Obras Sanitarias del Estado

POLITICA DE SEGURIDAD DE LA INFORMACION

Versión 01

Junio 2013

1. Glosario de términos

1.1 Propósito y alcance

En esta sección se definen los términos que se utilizarán comúnmente en el documento de Política de Seguridad de la Información.

1.2 Objetivo del glosario

Un glosario de términos relacionados con la Seguridad de la Información, garantiza la unificación de criterios y significados, y permite que se apliquen consistentemente en todas las áreas de lo Organización. Si existe algún término en la política de seguridad que necesita ser aclarado, por favor contáctese con el CPSI.

1.3 Glosario

a) Acceso remoto
Conectarse a los recursos informáticos de red desde una ubicación externa a través de una red pública.

b) Activo
Todo aquello que tiene valor para la Organización.

c) Administrador de la información
Un Administrador de la información es una persona a la que los responsables de la información le delegaron obligaciones sobre el manejo de la misma.

d) Asociado de Negocio
Socio de OSE en el negocio.

e) Autenticación
Un proceso por el cual un sistema informático confirma la identidad de usuario, equipos o sistemas, usualmente por medio de la validación de una cuenta y el esquema de verificación de contraseñas.

f) Autorización
Permisos asociados con la identidad de un usuario.

g) Cifrado
Aplicación de un algoritmo específico a los datos a fin de alterar su apariencia y volverlos incomprensibles, para que sólo puedan ser accedidos por el destinatario.

h) Confidencialidad

Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

i) Datos
Cualquier información, sin importar la forma, contenida o procesada por el equipamiento de sistemas de información, redes de comunicaciones, o medios de almacenamiento. Estos datos pueden presentarse en diferentes medios incluyendo: copias impresas, medios magnéticos, fichas, almacenamientos en línea, materiales físicos, etc.

j) Disponibilidad
La característica de los datos, información, y sistemas de información a ser accesibles y utilizables en el momento y formas requeridos.

k) Funcionario
Es todo el personal de OSE.

l) Integridad
La característica de los datos y la información de ser correctos y completos; y la preservación de la corrección y completitud de los mismos a través de la certeza que el ingreso, modificación o eliminación de los datos es realizado solamente por personal autorizado.

m) Necesidad de conocer
Hace referencia a la necesidad que tiene un usuario, de conocer la información necesaria para el desempeño de las funciones que hacen a su rol en la organización.

n) Proveedor
Persona física o jurídica que provee o abastece a OSE de Bienes o Servicios. Debe estar inscrito en el Registro de Proveedores del Estado y en el Registro de Proveedores del Organismo.

o) Registro
Se refiere a cualquier información generada como resultado de un procedimiento o utilizada de acuerdo con un procedimiento que tenga requerimientos de retención.

p) Seguridad Física
Se refiere al conjunto tangible de controles, aplicado al acceso a aquellos activos de información que impactan en la operación continua del ambiente informático, y/o aplicado en activos que tienen un valor intrínseco alto para OSE

q) Seguridad Lógica
Se refiere a los controles basados en software, comúnmente en sistemas de información, que soportan los objetivos de la declaración de la política de seguridad.

r) Servicios de terceras partes
A propósito de este documento, los servicios de terceras partes incluyen: almacenamiento de datos y servicios de procesamiento de datos, proveedores de hardware/software, consultores de negocio y personal de seguridad. Los servicios de terceras partes también incluyen los tipos de servicios que no pueden proveerse internamente.

s) Sistemas de Información
Es el conjunto de activos de información que permiten la toma de decisiones en el negocio, independiente del medio en que se encuentren.

t) Usuarios principales del Sistema de Información:

- Un Responsable de la Información
  i. comprende claramente la naturaleza de la Información, pudiendo advertir si la misma está completa y es correcta.
  ii. en caso de no ser correcta, tiene la capacidad de corregirla en base a su propio conocimiento.
  iii. conoce el tiempo de guarda requerido para la información.

- Un Administrador de la Información es un funcionario, que tiene la responsabilidad de mantener y/o soportar la información corporativa.

- Un Usuario de la Información es un funcionario, autorizado a utilizar la información en el desempeño de sus tareas.

2. Política de Seguridad de la Información

2.1. Propósito y alcance

La Política de seguridad de la información debe proveer dirección y apoyo al Directorio al establecer un marco de implementación de seguridad, y asegurar el cumplimiento de la seguridad de la información en OSE.

2.2. Declaración de la política

La política de seguridad de la información debe proveer una dirección estratégica adecuada para demostrar la importancia de la seguridad de la información para la Organización.

2.2.1. Documento de la política de seguridad de la información

El Directorio debe aprobar, publicar, y apoyar la Política de Seguridad de la Información.

2.2.2. Revisión y evaluación de la política de seguridad de la información

La Política de Seguridad de la Información se revisará y actualizará en lo que se considere pertinente cada 2 años, sin perjuicio de que existan elementos que ameriten una revisión previa por parte de la CPSI (Comisión Permanente de Seguridad de la Información) y se elevara al Directorio para su evaluación y aprobación.

3. Seguridad Organizacional

3.1. Propósito y alcance

Esta política define los diferentes roles y responsabilidades dentro de la OSE, relacionados a la protección de los activos de información..

