Índice	Política de Seguridad de la Información

1. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de ZANTZA
Es la política de ZANTZA asegurar que:

- La información está protegida contra pérdidas de disponibilidad, confidencialidad e integridad.
- La información está protegida contra accesos no autorizados.
- Su cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con esta Política.
- El responsable de Seguridad de la Información será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.
- Los responsables de cada área de negocio serán los encargados de implementar esta Política y sus correspondientes procedimientos dentro de su área.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto de trabajo.
- Es política de ZANTZA implementar, mantener y realizar un seguimiento del SGSI

Esta política ha sido aprobada por la dirección de ZANTZA y se revisará anualmente.

2. POLÍTICA DE SEGURIDAD

2.1. CONCEPTOS GENERALES

- Disponibilidad: Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten,

especialmente la información crítica.
● Utilidad: Los recursos del sistema y la información manejada en el mismo han de ser útiles para alguna función.
● Integridad: La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
● Autenticidad: El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
● Confidencialidad: La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
● Posesión: Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.
El ciclo PDCA es el que se utilizará durante todo el ciclo de vida del SGSI.
● P (Planificar): en esta fase se establecen las actividades, responsabilidades y recursos además de los objetivos a cumplir y cómo se van a medir estos objetivos.
● D (Desarrollar): se desarrollan los procesos y se implementan. Una vez implementados, hay que medir los resultados de la ejecución de dichos procesos.
● C (Comprobar): se analizan los resultados para comprobar si se han alcanzado los objetivos y si no es así, identificar las causas.
● A (Actuar): Se toman las acciones necesarias para corregir los fallos detectados en los procesos o para mejorarlos.

Las normas de referencia para la realización de los trabajos indicados así como su ámbito de aplicación son las siguientes:
● Norma UNE/ISO-IEC 27001 Tecnología de la Información. Especificaciones para los Sistemas de Gestión de Seguridad de la Información, en la que se recogen los requisitos para establecer, implantar, documentar y evaluar un SGSI. Es la norma sobre la que se desarrolla el sistema y la que permite obtener la certificación del mismo por parte de un organismo certificador independiente.
● Norma ISO 27002 Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información. Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad y constituir una práctica eficaz de la gestión.

2.2. PROPÓSITO

La información y los procesos que la apoyan, sistemas y redes son importantes activos de ZANTZA. La disponibilidad, integridad y confidencialidad de la información son esenciales para mantener la calidad de los servicios y la reputación e imagen de la entidad.
Este Documento tiene como objetivo establecer las directrices que garanticen la seguridad de la información en ZANTZA a un nivel adecuado según el nivel de riesgo de los activos y nuestras necesidades y recursos.

2.3. CAMPO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD

Todas las pautas descritas en el presente documento serán efectivas para el conjunto de ZANTZA, sus instalaciones y activos. Asimismo aplica a todos los empleados de ZANTZA, que seguirán las directrices en la medida que afecten a su trabajo. También aplica a los contratistas, clientes o cualquier otra parte interesada que tenga acceso a la información o los sistemas de ZANTZA, los cuales serán debidamente informados.

2.4. ALCANCE DEL SGSI

Gestión de la seguridad de la información asociada a los procesos de su actividad de Empresa de Trabajo Temporal.

2.4.1. Localización: Polígono Pinoa Parcela 8, Ofc. 25 48170 Zamudio (Bizkaia)

2.4.2. Organigrama

2.4.3. Infraestructura Informática

La red de ZANTZA está configurada en forma de grupo de trabajo Windows Server 2022 Standard,. El servidor se encuentra ubucado en un data center externo.
Existen 3 puestos de usuario con sistema operativo Windows.

La red de ZANTZA tiene salida a Internet mediante una conexión de banda ancha ADSL cableada.

