Seguridad de la Información

ayesa

Índice a una columna

1. ¿Qué es la seguridad de la Información?

1. ¿Qué es la Seguridad de la Información

Valor de la Información

La afirmación de que el conocimiento y la información asociada al mismo (como base o producto del mismo) tienen valor (utilidad), tanto para el que lo posee, como para el que desearía poseerlo. Es ampliamente aceptada, sobre todo cuando observamos el esfuerzo que usamos para obtenerla, conservarla, procesarla, trasmitirla,….

La inversión y uso de las tecnologías de la información, acompañada de una utilización inteligente de la información que dichas tecnologías nos permiten deriva del mejor uso de la información en los procesos (captura, generación, análisis, toma de decisiones,….), modifica el valor de la información.

El valor de la tecnología es, pues, el valor que se deriva del mejor uso de la información capturada y gestionada con la tecnología.

La protección del valor de la información ante amenazas y vulnerabilidades de los sistemas de información (tecnológicos a no) **es el objetivo de la seguridad de la información**

1. ¿Qué es la Seguridad de la Información

La norma UNE-ISO/IEC 27001 define la Seguridad de la Información como la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

De ahí podrás entender que para Ayesa es importante asegurar los "activos" que componen los sistemas de información para garantizar así la integridad, confidencialidad y disponibilidad de la información.

El **activo** esencial para Ayesa es **la información** que maneja el sistema, es decir, los datos, toda la información sea cual sea su formato: papel, electrónico o verbal.

No debes confundir **seguridad de la información** con **ciberseguridad**, esta sólo se encarga de proteger la información que permanece en los sistemas automatizados contra el acceso o modificación no autorizada, por lo que sería una parte que se engloba dentro de la Seguridad de la Información.

1. ¿Qué es la Seguridad de la Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas que las organizaciones y los sistemas tecnológicos pueden aplicar a fin de resguardar y proteger la información buscando mantener distintas propiedades de la información que le confieren valor, tales como:

- la confidencialidad,
- la integridad,
- la disponibilidad,
- la autenticidad
- la trazabilidad.

Confidencialidad: asegurar el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización

Integridad: mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados

Disponibilidad: Asegurar el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Autenticidad: permite identificar el generador de la información

Trazabilidad: garantizar que todos los datos y la información se registren, monitoreen y auditen de manera precisa

2. Política de Seguridad de la Información

3. Políticas de Seguridad de la Información

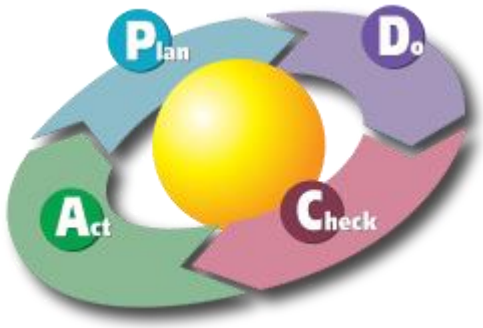
Las Políticas de Gestión de Ayesa son establecidas, implementadas y mantenidas por la Alta Dirección.

La dirección de Ayesa es consciente y tiene asumido que uno de los objetivos más importantes de Ayesa es la protección de los activos de información de cualquier amenaza.

La Política de Gobierno y Gestión de las Tecnologías de la Información incluye los compromisos de Ayesa con la Seguridad de la Información.

El SGSI se implanta para **garantizar** a largo plazo la actividad laboral y la prestación continuada de los servicios de Ayesa **frente a fallos, ataques, incidencias**, etc. que afectan a los datos y la información.

Ayesa considera que la planificación, la implantación de controles, la supervisión y la mejora continua de la seguridad de la información son procesos de gestión esenciales para asegurar la competitividad y la sostenibilidad del negocio.



3. Políticas de Seguridad de la Información

Política de Gobierno y Gestión de las TIC

Ayesa trabaja por construir un mundo más eficiente y justo, aplicando la ingeniería y la tecnología de vanguardia de manera integrada. Ayesa ofrece servicios de ingeniería, consultoría, tecnologías de la información y outsourcing en múltiples líneas de negocio y sectores de actividad, así como, servicios de diseño, outsourcing de back & front office, instalación y soporte de infraestructuras tecnológicas y servicios digitales.

La Dirección de Ayesa, es consciente y tiene asumido la importancia de las Tecnologías de la Información para la gestión eficiente de los procesos internos y la consecución de los objetivos estratégicos del Negocio.

Es por ello por lo **que la Dirección asume la responsabilidad de implantar, mantener y mejorar continuamente las prácticas de gobierno TI, siguiendo los siguientes principios:**

•**Responsabilidad:** las responsabilidades están definidas y todas las personas de Ayesa comprenden y aceptan dichas responsabilidades. En particular, asegura que se definen y comunican las funciones y responsabilidades del Gobierno TI y los sistemas de gestión TI.