3.2. Declaración de la política

Cualquier persona vinculada con OSE tiene un rol a cumplir en la consecución de los objetivos de seguridad de la información.

Por medio de la definición clara de roles y responsabilidades relacionados a la seguridad de la información, OSE puede asegurar que exista una protección adecuada de sus activos.

3.3. Infraestructura de la Seguridad de la Información

3.3.1. La infraestructura tecnológica para el procesamiento de la información deben estar autorizados y aprobados por la Gerencia General. Cada uno de ellos debe cumplir con los requerimientos de seguridad de la OSE determinados por la Gerencia TI.

3.3.2. El uso de todos los dispositivos de procesamiento de información propiedad del personal (por ej. computadoras de los funcionarios, asistentes personales digitales, etc.) deben ser aprobados y autorizados por la Gerencia TI si los mismos son utilizados para almacenar y/o procesar información de OSE.

3.4. Cooperación entre Organizaciones

Los contactos de seguridad con las organizaciones externas deben ser supervisados por los funcionarios de OSE. Siempre que amerite, se exigirá la firma de un contrato de confidencialidad con la Organización involucrada.

3.5. Revisión independiente de la Seguridad de la Información

La política de seguridad de OSE, las medidas y el entorno de seguridad deberán ser revisadas por procesos de Auditoría Internos y/o Externos. Se sugiere en un período no mayor a 2 años.

3.6. Coordinación de la Seguridad de la Información

3.6.1. Comité de Seguridad

El Comité de Seguridad debe estar formado por representantes del Directorio, Gerencia General, Gerencia TI (Seguridad de la Información) y Oficina Jurídica Notarial.

Este comité debe reunirse al menos dos veces al año para:

- Revisar el estado actual de la seguridad de la información de OSE;
- Revisar y analizar el seguimiento de los incidentes de seguridad dentro de OSE;
- Aprobar las medidas de la Seguridad de la Información nuevas o modificadas; y
- Realizar cualquier otra actividad de administración de la seguridad de la información de alto nivel, que sea necesaria.

3.6.2. Comisión permanente de Seguridad de la Información (CPSI)

La función de esta comisión es ser rector de la Política de Seguridad de OSE.

Estará integrada por representantes de Jurídica, Gerencia General, Gerencia de TI entre otros.

Debe promover la seguridad a través de todos los procesos de negocio y garantizar que la misma esté contemplada en la planificación y ejecución de las iniciativas del mismo.

La CPSI es responsable de:

- revisar y actualizar la política de Seguridad de la Información de OSE.
- establecer y documentar las responsabilidades de seguridad en OSE;
- mantener la Política de Seguridad, medidas, y controles técnicos de seguridad , incluyendo su revisión frecuente;
- determinar y apoyar las metodologías adecuadas y los procesos para la seguridad;
- comunicar los conceptos básicos de seguridad a los usuarios, incluyendo la formalización e implementación de un programa de Concientización en Seguridad;

- desarrollar, identificar, y documentar los controles técnicos de seguridad, incluyendo el seguimiento de las vulnerabilidades de los sistemas documentados por los proveedores y las organizaciones de seguridad externas;
- realizar el seguimiento del cumplimiento y de la aplicación de la Política de Seguridad de OSE;
- administrar e investigar cualquier incidente de seguridad y/o violación a la seguridad de OSE y asistir a otros grupos de la Organización en el manejo de los mismos;
- asistir a las distintas Áreas en la identificación de amenazas y vulnerabilidades de Seguridad de la Información, en base a las cuales cada una realizará un análisis de riesgo para tomar las medidas correspondientes.

3.7. Asignación de responsabilidades sobre la Información de OSE

Se definen tres categorías:

3.7.1. Responsable de la Información

- comprende claramente la naturaleza de la Información, pudiendo advertir si la misma está completa y es correcta.
- en caso de no ser correcta, tiene la capacidad de corregirla en base a su propio conocimiento.
- conoce el tiempo de guarda requerido para la información.

Las funciones de un responsable de la información incluyen:

- Aprobar los niveles iniciales de clasificación de información;
- Realizar revisiones periódicas para asegurar que la clasificación de la información actual cumple con las necesidades del negocio;
- Asegurar que existen controles de seguridad acordes a la clasificación;
- Asegurar que la información está etiquetada de acuerdo a su clasificación independientemente del medio que la contiene
- Determinar el criterio de seguridad en el acceso a la información ;
- Verificar que los derechos de acceso estén actualizados;
- Determinar los requerimientos de respaldo para la información de la cual es responsable;

- Archivar la información, ya sea manualmente o utilizando alguna herramienta de software.
- Mantener la información actualizada y/o supervisar las modificaciones que la misma sufra.
- Autorizar, y eventualmente realizar la eliminación de información del Sistema de Información de OSE
- Tomar las acciones adecuadas en caso de violaciones de seguridad.