2.5. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

● Asegurar que la plantilla conoce y comprende los problemas asociados a la seguridad de la información y que asumen y son conscientes de sus responsabilidades en este tema.
● Proporcionar una guía para establecer los estándares, procedimientos y medidas de seguridad para desarrollar un Sistema de Seguridad de la Información.
● Asegurar la confidencialidad de la información que nuestros clientes depositan y ZANTZA almacena en los sistemas de información.
● Maximizar la disponibilidad y calidad de los servicios prestados a los clientes de ZANTZA.
● Reducir o eliminar los peligros y riesgos inherentes a nuestras actividades por medio de la mejora continua del desempeño en seguridad en nuestros procesos, productos y servicios.
● Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.
● Mantener a disposición de las partes interesadas nuestra Política presente, así como los futuros desarrollos de la misma.

2.6. REQUISITOS LEGALES

Los requisitos Legales y su control y actualización vendrán definidos en el PR.SEG.06, Procedimiento de Cumplimiento Legal.

2.7. REVISIONES Y AUDITORÍAS

El Responsable de Seguridad revisará esta Política anualmente o cuando haya cambios significativos que así lo aconsejen, y

la someterá de nuevo a aprobación por la Dirección. Las revisiones comprobarán la efectividad de la política, valorando el origen, número e impacto de las incidencias de seguridad registradas desde la puesta en marcha de la vigente Política de Seguridad, el coste e impacto de los controles establecidos en la empresa y los efectos de los cambios tecnológicos. Estas revisiones incluirán los sistemas de información, a los proveedores de sistemas, a los propietarios de información y de activos de información, a los usuarios y también a la Dirección.
La dirección de ZANTZA será, en definitiva, la encargada de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a los activos evaluados originalmente y a las situaciones de riesgo establecidas en el presente Documento.

El Sistema de Gestión de la Seguridad se auditará según un plan de auditorías desarrollado por el Responsable de Seguridad. El SGSI se auditará completamente cada tres años. Las revisiones deben ser llevadas a cabo por personal independiente al personal que es auditado . Aunque pueden ser llevadas a cabo por personal interno siempre de áreas o departamentos independientes al auditado, conviene que de forma regular se realicen auditorías de cumplimiento de la seguridad de la información por personal externo.

Las Auditorías realizan según lo descrito en el procedimiento PR-03 (Procedimiento para la realización de las Auditorias Internas).

2.8. COMPROMISO DE LA DIRECCIÓN
La presente Política de Seguridad es una línea de actuación clara, manifiesta y pública de ZANTZA, por lo que la Dirección expresa su apoyo total a la misma y se compromete a mantener las directrices fijadas en el presente Documento. Asimismo, publicará y entregará a todos sus empleados y de la forma más apropiada el presente Documento, para que todos conozcan el objetivo establecido por la Dirección, las políticas, principios y normas adoptadas y su importancia para la seguridad de la Organización, las responsabilidades generales y específicas en materia de seguridad de cada miembro de la empresa y otras referencias a documentación que puedan ser útiles.

3. ORGANIZACIÓN E INFRAESTRUCTURA DE SEGURIDAD

3.1. RESPONSABILIDADES
Para gestionar de forma eficiente la Seguridad de la Información, cada uno de los departamentos de ZANTZA donde esté en riesgo la Seguridad en la operación, servicio y funcionalidad del departamento, deberá cumplir las normas y los procedimientos que correspondan. Todas estas normas y procedimientos serán ratificados por la Dirección.
3.1.1. Dirección
La política de ZANTZA es responder por las obligaciones inherentes a la seguridad de la información y proteger sus activos de información implementando las medidas de seguridad más apropiadas para conseguirlo de una manera efectiva con los recursos disponibles.
3.1.2. Propietario de Activos
El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:
● Definir si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.
● Asegurarse de que el software que se utiliza tiene licencia.
● Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
● Asegurarse de que el activo cuenta con el mantenimiento adecuado
● Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al Responsable de Seguridad de la Información para tratar la incidencia.
● Asegurarse de que la plantilla cuenta con la formación adecuada, conoce y comprende la Política de Seguridad y pone en práctica las directrices de seguridad.
● Asegurarse de que los soportes y equipos que contengan información son desechados según lo establecido.
● Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.
● Mantener documentación actualizada de todas las funciones críticas para asegurar la continuidad de las operaciones en caso de que alguien no esté disponible.
● Informar al Responsable de Seguridad cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la empresa) para que se modifiquen apropiadamente los permisos de acceso.
● En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.
3.1.3. Responsable de Seguridad
El responsable de seguridad es responsable de la seguridad de los sistemas. Entre sus obligaciones están:
● Administrar y gestionar las cuentas de los usuarios.
● Asegurarse de que sólo las personas autorizadas a tener acceso cuentan con él.
● Asegurarse de que los sistemas tienen los niveles de disponibilidad requeridos por la Organización.
● Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que apliquen.
3.1.4. Personal
● Conocer y comprender la Política de Seguridad y los procedimientos que apliquen a su trabajo.
● Asegurarse de que sus acciones no producen ninguna infracción de seguridad.
● Informar al propietario del activo de cualquier incidencia de seguridad, real o sospechada, que detecte.
3.2. POLÍTICA DE USO ACEPTABLE
Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:
● La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
● Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están