•**Estrategia**: los planes de tecnologías de la información estarán alineadas con los objetivos y estrategias de negocio de la compañía y aportarán valor al negocio de la compañía, concentrándose en optimizar costes.

•**Adquisición**: las inversiones TI y las adquisiciones están priorizadas en base a las necesidades del negocio y se llevan a cabo siguiendo procedimientos que aseguran la idoneidad de estos y su aportación a las estrategias de negocio, concentrándose en optimizar costes

•**Desempeño**: Los Sistemas de Información aseguran la provisión de servicios, niveles de servicio y calidad de servicio requeridos para alcanzar los requisitos presentes y futuros del negocio

•**Cumplimiento:** se han establecido procedimientos y medidas que aseguran el cumplimiento de la legislación y las normativas (poniendo especial interés en la legislación de protección de datos personales de cada País) y se realizan revisiones y auditorias periódicas para asegurar que están implantadas y se cumplen.

•**Factor Humano**: Ayesa facilitará los recursos humanos necesarios para satisfacer las necesidades de Negocio y se realizan actividades de comunicación, formación, concienciación y motivación a todo el personal de Ayesa para el adecuado uso de las TI.

3. Políticas de Seguridad de la Información

Política de Gobierno y Gestión de las TIC

El Gobierno TI de Ayesa se apoya por los diferentes sistemas de Gestión TI implantados: Seguridad de la Información (ISO 27001 y ENS), Gestión de Servicios TI (ISO 20000-1), Desarrollo software (CMMI) y Gestión de la continuidad (ISO 22301). Así como en las normas ISO 27002 (Control de la seguridad de la información) y sus extensiones ISO 27018 (Código de prácticas para proteger los datos personales en la nube) e ISO 27701 norma de referencia para el cumplimiento de la normativa del RGPD.

Para asegurar el cumplimiento de los requisitos y la mejora continua, la Dirección de Ayesa adquiere los siguientes compromisos

En relación a la seguridad de la Información

- Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
- Proteger los recursos de información de Ayesa y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Evaluar y tratar los riesgos y amenazas a los que están expuestos la información, los servicios y sistemas de Ayesa, incluyendo los riesgos derivados del tratamiento de datos personales y los riesgos clave para la continuidad de los procesos considerados críticos por la organización.
- Asegurar que, para cualquier adquisición de productos, tanto software como hardware, se tengan en cuenta requisitos de seguridad.
- Implementar las medidas necesarias para el registro de la actividad y el análisis de los mismos en busca de patrones anormales y la puesta en marcha de las acciones adecuadas para su tratamiento.

Política de Gobierno y Gestión de las TIC

En relación al Sistema de Gestión de la Continuidad

- La primera premisa y el objetivo prioritario es la protección y seguridad del personal, tanto en situación normal como en situación de contingencia. .
- Disponer de los procedimientos necesarios para responder de forma adecuada ante la aparición de un incidente perturbador, desde el momento en que se declare hasta la completa recuperación de la normalidad en las distintas actividades de negocio, minimizando el impacto originado en las operaciones.
- Tratar de minimizar el impacto que se pudiera derivar de cualquier situación de emergencia sobre los servicios identificados como críticos o el nivel de prestación de los mismos. .
- Conseguir retornar al estado de normalidad en la localización afectada lo antes posible una vez mitigadas las consecuencias del incidente perturbador.
- Garantizar que se elaboran, implementan y mantienen de forma adecuada los Planes de Continuidad, teniendo en cuenta los servicios y procesos críticos y tomando como referencia la evaluación de los riesgos.
- Probar de forma periódica el Sistema de Gestión de Continuidad de Negocio para asegurar la adecuación del mismo a las necesidades de Ayesa y adaptarlo siempre que sea necesario a la vista de los resultados de dichas pruebas

En relación con el Sistema de Gestión de Servicios TI:

- Asegurar la satisfacción de las necesidades y expectativas de clientes y usuarios con respecto a los servicios acordados
- Garantizar el cumplimiento de los niveles de servicio acordados entre Ayesa y sus clientes, así como a gestionar cualquier incidente o problema que pudiera surgir
- Poder detectar, analizar, informar y corregir las posibles deficiencias y carencias en relación con los acuerdos de nivel de servicio establecidos

Política de Gobierno y Gestión de las TIC

En relación al Sistema de Gestión de los desarrollos software

- Asegurar el cumplimiento de los requisitos de los clientes y los requisitos de Seguridad de la Información durante todo el ciclo de vida del desarrollo. .
- Asegurar la satisfacción de las necesidades y expectativas de clientes. Tratar de minimizar el impacto que se pudiera derivar de cualquier situación de emergencia sobre los servicios identificados como críticos o el nivel de prestación de los mismos.
- Llevar a cabo todas las prácticas establecidas en el modelo CMMI.