Los Responsables de la Información tienen derecho a delegar el mantenimiento de los datos y las responsabilidades por la propiedad de la información a los Administradores de la Información. Cuando los Responsables de la Información eligen delegar, deben existir acuerdos de nivel de servicio entre el Responsable de la Información y el Administrador de la Información donde se comuniquen las expectativas y responsabilidades. El Responsable de la Información debe designar uno o más Administradores de la información basado en el nivel de responsabilidades delegadas.

3.7.2. Administrador de la Información: es un funcionario u otra persona autorizada que tiene la responsabilidad de mantener y/o soportar la información corporativa.

Las funciones de un Administrador de la información incluyen, pero no están limitadas a:

- Instrumentar la custodia de la información, ya sea mediante procedimientos manuales o automáticos.
- Conocer y/o administrar las herramientas mediante las cuales se registra/almacena/procesa/distribuye la información.
- Posibilitar la utilización de las herramientas para realizar altas, bajas y modificaciones sobre la información.
- Apoyar en las tareas de recuperación de la información ante incidentes.

El Administrador de la Información debe brindar lo siguiente:

- niveles de servicio adecuados para el Responsable de la Información
- asistencia al Responsable de la Información para determinar las mejores soluciones técnicas
- seguridad en el trato de la confidencialidad, disponibilidad e integridad de la información.

3.7.3. Usuario de la Información: es un funcionario u otra persona autorizada a utilizar la información en el desempeño de sus tareas.

Las funciones de un Usuario de la información incluyen, pero no están limitadas a:

- Mantener la confidencialidad de las contraseñas de los sistemas operativos y las aplicaciones
- Reportar cualquier sospecha de violación de la seguridad a la CPSI.
- Adherir a la Política de Seguridad de la Información de OSE, medidas, y controles técnicos; y
- Utilizar la información corporativa y los recursos de información con responsabilidad y los propósitos autorizados.

3.7.4. Administradores.

3.7.4.1. **Los Administradores de Sistemas** son quienes deben mantener, operar e implementar las soluciones tecnológicas para la Organización.

Son responsables de instalar, implementar, y realizar el seguimiento de los controles de seguridad dentro de la operativa básica. Los lineamientos para los controles específicos deben ser dados por GTI, incluyendo:

- la aplicación de actualizaciones de seguridad del sistema;
- la documentación de sistemas;
- el seguimiento de performance y seguridad de los sistemas;
- aplicación de los controles técnicos de seguridad necesarios
- la comunicación sobre incidentes y asuntos relacionados a la seguridad.

3.8. Terceras partes

3.8.1. Se considera Proveedor a cualquier persona o compañía que provee productos y/o servicios a OSE.

3.8.2. OSE debe establecer requerimientos para que los proveedores adhieran como mínimo al mismo nivel de restricciones que sus funcionarios. El acceso a la información debe estar limitado a las necesidades laborales.

3.8.3. Las compañías que proveen productos y/o servicios a la OSE deben firmar un Acuerdo de Confidencialidad independientemente de su

ubicación física. La CPSI, deben proveer los mecanismos para que los proveedores firmen Acuerdos de Confidencialidad adecuados.

3.8.4. Todo el personal no perteneciente a la OSE que requiera acceso a los recursos vinculados al Sistema de información, debe disponer de la autorización de un funcionario responsable de la información de la misma. No se dará acceso hasta que se obtenga una autorización por el funcionario correspondiente.

3.8.5. Donde, por una necesidad de negocio se deba contar con una conexión con terceras partes, la misma debe ajustarse al estándar definido por OSE, el cual determina las implicancias de seguridad asociadas a la misma, y los requerimientos de control.

3.8.6. El acceso remoto, por parte de los proveedores, a los sistemas de información de OSE será provisto basándose en las necesidades del negocio. La configuración de la conexión requerida debe estar por defecto deshabilitada hasta que su uso sea necesario. Una vez completada las tareas, debe deshabilitarse la conexión.

3.8.7. Las organizaciones externas no tienen permitido el acceso ilimitado a las computadoras o redes de la Organización.

3.9. Requerimientos de seguridad en contratos de outsourcing

3.9.1. Los responsables de los contratos de outsourcing deben solicitar y verificar información de los proveedores y usuarios involucrados en los mismos, de acuerdo a las leyes, regulaciones y normativas existentes; y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida y los riesgos percibidos.

3.9.2. Los contratos de servicios informáticos y de outsourcing deben ser desarrollados de acuerdo al siguiente proceso:

(a) Análisis de las necesidades del negocio y/o análisis de costo/beneficio;

(b) Preparar un pedido de propuesta;

(c) Evaluar proveedores y las ofertas presentadas;

(d) Identificar requerimientos de contratos

(e) Realizar el seguimiento a las actividades tercerizadas.

3.9.3. El equipo de OSE responsable de la selección y aprobación de servicios de terceros y un representante Jurídico, deben aprobar todos los acuerdos de servicios de información contratados. La aprobación de la

Gerencia TI de OSE también debe obtenerse si los servicios provistos afectan la seguridad o la integridad de las redes de la misma.

3.9.4. La Gerencia TI y la CPSI en caso que lo amerite, debe asegurar que se obtengan los registros apropiados teniendo en cuenta la estructura de control a la que estarán sujetos los proveedores que realicen funciones de procesamiento de datos críticos, o tengan acceso a información sensible. También debe asegurar que el contrato sea adecuado a efectos de sostener la política de seguridad de la información, lineamientos y procedimientos de la organización.