autorizados a ello).
● El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
● Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
● Malgastar los recursos de la red de manera premeditada.
● Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
● Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
● Revelar las contraseñas y los medios de acceso voluntariamente.
● Utilizar los equipos para lucro personal
● La creación, utilización o transmisión de material ofensivo, obsceno o que pueda molestar u ofender.
● Enviar mensajes de correo muy grandes ó a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones)
● No verificar que los correos estén libres de virus
La evaluación de riesgos se realizará analizando los riesgos que afecten a los activos de la organización.
Cada activo tiene una valoración en términos de confidencialidad, disponibilidad e integridad
4.2. GESTIÓN DE RIESGOS
La gestión de esos riesgos implicará seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.
Se puede elegir entre las siguientes estrategias para mitigar el riesgo:
● Asumir el riesgo. Aceptar el riesgo y no implantar controles para su disminución o eliminación.
● Evitar el riesgo. Eliminar la causa o la consecuencia de dicho riesgo.
● Disminuir el riesgo. Limitar el riesgo implementando controles que disminuyan el impacto.
Transferir el riesgo. Pasar el riesgo a otros, como por ejemplo una aseguradora.

4. ANÁLISIS DE RIESGOS DE SEGURIDAD

El Informe de Análisis de Riesgos detallará las amenazas que se ha detectado que afectan a la Organización, el nivel de riesgo al que nos enfrentamos y cual va a ser la estrategia a seguir para los riesgos que no se consideren aceptables, es decir, si se va a asumir, a transferir, a evitar o a disminuir.
Un riesgo se considera que es aceptable cuando implementar más controles de seguridad se estima que consumiría más recursos que el posible impacto que pueda producir la ocurrencia, valorando la periodicidad de la misma. Como herramienta para medir la ocurrencia puede utilizarse la gestión de incidencias.
El Documento de Aplicabilidad especificará para cada control, si se aplica o no y el motivo por el que se toma esa decisión.
Los riesgos y los controles adoptados tras el análisis de los riesgos deben ser revisados anualmente, así como siempre que las circunstancias lo aconsejen. Esto se considerará una parte más de la gestión de la seguridad.
Para gestionar correctamente los activos el Responsable de Seguridad mantendrá un inventario actualizado de los activos importantes.
En este inventario se registrará quién es el propietario del activo. Esta responsabilidad será asignada al responsable del área ó departamento de ZANTZA donde esté ubicado física o lógicamente el activo.
5.2. CLASIFICACIÓN DE LA INFORMACIÓN
La clasificación de la información será de acuerdo con la siguiente escala:
Confidencial Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias serias para la organización
Uso Interno Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.
Publica Información sin ninguna necesidad de restringir el acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización

5. GESTIÓN DE ACTIVOS

Existirá una relación de cada tipo de documento existente en ZANTZA con la clasificación que le corresponde (uso interno / Publico / Confidencial). El personal de ZANTZA tendrá conocimiento de esta clasificación de manera que sepan en todo momento el tipo de información que utilizan, sin necesidad de establecer un marcado de la misma, no revelando así a fuentes externas la clasificación de la información. La destrucción de esta información la realizará el responsable del activo siguiendo las pautas aprobadas por el Responsable de Seguridad y con su colaboración si es necesaria.