Para llevar a cabo esta política, Ayesa ha establecido sistemáticas de trabajo documentadas en procedimientos, instrucciones, documentos y plantillas que están a disposición del personal de Ayesa en la intranet y que son de obligado cumplimiento para todos los empleados, así como para terceras partes que suministren bienes o servicios a Ayesa.

Nuestra Política de Gobierno y Gestión de las Tecnologías de la Información la tienes disponible en la **página Web de Ayesa, en la intranet y en Power Alejandría.**

3. Actores que intervienen en la Seguridad de la Información

3. Actores que intervienen en la Seguridad de la Información

En el proceso de seguridad de la información intervienen varios actores, sigue para conocer a cada uno de ellos:

Activos y propietarios

Como sabes Ayesa tiene gran variedad de activos ¡tú eres uno de ellos! Pero... ¿sabías que esos activos tienen propietarios?

Pues sí, Ayesa mantiene un inventario de los activos e identifica a sus propietarios. Un propietario es el individuo o entidad al que se le ha asignado la responsabilidad administrativa para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.

Los propietarios de los activos de información de Ayesa deben asegurar que todas las personas bajo su supervisión siguen los procedimientos de seguridad de la información del SGSI.

¡Ojo! El término "propietario" no significa que la persona tenga realmente algún derecho de propiedad sobre el activo.

En Ayesa existen diferentes tipos de activos:

- Servicios
- Datos o información
- Software y hardware, redes de comunicaciones
- Instalaciones, personal, etc.
- Imagen de la empresa, prestigio, valores abstractos, etc.

3. Actores que intervienen en la Seguridad de la Información

Usuarios

Como usuario de los activos de información de Ayesa tienes la responsabilidad de su buen uso y del acceso a la información siguiendo los procedimientos de seguridad de la información del SGSI.

Además, eres responsable de comunicar cualquier incidente o problema detectado a través de GPI o de los teléfonos establecidos en el documento DO-SI02 Guía de buenas prácticas de seguridad de la información.

3. Actores que intervienen en la Seguridad de la Información

Amenazas

Se habla de amenaza cuando se ataca a la integridad, confidencialidad y disponibilidad de la información y sistemas de información.

Una amenaza es la causa potencial de un incidente que puede causar daños a la información o el sistema que lo soporta.

Amenazas hay muchas, a modo de resumen podemos clasificarlas de la siguiente manera:

- De origen natural: accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva,.
- Del entorno (de origen industrial) : desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva.
- Defectos de las aplicaciones: equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas.
- Causadas por las personas de forma accidental :Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- Causadas por las personas de forma deliberada : Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Riesgos

El riesgo es la probabilidad de que una amenaza se materialice y aproveche una vulnerabilidad del sistema.

Todos los sistemas tienen vulnerabilidades y están sujetos a amenazas, pero cada una de ellas, por separado, no representan un peligro. Si se unen, se convierten en un riesgo, en la probabilidad de que ocurra algo, normalmente malo.

Pues bien, para Ayesa, los riesgos son los acontecimientos futuros inciertos que pueden afectar al logro de los objetivos estratégicos, operativos, financieros o de cumplimiento legislativos.

El riesgo se puede y debe prevenir y mitigar.

La prevención y mitigación comienzan por:

- Conocer cuáles son las amenazas y riesgos a los que los activos de tu empresa están expuestos.
- Hacer planes de tratamiento de riesgos para reducir esas amenazas y riesgos o evitar que hagan daño.
- Realizar lo planeado para reducir la vulnerabilidad

3. Actores que intervienen en la Seguridad de la Información

Riesgos

Conocer los riesgos implica la identificación y la evaluación de los mismos.

Para evaluar el riesgo, Ayesa tiene que poner en marcha el proceso de evaluación de las amenazas, vulnerabilidades e impactos sobre la información y sobre los medios de utilizados para su tratamiento.

Para el análisis y gestión de los riesgos, Ayesa toma como base la metodología MAGERIT y la herramienta PILAR.

La metodología MAGERIT ha sido elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España y es específica para la gestión de riesgos TIC.

Con PILAR conjugamos los activos de Ayesa con las amenazas posibles, calculamos los riesgos y nos permite incorporar salvaguardas para reducir el riesgo a valores residuales aceptables. Esto nos permite fundamentar la confianza en el sistema.

3. Actores que intervienen en la Seguridad de la Información

Salvaguardas

Ayesa se protege de las amenazas y sus riesgos mediante salvaguardas.

Igual que no es suficiente un jarabe para curarte una gripe, las herramientas técnicas de seguridad no garantizan la total protección de la información.

Las salvaguardas actúan sobre amenazas:

- limitando el impacto
- reduciendo la probabilidad
- atenuando el riesgo

Implantando un conjunto de salvaguardas se reducen los riesgos provocados por las amenazas a los diferentes sistemas de información.