3.9.5. El gerente responsable de los contratos con servicios de procesamiento de datos externos debe especificar los requerimientos de seguridad y las acciones a tomar por violaciones en los contratos.

3.9.6. La propiedad del software desarrollado por personal externo debe estar específicamente definida en el acuerdo del contrato.

3.9.7. Todos los contratos de servicios informáticos y/o outsourcing deben incluir lo siguiente:

- acuerdos de controles de seguridad y políticas aceptables;
- una cláusula de “Derecho a auditar” asegurando que el personal de OSE y/o los representantes autorizados deben evaluar física o lógicamente el ambiente de control de las terceras partes
- determinación de niveles de servicio aceptables y disponibilidad;
- documentación de controles físicos y lógicos definidos por el proveedor para proteger la confidencialidad, integridad y disponibilidad de los datos y equipamiento de OSE;
- determinación de todos los requerimientos legales, incluyendo privacidad y protección de datos
- acuerdos referentes a que el proveedor debe probar y mantener la seguridad del sistema sobre una base reglamentada.
- lineamientos para designar otros participantes involucrados y las condiciones para su acceso.

3.9.8. El proveedor es responsable por informar inmediatamente al gerente responsable del contrato, de cualquier brecha en la seguridad, incluyendo accesos no autorizados, o que ciertos datos o recursos de la Organización se encuentren comprometidos. Cualquier funcionario que esté al tanto de violaciones de seguridad por proveedores debe reportarlo a la CPSI.

4. Clasificación y control de activos

4.1. Propósito y alcance

Esta política define los requerimientos para la clasificación y control de activos. Un activo es definido como cualquier ítem tangible o no, poseído o controlado por OSE. Esto incluye activos lógicos y físicos.

Esta política se aplica para todos los Funcionarios, Proveedores y Asociados de Negocio de OSE.

4.2. Declaración de la Política

Todos los activos de OSE (tangibles o no) deben tener un responsable y ser controlados de manera adecuada. Estos activos son cruciales para el éxito de OSE y deben ser protegidos por los controles adecuados para minimizar cualquier riesgo de daño, interrupción de servicios o revelación de información propietaria.

Toda la información, debe ser clasificada por las definiciones descriptas en el punto 4.4 “Guías para la clasificación de la información".

4.3. Medidas de Seguridad Generales

4.3.1. La Gerencia Financiero Contable (Activo Fijo) debe recopilar y mantener un catálogo de todos los activos físicos poseídos por OSE. Este catálogo debe ser revisado y actualizado periódicamente. El mismo debe contener información descriptiva de los activos (por ej. tipo de activo, ubicación física (si aplica), parte dueña /responsable, clasificación y criticidad, etc.)

4.3.2. La Gerencia TI (Gestión de equipamiento) debe recopilar y mantener un catálogo de todos los activos de software. Este catálogo debe ser revisado y actualizado periódicamente y debería contener información descriptiva del activo (proveedor, ubicación lógica/aplicaciones o sistemas asociados, ubicación física, responsable, responsabilidades del Administrador de los datos, clasificación de información, y el nivel de criticidad).

4.4. Guías para la clasificación de la información

4.4.1. Las personas que envían información deben asegurarse de que quienes la reciben tienen derecho a conocerla antes de transferirla. El principio de “derecho a conocer” debe definirse en función de los procesos de negocio. Si el usuario necesita acceder a la información para cumplir

con un proceso de negocio real, entonces le será permitido el acceso a dicha información.

4.4.2. La información de OSE en cualquier formato y contenedor de información (por ej. en papel, discos, cintas, etc.) debe ser protegida por todos los Funcionarios, Proveedores y Asociados del Negocio de OSE, vinculados a la misma, de una forma adecuada, según su valor determinado por la clasificación de la misma.

4.4.3. A efectos de proteger los activos de información se deben clasificar de acuerdo a la Ley 18381 (Dec.232/10) en:

- Información pública (**Art. 4º.**).- Se presume pública toda información producida, obtenida, en poder o bajo control de los sujetos obligados por la presente ley, con independencia del soporte en el que estén contenidas.
- Información reservada (**Art. 9º.**).- Como información reservada podrá clasificarse aquella cuya difusión pueda:
  - a) Comprometer la seguridad pública o la defensa nacional.
  - b) Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de reservado al Estado uruguayo.
  - c) Dañar la estabilidad financiera, económica o monetaria del país.
  - d) Poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona.
  - e) Suponer una pérdida de ventajas competitivas para el sujeto obligado o pueda dañar su proceso de producción.
  - f) Desproteger descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de los sujetos obligados.
- Información confidencial (**Art. 10.**).-Se considera información confidencial:
  - I) Aquella entregada en tal carácter a los sujetos obligados, siempre que:

    a) Refiera al patrimonio de la persona.

    b) Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica, que pudiera ser útil para un competidor.

    c) Esté amparada por una cláusula contractual de confidencialidad.

- II) Los datos personales que requieran previo consentimiento informado.
  Tendrán el mismo carácter los documentos o secciones de documentos que contengan estos datos.