5.3. DEVOLUCION DE ACTIVOS
Una vez superado el periodo de utilización, de relación laboral o acuerdo empresarial todos los empleados, contratistas, etc deberán devolver el Activo.
El Responsable de Seguridad, en función del tipo de Activo deberá actuar en consecuencia: transferencia y borrado de información de forma segura, devolución de equipos, devolución de llaves, modificación de accesos…
La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.
En las condiciones de la relación laboral deberán quedar reflejadas las responsabilidades del empleado en materia de seguridad de la información. Esta responsabilidad continuará durante un tiempo establecido tras la finalización del contrato.

6. SEGURIDAD DE LA GESTIÓN DE RECURSOS HUMANOS

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información secreta.
Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede. Se realizan periódicamente seminarios para que el personal conozca los procesos y tareas que deben realizar en materia de seguridad.
Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

7. SEGURIDAD FÍSICA Y DEL ENTORNO

Para que una seguridad lógica sea efectiva es primordial que las instalaciones de ZANTZA mantengan una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.

7.1. ÁREAS SEGURAS

ZANTZA tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las oficinas de ZANTZA cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.

Los lugares donde se ubican el servidor y el cableado estarán cerrados bajo llave y sólo tendrán acceso las personas autorizadas y los proveedores de servicios cuando vayan acompañados por alguien autorizado.

Las ventanas y puertas deberán permanecer cerradas cuando las instalaciones estén vacías.

Las instalaciones de ZANTZA están dotadas de dispositivos de extinción de incendios marcados por la legislación vigente en esa materia. En este sentido, se dispone de extintores y salidas de emergencia debidamente señalizados.

Se prohíbe expresamente al personal comer y beber cerca de los equipos informáticos. Así mismo, se tendrá especial cuidado con el manejo de cualquier producto que pueda verterse sobre activos de información.

Para la prevención de fugas de agua e inundaciones será necesaria la revisión periódica de la grifería, sanitarios y demás instalaciones que puedan causar daños de este tipo.

7.2. SEGURIDAD DE LOS EQUIPOS

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades de la organización, por lo que serán protegidos de manera adecuada y eficaz.

El servidor cuenta con medidas de protección de puerta cerrada, en armario rack cerrado, solo accesible por técnicos del DataCenter y la empresa alojadora.

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información.

Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

La eliminación de equipos sólo se llevará a cabo por el Responsable de Seguridad o personal en el que éste delegue.

8. GESTIÓN DE COMUNICACIONES Y OPERACIONES

8.1. PROCEDIMIENTOS OPERATIVOS Y RESPONSABILIDADES

ZANTZA controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de ZANTZA y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red de ZANTZA existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los trabajadores autorizados para el manejo de información automatizada deberán estar registrados como usuarios del sistema de información. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente al menos de manera trimestral.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

8.2. GESTIÓN DE LOS SERVICIOS SUMINISTRADOS POR TERCEROS

ZANTZA al contratar un servicio externo para gestionar activos de información introduce en el proceso nuevas vulnerabilidades, ya que los recursos se exponen a posibles daños, pérdidas o filtraciones de información. Por todo ello será necesario tomar una serie de precauciones que aseguren el perfecto uso de la información de ZANTZA.

Antes de contratar un servicio externo para la gestión de la información, ZANTZA identificará los riesgos que esta situación conlleva y elaborará un acuerdo en el que se traten las siguientes cuestiones: qué aplicaciones se mantienen en ZANTZA por su especial criticidad, la aprobación de los propietarios de la aplicación, qué implicaciones tiene el contrato para los planes de continuidad del negocio, las normas de seguridad y cómo se medirá su eficacia, quiénes son los responsables y qué procedimientos especiales se seguirán para monitorizar las actividades importantes de seguridad, quién y cómo manejará las incidencias de seguridad y mediante qué procedimientos se informará a ZANTZA de esas incidencias.