Para hacer frente a los riesgos deben utilizarse los tres tipos de salvaguardas conjuntamente, algunos ejemplos de salvaguardas pueden ser:

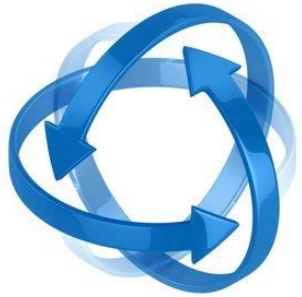
Salvaguardas		
Técnicas	Físicas	Administrativas
• Tarjetas inteligentes • Antivirus • Gestión contraseñas	• Control de acceso • Detectores de humo • Extintores	• Conocer la información técnica • Eliminar accesos antiguos usuarios • Cambiar contraseñas cada cierto tiempo

4. ¿Qué hace la empresa en materia de seguridad de la información?

5. ¿qué hace la empresa en materia de Seguridad de la Información?

Implantar, mantener y mejorar de forma continua el **Sistema de Gestión de Seguridad de la Información** de acuerdo a los estándares internacionales.

Gestiona el Inventario de **Activos:** Servicios, Datos o información, Software, Hardware, Redes de Comunicaciones, Instalaciones, Personal, Imagen de la empresa, prestigios, valores abstractos…



Define **Propietarios de activos**:
un propietario es el individuo o entidad al que se le asigna la responsabilidad administrativa para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. No tiene derecho de propiedad sobre el activo.

Informa y Compromete a los **Usuarios:** Los usuarios tienen la responsabilidad de un buen uso de los activos de información, accediendo a ellos y siguiendo los procedimientos de seguridad.

4. ¿Qué hace la empresa en materia de Seguridad de la

Detecta y evalúa **Amenazas** a las que están expuestos los activos y el impacto sobre la información o sobre los medios utilizados para su tratamiento. Ayesa toma en consideración las amenazas que se ciernen sobre la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de la información y sobre sus sistemas de información.

Elabora Planes para prevenir y mitigar **Riesgos** (probabilidad de que una amenaza se materialice y aproveche una vulnerabilidad del sistema). Los riesgos son acontecimientos futuros inciertos que pueden afectar al logro de los objetivos estratégicos, operativos, financieros o de cumplimiento legislativo.

Reducir **vulnerabilidades**.
Obliga a los usuarios a cambiar la contraseña cada tres meses.
Recordatorios.
Implementa y actualiza periódicamente un conjunto de **salvaguardas** para proteger sus activos frente a amenazas y riesgos, de manera que reducen la probabilidad de que se produzca, atenúan el riesgo y limitan su impacto.

5. El Sistema de Gestión de la Seguridad de la Información de Ayesa

5. El Sistema de Gestión de Seguridad de la Información de AYESA

Objetivos

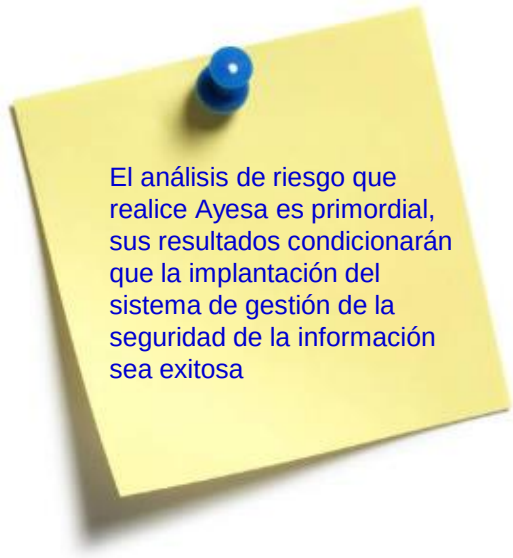
Un nivel de protección de la información total es algo prácticamente imposible de garantizar, por eso Ayesa ha implantado un Sistema de Gestión de la Seguridad de la Información, SGSI, para garantizar que los riesgos de la seguridad son:

- Conocidos
- Asumidos
- Gestionados
- Minimizados

Garantizando eso, nuestra empresa puede mantener y adaptarse a los cambios que se produzcan para mejorar así la seguri información. ¡Además desarrollando un sistema de gestión de la seguridad de la información mejorará sus niveles de seguri

El SGSI garantiza a Ayesa de que los riesgos que afectan a su información son conocidos y gestionados.

La norma UNE-ISO/IEC 27001 es una norma certificable. Para Ayesa es importante la certificación, ya que el certificarse supone además de tener un Sistema de Gestión seguro y auditado anualmente por entidad independiente, una ventaja comercial para la empresa.