4.4.4. La información sensible, en cualquier formato, requiere procedimientos especiales durante el almacenamiento para protegerla de divulgación accidental o maliciosa.

4.4.5. La clasificación de la información no puede ser modificada sin una previa autorización del Responsable de la información.

4.4.6. El Responsable de la información debe realizar el seguimiento y revisar continuamente la clasificación de la misma.

4.5. Manipulación e identificación de la información

4.5.1. Todos los medios deben ser etiquetados con su clasificación de información (p.ej. “pública”, “confidencial” o “reservada”).

4.5.2. La información electrónica clasificada “pública” puede ser almacenada en cualquier sistema informático de OSE. Se deben realizar esfuerzos para separar la información “pública” de la “reservada”.

4.5.3. Todos los datos "confidenciales" y "reservados" deben ser marcados al comienzo y final de cada página con la clasificación de la información contenida en el documento.

4.5.4. Los documentos electrónicos deben tener la etiqueta de clasificación en el encabezado y final de cada página.

4.5.5. Los documentos en papel deben ser sellados con la clasificación o debe aplicarse una etiqueta física.

4.5.6. Todos los documentos "confidenciales" o "reservados" deben tener una carátula identificando la clasificación de la información.

4.5.7. La información identificada como "reservada" debe estar segura en una de las siguientes maneras:

- La información en papel debe mantenerse en un área de acceso controlado, que permanezca cerrado (asegurado) cuando no se encuentre ocupado. La información en papel también puede ser almacenada en archivos bajo llave con acceso limitado si no hay disponible una sala segura.

- La información electrónica debe estar encriptada usando un método aprobado por la Gerencia TI, cuando se almacene en cualquier medio.

5. Seguridad del Personal

5.1. Propósito y alcance

La política define las medidas de seguridad que deben aplicarse con respecto al personal.
Deberán seguirse para asegurar que los potenciales funcionarios sean evaluados correctamente antes de vincularse al organismo y que luego sean fácilmente identificables. Que sus accesos sean revocados o modificados en caso de desvincularse al organismo o sean trasladados dentro del mismo. También deberán seguirse medidas complementarias que aseguren la concientización de todo el personal en cuando a su responsabilidad en la seguridad y las acciones a realizar ante el reporte de accidentes.

5.2. Declaración de la política

El personal que trabaja para OSE es el activo mas importante de la organización. Sin embargo, una gran cantidad de problemas de seguridad, pueden ser causados por descuidos, desinformación o incluso sabotaje. Deben implementarse los procedimientos para manejar estos riesgos, y ayudar al personal a crear un ambiente de trabajo seguro.

5.3. Responsabilidades generales

5.3.1. Todos los Funcionarios, Proveedores y personas con acceso a las instalaciones e información de OSE, deben regirse de acuerdo a las medidas establecidas en la política de seguridad del organismo como una de sus responsabilidades principales.

5.3.2. La Gerencia de Gestión del Capital Humano debe realizar una evaluación de todos los funcionarios a contratar. Se les facilitará a los funcionarios capacitación en temas de Seguridad de la Información.

5.3.3. La Gerencia de Gestión del Capital Humano debe notificar inmediatamente a la Gerencia de TI en caso de desvinculación o traslado de personal quien debe asegurar el borrado o modificación de todo lo que permita el acceso a recursos de la información.

5.3.4. Todos los usuarios del sistema de información de OSE o de su infraestructura de soporte son responsables de aplicar y comprender las políticas y procedimientos de seguridad.

5.3.5. Todos los usuarios deben firmar un Compromiso de Confidencialidad antes de acceder a las instalaciones restringidas

5.3.6. Los Proveedores o Asociados del Negocio de OSE deben estar cubiertos por un Acuerdo de confidencialidad, bajo el contrato de Terceras Partes.

5.3.7. La correcta responsabilidad por la seguridad es parte de los términos y condiciones del vínculo laboral. Violar o ignorar las responsabilidades y medidas documentadas en la Política de seguridad de OSE, habilitará a OSE a ejercer todas las acciones y recursos legales que entienda pertinentes.

5.3.8. La revisión casual del correo electrónico y del correo de voz por parte de los Administradores es una violación de la política de Seguridad de OSE. Excepcionalmente frente a la posibilidad de un uso inadecuado, el jerarca de la organización, podrá solicitar el análisis de dicho contenido con las debidas garantías para los involucrados.

5.3.9. Las responsabilidades de seguridad se extienden más allá de las instalaciones de OSE con respecto a la información de la organización. Por lo tanto, los funcionarios deben mantener la confidencialidad de la información en situaciones fuera del trabajo.

5.4. Entrenamiento y concientización del personal en seguridad

5.4.1. Es responsabilidad del CPSI, promover constantemente la concientización en seguridad para todos los usuarios de los sistemas de información.

5.4.2. La Gerencia TI es responsable por enviar avisos de seguridad a todos los usuarios quienes pueden ser afectados por temas de seguridad en los sistemas informáticos. Estos avisos deben incluir alertas sobre riesgos específicos como ser virus, ingeniería social, nuevas vulnerabilidades técnicas y riesgos específicos de OSE y las medidas asociadas a tomar.

