad operativos y tecnológicos.
Uso de criptografía	El cifrado expone la información únicamente a usuarios autorizados, asegura que no se ha manipulado y confirma su autenticidad o identidad.
Ciclo de vida de desarrollo seguro	Los controles en el desarrollo de software reducen vulnerabilidades, mitiga el impacto por explotación, analiza causas raíz, minimiza incidentes futuros y refuerza la confianza de clientes.
Requisitos de seguridad de la aplicación	La completa identificación y atención de requisitos evita reprocesos, garantiza la aceptación de terceros y cumplimiento contractual.
Principios de arquitectura e ingeniería de sistemas seguros	La implementación de una metodología estable y probada permite corregir desviaciones y mantener el sistema protegido en producción.
Codificación segura	Mantiene estándares de codificación eficientes, para evitar errores que den lugar a amenazas que aprovechen vulnerabilidades de seguridad.
Pruebas de seguridad en desarrollo y aceptación	Evalúan la eficacia de los controles de seguridad e identifican nuevas vulnerabilidades en el software.
Desarrollo subcontratado	En la subcontratación se requiere una visión clara de requerimientos, evaluación de viabilidad y capacidades del tercero, seguimiento durante y posterior a las actividades, para garantizar el cumplimiento de los objetivos.
Separación de los entornos de desarrollo, prueba y producción	La separación de entornos reduce los riesgos de acceso no autorizado y cambios no controlados en el ambiente de operación.
Gestión del cambio	Los cambios controlados facilitan la implementación exitosa, sin afectar la continuidad del negocio y seguridad de la información.

Información de prueba	Los datos de prueba reducen riesgos de privacidad y permiten evaluar el rendimiento, seguridad y funcionalidad, sin afectar los datos reales.
Protección de los sistemas de información durante las pruebas de auditoría	Durante las actividades de auditoría interna y externa se debe seguir garantizando el adecuado tratamiento de la información, de acuerdo con los niveles de clasificación.

5.5. Control y seguimiento.

Belltech adopta medidas de vigilancia y control, para comprobar la correcta utilización de los sistemas que pone a disposición de sus colaboradores, incluyendo el contenido de las comunicaciones y dispositivos, respetando, la legislación vigente y garantizado la dignidad de cada persona.

Belltech se someterá a revisiones periódicas, como auditorías internas y externas, para verificar el cumplimiento de esta política y demás documentos del SGSI.

El incumplimiento de esta política se determinará en el procedimiento correspondiente, según las disposiciones vigentes, para establecer sanciones en el ámbito laboral aplicable.

5.6. Comunicación de la política.

La presente política estará disponible en la página web www.belltech.la, para todos los colaboradores y grupos de interés de la compañía. Este documento será objeto de divulgación, capacitación y sensibilización, para su adecuada comprensión y puesta en práctica.

5.7. Actualización y revisión.

La presente política será revisada anualmente y actualizada, cuando proceda, con el fin de adaptarla a los cambios que puedan surgir en el modelo de negocio o contexto de Belltech, garantizando en todo momento la efectiva implantación y mejora continua del SGSI.

6. FLUJOGRAMA

No aplica.

7. ROLES Y RESPONSABILIDADES

La responsabilidad de la protección de la información y los sistemas que la tratan, almacenan o transmiten, se extiende a todos los niveles organizativos y funcionales de Belltech.

Alta Dirección	- Asegurar que las buenas prácticas sobre la gestión de la seguridad se apliquen de manera efectiva y consistente en todo Belltech. - Supervisar la estrategia de seguridad de la información.

	- Proporcionar los recursos necesarios para la definición, implementación y mantenimiento del SGSI.
Área Sistemas de Gestión	- Definir una estrategia de seguridad de la Información, que establezca lineamientos y controles de seguridad de la información, alineados con la norma aplicable. - Ejercer su función de control y verificación de cumplimiento del SGSI. - Liderar la capacitación y sensibilización sobre seguridad de la información y ciberseguridad. - Mantener y mejorar el SGSI, de manera continua.
Área TI	- Implementar controles definidos en el SGSI. - Prevenir, detectar y responder ante eventos e incidentes de seguridad de la información.
Colaboradores	- Conocer, asumir y cumplir con las políticas, manuales y procedimientos. - Mantener el secreto profesional y la confidencialidad de la información manejada en su entorno. - Comunicar, según los procedimientos establecidos, los eventos, incidentes o problemas de seguridad que se detecten. - Identificar, valorar y gestionar los riesgos del proceso al que pertenece y de los servicios con terceros que impliquen el uso o acceso de información clasificada. - Usar los activos de información de Belltech, exclusivamente con fines corporativos, en la realización de sus funciones.
Terceros	- Incluir requerimientos específicos de seguridad sobre activos tecnológicos y procesos, según el servicio contratado o producto adquirido. - Conocer y cumplir la presente política, según aplique. - Mantener el secreto profesional y la confidencialidad de la Información manejada en su relación con Belltech.

8. FORMATOS RELACIONADOS

- REFRSI05 Declaración de Aplicabilidad - SoA