5. El Sistema de Gestión de Seguridad de la Información de AYESA

Estructura organizativa para la Gestión de la Seguridad de la Información

Conoce las diferentes figuras que actúan en el Sistema de Gestión de Seguridad de la Información:

- Responsable de Seguridad de la Información (CISO)
- Responsable del Sistema de Gestión de seguridad de la Información
- Delegado de protección de datos
- Propietarios de los activos
- **Usuarios**

Tu papel es muy importante para la Seguridad de la Información de Ayesa.

Para el seguimiento del Sistema de Gestión de la Seguridad de la Información se ha creado el **Comité de Seguridad de la Información**

Estructura organizativa para la Gestión de la Seguridad de la Información

Responsable de Seguridad de la Información.

Funciones y responsabilidades:

- Mantenimiento y mejora continua del Inventario de Activos del SGSI.
- Identificación y evaluación periódica de los riesgos de los activos.
- Asegurar el establecimiento y eficacia de las políticas de seguridad de la información
- Elaborar en documento de Declaración de Aplicabilidad
- Propuesta, definición y ejecución de las acciones correctivas y las acciones de mejora de la seguridad de la información.
- Establecer y mantener contactos con los grupos de interés, foros profesionales, organismos de seguridad de la información (CERT, INTECO, AEPD, ENISA…).
- Asegurar que se tienen en cuenta requisitos de seguridad en la adquisición de productos y servicios TI.
- Analizar los resultados de las auditorias, junto con el Responsable del Sistema de Gestión de Seguridad de la Información para establecer las correspondientes acciones correctoras
- Suministrar al Responsable del Sistema de Gestión de Seguridad de la Información la información necesaria para el seguimiento del SGSI, de la eficacia de los controles de seguridad y de los incidentes de seguridad acontecidos con la periodicidad establecida.
- Asegurar que se realizan las copias de seguridad según se establece en el procedimiento correspondiente.
- Asegurar que se realizan las pruebas de los planes de seguridad que correspondan y enviar los resultados al Responsable del Sistema de Gestión de Seguridad de la Información.
- Establecimiento y seguimiento de los planes de continuidad en el negocio, así como de la realización de las pruebas del mismo.
- Actuar como persona de contacto con INCIBE, comunicando los incidentes de seguridad con efectos perturbadores en la prestación del servicio, recibiendo y interpretando las guías e instrucciones enviadas y recopilando y suministrando la información o documentación solicitada.
- Asesoramiento y validación en la elaboración de ofertas a clientes en aquellos apartados relacionados con la seguridad de la información.
- Promover la formación y concienciación en materia de seguridad de la información

Estructura organizativa para la Gestión de la Seguridad de la Información

Responsable del Sistema de Gestión de Seguridad de la Información.

Funciones y responsabilidades:

- Mantenimiento y mejora continua del SGSI en coordinación con el Responsable de Seguridad de la Información
- Planificación y coordinación de la ejecución de auditorías del SGSI en coordinación con Calidad
- Coordinación de la ejecución y seguimiento de las acciones formativas del bloque de seguridad de la información, en coordinación con Formación
- Realización de informes:
  - ✓ Seguimiento del SGSI para el Comité de Dirección de Seguridad de la Información (cumplimiento de objetivos, métricas e indicadores, resultados de auditorías realizadas, situación de acciones correctivas y preventivas, planteamiento de nuevos objetivos, propuestas de mejora, …).
  - ✓ Seguimiento de objetivos e indicadores. Periodicidad trimestral.
  - ✓ Informes de eficiencia de los controles de seguridad establecidos.
  - ✓ Informes de incidentes en la seguridad de la información. Lecciones aprendidas.
- Mantenimiento y mejora continua del proceso de Análisis y Gestión de Riesgos.
- Identificación e incorporación de nuevos riegos
- Coordinar de forma permanente el proceso de concienciación en materia de seguridad para toda la compañía
- Seguimiento permanente de las acciones preventivas y correctivas.
- Seguimiento permanente del desempeño y de los objetivos del SGSI y SGCN
- Mantener actualizado los Planes de Continuidad, teniendo en cuenta la información suministrada por el Responsable de Seguridad de la Información.

Estructura organizativa para la Gestión de la Seguridad de la Información

Delegado de protección de datos.

Funciones y responsabilidades:

- Informar y asesorar de las obligaciones en virtud de la GDPR
- Llevar a cabo un registro de actividades de tratamiento (RAT)
- Realizar evaluaciones de riesgo y análisis de impacto conjuntamente con el responsable de gestión de seguridad de la información y el responsable de seguridad de la información.
- Concienciación y formación del personal en materia de protección de datos
- Soporte en auditorias y certificaciones
- Gestión y notificación de violaciones de seguridad en materia de protección de datos
- Elaborar y mantener actualizados los procedimientos relacionados con la protección de datos
- Soporte en proyectos para cumplir la privacidad de los datos
- Cooperar con el responsable de seguridad para el cumplimiento de la legislación aplicable.
- Gestionar los derechos ARCO+ en el plazo legal
- Supervisar y adecuar el clausulado en protección de datos y páginas web
- Implementar un procedimiento de conservación, bloqueo y supresión de datos

Estructura organizativa para la Gestión de la Seguridad de la Información

Propietario de los activos.