5.5. Respuesta a fallas e incidentes de seguridad

5.5.1. La CPSI debe documentar todos los reportes de incidentes de seguridad. Debe también incluir un proceso para revisar todos los incidentes, documentar los casos ocurridos y coordinar sesiones de capacitación y aprendizaje para las áreas aplicables dentro de OSE.

5.5.2. Las acciones resultantes de la violación de cualquier política por parte de los asociados o proveedores de OSE, serán consistentes con la seriedad del incidente, determinada mediante una investigación pertinente. Las sanciones derivadas de este incumplimiento pueden incluir, pero no están limitadas a: pérdida de privilegios de acceso a los recursos de procesamiento de datos, u otras acciones que se consideren apropiadas.

6. Política de uso aceptable

6.1. Propósito y alcance

Esta política define el uso apropiado de los recursos informáticos. La misma se refiere a la información almacenada o transferida por medio de redes informáticas, teléfonos u otros dispositivos de comunicaciones, así como al uso y protección de los activos físicos en sí mismos. Esta política se aplica para todos los Funcionarios, Proveedores y Asociados de Negocio de OSE.

Declaración de la Política de Seguridad de la Información de OSE.

El uso de computadoras, redes, teléfonos y demás dispositivos se ha generalizado, constituyendo una parte esencial al hacer negocios. Es responsabilidad y obligación de cada usuario, asegurar que todos los recursos informáticos y de comunicaciones son utilizados solamente para su propósito de negocio y que la información contenida o transmitida por estos medios, sea protegida de usos no autorizados, apropiación o corrupción.

6.2. Uso aceptable de Internet

6.2.1. La conectividad a Internet será al personal con fines de negocio válido y justificado y con la autorización adecuada.

6.2.2. La conectividad a Internet será dada al personal con fines de negocio válido y justificado y con la autorización adecuada.

6.2.3. El acceso a Internet estará disponible para el personal de la Organización a efectos de permitirles llevar a cabo actividades directamente relacionadas con sus responsabilidades dentro de la organización.

6.2.4. Los usuarios deben estar al tanto de los riesgos asociados al acceso a Internet. Estos incluyen la falta de confidencialidad e integridad de la información accedida o enviada vía Internet.

6.2.5. Los usuarios no deben divulgar en Internet, información clasificada como reservada o confidencial

6.2.6. No se debe enviar vía mail ninguna comunicación considerada crítica o necesaria, a menos que se realicen esfuerzos suficientes para asegurar la entrega y transmisión de la misma en forma segura. Los usuarios no deben usar direcciones de la organización para publicar información en sitios de Internet públicos.es de dejar disponible nueva información en los servidores

de información, es necesaria una aprobación por parte del responsable de la misma.

6.2.7. Los usuarios autorizados deben utilizar los mecanismos aprobados e implantados por OSE para la salida a Internet.

6.2.8. Cada Gerencia deberá aprobar los contenidos de los datos que desea publicar.

6.2.9. GTI es responsable de la definición técnica de la publicación de los datos así como el control del tráfico y ancho de banda.

6.2.10. Cualquier información publicada por funcionarios de la Organización, en grupos de discusión, redes sociales, etc. no debe divulgar ningún tipo de información de la organización, sin ser previamente aprobada por la superioridad.

6.2.11. Los usuarios deben saber que cuando se navega en Internet, cada servidor web puede obtener información relativa a la computadora que se esté utilizando, en algunos casos respecto a las preferencias de la persona y otros sitios de Internet que se han visitados durante la sesión.

6.2.12. La información transferida desde direcciones de correo de la Organización debe ser tratada con las mismas medidas que la información que sale de OSE en papel membretado. Se realizará el seguimiento del uso de Internet bajo políticas de control de acceso y contenidos.

6.3. Uso aceptable de las comunicaciones telefónicas con fines corporativos

6.3.1. Cuando se utiliza cualquier tipo de teléfono, especialmente con alto parlantes, para discutir información sensible, los usuarios deben asegurarse que sus conversaciones no son escuchadas.

6.3.2. El responsable/auspiciante de una conferencia telefónica debe asegurarse que sólo las personas autorizadas están conectadas a dicha conferencia.

6.3.3. Cualquier información clasificada como Reservada o Confidencial no debe ser dejada como mensajes de voz en sistemas internos o externos.

7. Seguridad física y ambiental

7.1. Propósito y alcance

Esta política define los niveles mínimos de seguridad física para las instalaciones con equipamiento y o información de OSE, con el objeto de proteger los activos de información ubicados en dichas instalaciones.

Se establecen medidas que deben observarse a los efectos de lograr esos mínimos de protección física. La misma aplica a todos los Funcionarios, Proveedores y Asociados de Negocio de OSE.

7.2. Declaración de la política

Las medidas de seguridad física que se establezcan, tendrán como objeto el asegurar la integridad de las instalaciones edilicias, de los bienes materiales y de los activos de información,–cualquiera sea el soporte físico de éstos. Estas medidas estarán de acuerdo con la clasificación propuesta para los activos de información involucrados, de acuerdo a lo establecido en la presente Política

7.3. Áreas de acceso restringido

Cualquier instalación de OSE, que sea considerada como crítica y requiera por lo tanto una mayor seguridad física, deberá tener sus propios perímetros físicos de seguridad. Estas áreas se definen como “áreas de acceso restringido”.