8.3. PROTECCIÓN FRENTE A CÓDIGO MALICIOSO Y CÓDIGO MOVIL

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de ZANTZA.

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la Red deberá ser evaluado por el Responsable de Seguridad.

El departamento de Informática instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

8.4. COPIAS DE SEGURIDAD

Habrá procedimientos para la realización de copias de seguridad que se archivarán para recuperar los datos en caso de incidencia. Estas copias estarán claramente identificadas y se guardarán en sitio seguro, preferiblemente fuera de las instalaciones de la organización.

También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

Si se corrompe la información en operación, hay que comprobar el software, el hardware y las comunicaciones implicadas antes de utilizar las copias de seguridad, para asegurarse de que no se pueda corromper la información contenida en ellas también.

8.5. GESTIÓN DE LA SEGURIDAD DE LA RED

Todos los equipos informáticos que estén o sean conectados a la red, o aquellos que en forma autónoma se tenga y que sean propiedad de ZANTZA deberán estar sujetos a las normas y procedimientos de instalación que emite el departamento de Informática y que han sido ratificados previamente por la Dirección.
Los elementos de red (switch, router...) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad de del sistema.

8.6. GESTIÓN DE SOPORTES

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.
Los soportes (tanto papel como lógicos) que contengan información sensible deben permanecer en cajones o armarios cerrados bajo llave. Cuando alguna persona autorizada deba utilizarla para realizar alguna gestión relacionada con las labores propias de la empresa, ésta se hará responsable del buen cuidado de los soportes. No los dejará encima de su mesa cuando abandone su puesto de trabajo ni los colocará en cualquier otro lugar donde una persona sin autorización pueda verlos o apropiarse de ellos.
Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas. Algunos procedimientos de destrucción que se consideran adecuados son la incineración, el triturado o vaciamiento de los soportes para que sean usados en otra aplicación dentro de la propia ZANTZA.
Siempre será necesario registrar la eliminación de soportes que contengan información sensible para mantener una pista de auditoría.

8.7. INTERCAMBIO DE INFORMACIÓN

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, , etc.).

8.8. SEGUIMIENTO

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implica realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario.

9. CONTROL DE ACCESOS

9.1. REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESOS

La información debe estar protegida contra accesos no autorizado.
Cada responsable de departamento o área definirá las necesidades de acceso a la información a dos niveles, para el conjunto del departamento o área y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.
En el caso de que visitantes o personal no autorizado acceda a las instalaciones o a la información de ZANTZA deberá ir siempre acompañado por un miembro responsable de ZANTZA que controlará en todo momento que la seguridad de los recursos está garantizada.

9.2. GESTIÓN DE ACCESOS DE LOS USUARIOS

El Responsable de Seguridad es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.
Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a Información y sistemas que no le son necesarios para las competencias de su trabajo.

9.3. RESPONSABILIDADES DEL USUARIO

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.
De igual forma, es necesario configurar los equipos informáticos para que éste quede bloqueado cuando el usuario no se encuentra en su puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el Terminal. También deben protegerse los puntos de entrada y salida de correo, y las impresoras que no se encuentren atendidas por alguna persona de ZANTZA.

9.4. CONTROL DE ACCESO A LA RED

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.
En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con la organización para mantener el mismo nivel de seguridad que si fueran empleados de ZANTZA.
El Responsable de Informática controlará las altas y bajas de todos los usuarios.

10. GESTIÓN DE INCIDENCIAS

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.
Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.
El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados

11. CONTINUIDAD DEL NEGOCIO

Es imprescindible para ZANTZA establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades del negocio por fallos graves en la seguridad o desastres de cualquier tipo.
Para garantizar la continuidad del negocio en estos casos, ZANTZA establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del negocio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del negocio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.
La gestión de la continuidad del negocio se incorporará a los procesos de ZANTZA y será responsabilidad de una o varias personas dentro de la empresa.