Funciones y responsabilidades:

- Desarrollar, operar y mantener el sistema de información del que es propietario durante todo su ciclo de vida incluyendo especificaciones, instalación y verificación del correcto tratamiento
- Definir la topología y la gestión del sistema de información del que es propietario, estableciendo criterios de uso y los servicios disponibles
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

Usuarios

Funciones y responsabilidades:

Como usuario de los activos de información de tu empresa tienes la responsabilidad de su buen uso y del acceso a la información siguiendo los procedimientos de seguridad de la información del SGSI y en particular la Guía de Buenas prácticas de Seguridad de la información.

Mas Adelante, en esta Formación, nos detendremos en tu papel dentro del Sist6ema de Gestión de Seguridad de la Información

Estructura organizativa para la Gestión de la Seguridad de la Información

Comité de Seguridad de la Información.

El Comité de Gestión Seguridad de la Información estará constituido por:

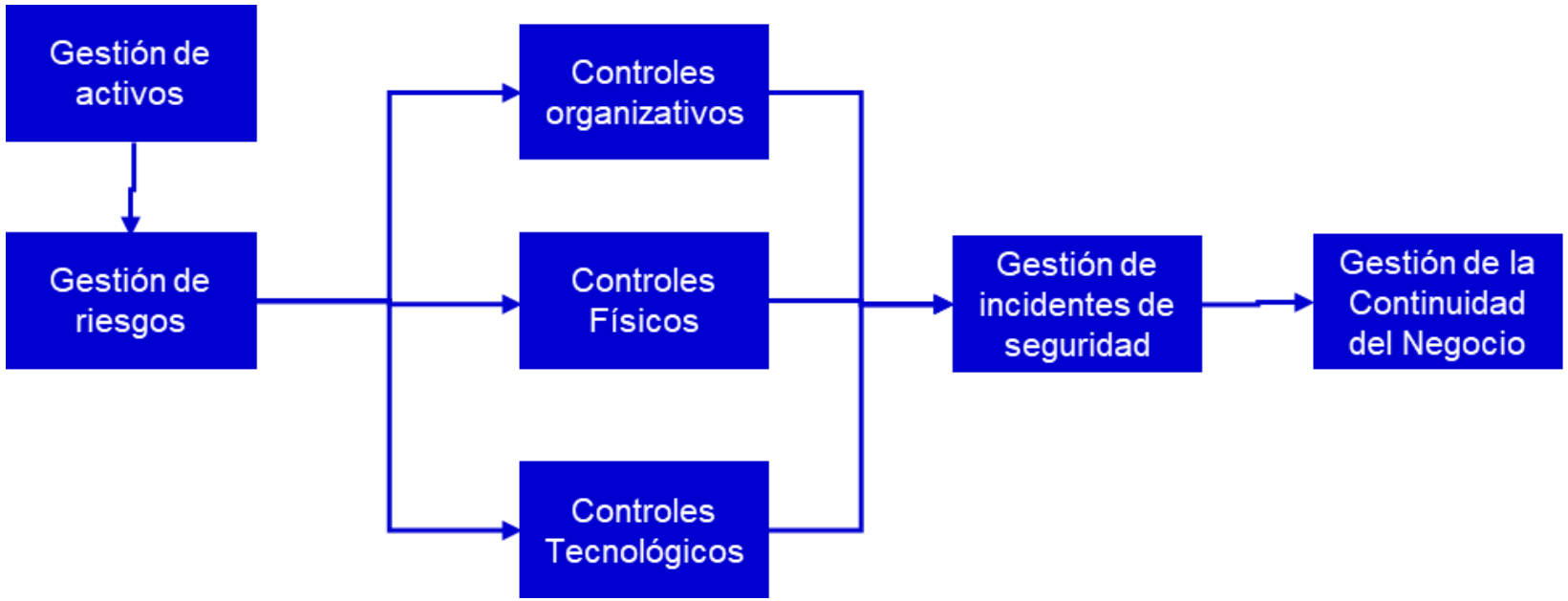
- Responsable de Seguridad de la Información
- Responsable Sistemas de Gestión de Seguridad de la Información
- CIO
- Representante de la DSI (Departamento corporativo de Sistemas de Información)
- Representante de la OTCISO
- Representantes del SGSI de sociedades LATAM

Las funciones y responsabilidades del Comité de Gestión de Seguridad de la información son:

- Gestionar los asuntos cotidianos respecto a la seguridad de la información y Gestión de la continuidad
- Análisis del cumplimiento de los objetivos
- Análisis de métricas e indicadores
- Análisis de los incidentes de Seguridad
- Seguimiento de riesgos y oportunidades
- Seguimiento de Acciones correctivas y acciones de mejora
- Gestión de cambios
- Promover la realización de auditorías internas
- Coordinar los planes de seguridad
- Análisis de las pruebas de recuperación de datos y pruebas del Plan de continuidad. Establecimiento de mejoras del Plan de Continuidad
- Análisis de las situaciones de Activación del Plan de continuidad y de los informes generados. Establecimiento de acciones de mejora del Plan de Continuidad
- Análisis de amenazas
- Necesidad de documentación y formación

5. El Sistema de Gestión de Seguridad de la Información de AYESA

Los procesos del Sistema de Gestión de Seguridad de la Información



La documentación del Sistema de Gestión de Seguridad de la Información

Para llevar a cabo la política de Gobierno y Gestión de las TI, Ayesa ha establecido sistemáticas de trabajo documentadas en oilíticas, procedimientos, documentos e instrucciones que son de obligado cumplimiento para todos los empleados de Ayesa, así como para terceras partes suministren bienes o servicios que puedan tener impacto en la seguridad de la información.

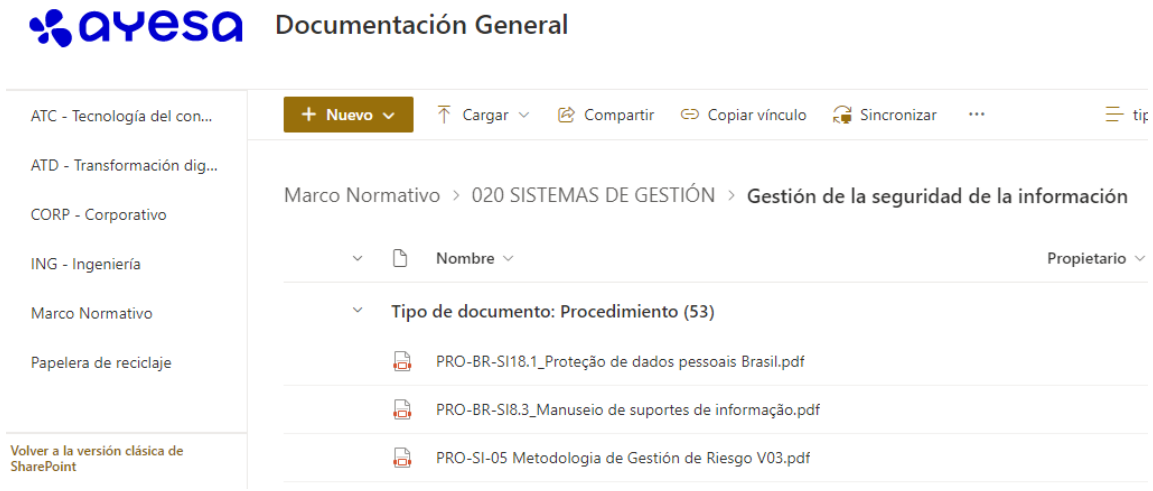
La documentación del SGSI está accesible a todas las personas de Ayesa en Alejandría y en la Intranet.

My Company/Calidad/Mapa de procesos y documentos/Gestión de la Seguridad de la Información

Enlace:

Documentación General - Gestión de la seguridad de la información - tipo_documento

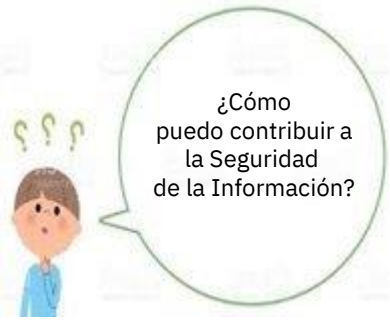
Podrás encontrar la documentación en Español y en portugués, en breve también se publicará la documentación en Ingles



6. Mi responsabilidad como usuario de los sistemas de información de Ayesa

6. Mi responsabilidad como usuario

En mi puesto de trabajo



•Mantén tu puesto de trabajo organizado y limpio. Recuerda no dejar a la vista documentos con datos sensibles, como por ejemplo: contraseñas, números de cuenta o identificación, contratos, cartas… entre otros.

•Guarda la documentación sensible en cajones o armarios cerrados con llave cuando no la estés utilizando.

•Evita el acceso no autorizado a tu ordenador, bloqueando la sesión cada vez que te levantes. Utiliza el commando Windows L

•Utiliza sólo software con licencia y descargado de sitios de confianza, así evitarás la entrada de virus a tu equipo. Si tienes dudas, dirígete al equipo de Soporte, a través de GPI.