7.4. Controles de entrada física

7.4.1. Las áreas de acceso restringido deberán contar con controles de acceso con registro de logs y eventualmente cámaras de vigilancia.

7.4.2. Todos los funcionarios, Proveedores y Asociados de Negocio de OSE, deben cumplir con los lineamientos de la Seguridad de la Información referidas a tarjetas de identificación.

7.4.3. El acceso físico a las áreas de acceso restringido debe ser fuertemente controlado. Las puertas deben estar trancadas en todo momento y sólo el personal autorizado debe tener la llave o combinación.

7.4.4. El personal autorizado no debe permitir que personas desconocidas o no autorizadas ingresen en áreas de acceso restringido sin compañía. Cualquier persona no identificada o personal no acompañado en un área restringida de OSE debe ser inmediatamente indagado acerca de la causa de su presencia allí.

7.5. Perímetro de seguridad física

7.5.1. Las instalaciones de OSE dispondrán de un perímetro de seguridad, la fortaleza de este será determinada por un análisis de los riesgos y amenazas del ambiente físico.

El perímetro de seguridad incluye una lista que no es exhaustiva:

- La definición de las instalaciones y de la frontera.
- Componentes físicamente sólidos –tales como: paredes, puertas, ventanas, etc.–
- Área de recepción controlada por personas en la entrada principal de las instalaciones y controles apropiados en las entradas secundarias.
- Puertas de control conectadas con la central de detección de incendios, a los efectos de cumplir con los requerimientos de seguridad.

El perímetro de seguridad deberá cumplir con todas las regulaciones aplicables en la materia.

7.6. Seguridad de oficinas, habilitaciones y demás facilidades

7.6.1. Movimientos de activos

Los Funcionarios, Proveedores y Asociados de Negocio de OSE, no deben mover activos de las instalaciones de OSE, sin autorización previa. Todas las personas deben estar al tanto de que pueden llevarse a cabo inspecciones sin previo aviso. Todo el equipamiento que es movilizado debe ser registrado.

7.6.2. Seguridad en oficinas, salas e instalaciones

Todas las salas de informática y centros de datos deben ser supervisados las 24 horas del día. Esta supervisión podrá realizarse a través de cámaras de vigilancia, puertas y ventanas con alarmas, personal de seguridad o una combinación de ellos.

7.6.2.1. Los edificios en los que se encuentran las computadoras de la Organización o los sistemas de comunicaciones se deben proteger con medidas de seguridad física que prevengan accesos no autorizados.

7.6.2.2. El acceso a las salas de área restringidas se debe limitar solamente a aquellas personas que tengan razones de negocio válidas para su ingreso.

7.6.2.3. Los centros de cómputos y centros de datos de OSE deberán clasificarse como áreas de acceso restringido.

7.6.2.4. La información interna que identifique la ubicación de las áreas de acceso restringido de OSE no debe estar disponible para el público.

7.6.2.5. Cualquier material peligroso o combustible se debe almacenar a una distancia prudencial de las “áreas de acceso restringido”, de acuerdo a las regulaciones locales de seguridad y a las especificaciones de fábrica de dichos materiales.

7.6.2.6. Las instalaciones de respaldo y recuperación se deben ubicar a una distancia segura de las instalaciones principales, a los efectos de protegerlas de daños en caso de incidentes en las primeras.

7.6.3. Trabajo en áreas de acceso restringido

7.6.3.1. Cualquier persona que trabaje o tenga acceso a “áreas de acceso restringido” debe estar informada de los requerimientos de seguridad de dicha área, los detalles del perímetro de seguridad y las responsabilidades asociadas del trabajo en la misma.

7.6.3.2. No se permite el registro de imágenes, ni el registro de audio de las instalaciones, a menos de que exista una autorización específica

7.6.3.3. Cualquier tercera parte que tenga acceso a un “área de acceso restringido” debe ser controlada y supervisada estrictamente.

7.6.3.4. Cualquier área clasificada como “área de acceso restringido” debe permanecer trancada cuando está vacía.

7.7. Seguridad del equipamiento

7.7.1. Mantenimiento del equipamiento

7.7.1.1. Todo el equipamiento debe ser mantenido correctamente para proveer la disponibilidad, proteger la integridad y confidencialidad de la información. El equipamiento debe ser

supervisado e inspeccionado considerando las especificaciones de fábrica. Las reparaciones deben ser realizadas por personal de mantenimiento autorizado, y todos los trabajos de servicios o reparaciones deben ser registrados. Si el equipamiento tiene que ser enviado fuera de las instalaciones para su reparación, se debe asegurar la integridad y confidencialidad de la información.

7.7.2. Ubicación y protección del equipamiento

7.7.2.1. Todo el equipamiento de OSE debe ser ubicado teniendo en consideración el minimizar los riesgos y las amenazas. Esto incluye:

- riesgo de robo o vandalismo.
- riesgo de fuego, explosión, humo, agentes químicos, inundaciones.
- pérdida de servicios tales como energía, comunicaciones o agua.