•Para la transferencia de información voluminosa, evita el uso de plataformas públicas no protegidas (Mega, Dropbox, etc.).

•Teams deberá ser el canal utilizado de mensajería instantánea internamente. Se debe evitar utilizar Whatsapp.

•La política y normativa del uso de correo electrónico corporativo están detalladas en el PRO-CORP.02.09 Normas de uso del correo electrónico corporativo.

•Cuando elabores documentación no olvides Clasificarla en pública, confidencial o reservada, ten en cuenta los criterios para el almacenamiento, transmisión retención y borrado establecido en el PRO-CORP- XX Gestión documental

•Si manejas información con datos personales, consulta con el Delegado de protección de datos (DPD) de Ayesa para asegurar el adecuado tratamiento de la misma.

6. Mi responsabilidad como usuario

En mi puesto de trabajo

- Abstente de visitar sitios web restringidos por la empresa.
- No utilices correos personales o proporcionadas por otras partes interesadas para tratar temas de trabajo.
- Haz tu contraseña segura, evitando incluir datos personales y palabras del diccionario.
- Limpia los metadatos de los ficheros word que generes (Archivo ->Información->Inspeccionar Documento)
- Cuando recibas correos electrónicos solicitando información personal, bancaria, nombres de usuario o contraseñas, no respondas, podrías ser víctima de fraude electrónico.
- Al terminar la jornada laboral, tómate el tiempo necesario para recoger y guardar el material sensible.
- Los portátiles y teléfonos móviles propiedad de Ayesa están asignados a un único usuario que es responsable de su cuidado y custodia. Puedes retirar el equipo de las oficinas para utilizarlo en teletrabajo o en instalaciones del cliente.

6. Mi responsabilidad como usuario

Cuando teletrabajes

Solo se emplearán los equipos suministrados por Ayesa para la ejecución de los trabajos, no permitiéndose el uso de otros equipos propiedad del trabajador, ni siquiera en caso de avería de los equipos suministrados por la empresa, salvo autorización expresa de sus responsables.

El trabajador se compromete:

- A la salvaguarda de los sistemas telemáticos puestos a su disposición para la prestación de los servicios contratados, así como, toda la documentación e información de la Compañía.
- A no hablar sobre la información de la Compañía con nadie que no sea miembro de la misma y esta exclusión alcanza tanto a los miembros de la familia como a otras personas.
- Los papeles documentos de trabajo deben tratarse con mucho cuidado y guardarse en carpetas apropiadas, escritorios o archivos de manera que no puedan ser visibles o manipulables por otras personas que puedan entrar en el domicilio. Asimismo, la documentación y soportes de información empleados, en su caso, deberán ser guardados bajo llave cuando no se estén usando y deberán preservarse de la visión de terceros, familiares o amigos mientras se usen.

Fuera de tu puesto de trabajo

- Los dispositivos móviles (portátiles y telefonía) son un medio de trabajo y deben usarse exclusivamente para estos fines.
- Cuando te encuentres fuera de la oficina no los pierdas nunca de vista evita dejarlos en el coche mientras te ausentas del mismo.
- Recuerda que los dispositivos portátiles que contengan información confidencial de la empresa deben tener contraseña para su acceso de manera que se eviten accesos indeseados. Igualmente, debes usar algún tipo de encriptación de datos para la información más sensible.
- Cuando los dispositivos se usen en lugares públicos, tales como salas de reunión u otras áreas desprotegidas fuera de las instalaciones de Ayesa, es importante extremar las precauciones para evitar el riesgo de acceso no autorizado o revelación de información almacenada.
- En caso de robo o pérdida de dispositivos móviles, el usuario debe comunicar al responsable de Seguridad de la Información lo antes posible.
- Evita llevar información impresa y si es estrictamente necesario, tenla a buen recaudo siguiendo las mismas pautas que en el caso de dispositivos portátiles.
- Infórmate de las amenazas existentes y de cómo puedes evitarlas si tienes que desplazarte a otro país.

La protección de la información y de los dispositivos que la contienen son responsabilidad tuya

6. Mi responsabilidad como usuario

Incidentes de Seguridad

Comunica cualquier anomalía, suceso o incidente que pueda afectar a la seguridad de la información mediante la creación de un ticket en GPI.

GPI

Para casos en los que no puedas acceder a GPI puedes ponerte en contacto con el CAU

Telf.: 943 413 933/ 3333

Correo: cau@ayesa.com

Se considera una incidencia grave cualquier suceso que ponga en riesgo la prestación de los servicios y pueda provocar una parada de los mismos o un suceso que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos o el acceso no autorizado.

Las incidencias graves serán gestionadas de manera inmediata por el personal de soporte y se informará al usuario del avance de su resolución, en la medida de lo posible, según el procedimiento PRO-SI524 Gestión de brechas e incidentes de seguridad de la información