7.7.2.2. El equipamiento informático debe ser ubicado en un ambiente equipado con detectores de humo, en la medida de lo posible, y medidas preventivas. Alterar o retirar dichos detectores será considerado falta funcional grave.

7.7.2.3. Para minimizar robos o daños causados por el agua, las instalaciones informáticas deben estar ubicadas por encima, en la medida de lo posible, del primer piso del Edificio correspondiente.

7.7.2.4. Todo el equipamiento de informática debe operar con clima controlado en todo momento. Deben proveerse sistemas de acondicionamiento de respaldo para el caso de que los sistemas principales fallen.

7.7.2.5. Los sistemas de detección y extinción de incendios deberán ser probados según las normas vigentes, los resultados de estas pruebas deberán ser documentados y los registros serán guardados por lo menos un año.

7.8. Energía eléctrica

7.8.1. A los efectos de evitar fallas en la energía, se debe contar con una fuente de energía eléctrica adecuada, de manera que se puedan evitar puntos de falla individuales.

7.8.2. Se deben utilizar unidades UPS (Uninterrupted Power Supply) para dar soporte a las operaciones del negocio críticas, a los efectos de realizar un cierre ordenado y permitir a los sistemas que sigan operando. Las

mismas deberán ser supervisadas según lo establezca la normativa específica.

7.9. Desecho o re-utilización segura de equipamiento

7.9.1. En cualquier equipo de procesamiento de información de OSE que deba ser desechado, o re-utilizado se debe realizar la remoción, el borrado seguro de toda la información que este contenga., según establece la presente Política.

7.9.2. En el caso de que no sea posible el borrado seguro de la información y esta sea clasificada como Reservada o Confidencial, se deberá destruir el soporte físico de la misma.

7.10. Controles generales

7.10.1. Todos los puntos de entrada y salida de información –correo electrónico, fotocopiadoras, equipos de fax, etc., deben ser protegidos de accesos no autorizados y del uso impropio de los mismos.

7.10.2. Todos los medios de almacenamiento de información, que contengan datos Ejecutivos, Operacionales y de Desarrollo, deberán estar protegidos contra accesos no autorizados.

7.11. Política de escritorios limpios

7.11.1. Toda la información sensible deberá ser guardada en lugares seguros, armarios o salas de archivo bajo llave. Si la información clasificada como Reservada o Confidencial ni va a ser ni utilizada ni archivada debe ser destruida.

7.11.2. Los funcionarios, Proveedores y Asociados de Negocio de OSE, deberán retirar todos los documentos impresos con información clasificada como Reservada o Confidencial (en impresoras, equipos de fax, fotocopiadoras), en forma inmediata a la impresión, para evitar accesos no autorizados.

7.12. Política de pantallas limpias.

7.12.1. Ninguna computadora debe estar logueada cuando no esté siendo utilizada por el usuario. En el caso de que el equipo no se esté utilizando, deberá estar bloqueado y protegido con contraseña de seguridad.

7.12.2. Cuando sea necesario, se deberán tomar medidas para asegurar que luego de cierto período de tiempo de inactividad, el equipo sea automáticamente bloqueado.

8. Política de comercio electrónico

8.1. Propósito y alcance

El propósito de esta política es exponer cuál es el comportamiento adecuado cuando se lleva a cabo comercio electrónico en OSE. Cuando aplique, los controles mencionados intentan proteger la actividad de numerosas amenazas que pueden resultar en acciones fraudulentas, problemas con contratos y revelación o modificación indebida de la información. Esta política debe ser cumplida por todos los funcionarios de OSE relacionados con el comercio electrónico, así como Proveedores y Asociados de negocio en ésta área.

8.2. Declaración de la política

OSE debe asegurar la claridad de toda la información documentada y relevar la información necesaria para garantizar la realización apropiada de los eventos y transacciones de comercio electrónico. OSE y sus socios deben cumplir con la legislación nacional teniendo en cuenta toda la información relacionada con los usuarios.

Los sistemas de información deben asegurar el cumplimiento de las medidas de seguridad corporativas antes de estar disponibles en producción. En los sistemas de comercio electrónico se deben publicar los términos de negocio referidos a los usuarios. El uso de archivos de autoridades de certificación y terceras partes en las que se confía, debe estar documentado de acuerdo a la Política de Seguridad de la Información de la OSE.

Las actividades relacionadas a roles y responsabilidades, entre OSE y los socios de comercio electrónico se deben establecer, documentar y respaldar por un acuerdo que comprometa a ambas partes en los términos acordados en las transacciones.

8.3. Obtención de datos y privacidad de la información

8.3.1. La Organización debe utilizar niveles de seguridad apropiados, según el tipo de información recopilada, mantenida o transferida a terceras partes, y debe:

- Aplicar medidas de seguridad de cifrado y autenticación corporativas para la transferencia de información sensible;
- Aplicar controles de seguridad corporativa pertinentes para proteger los datos almacenados en su infraestructura y base de datos.

- Requerir a las terceras partes involucradas en el cumplimiento de transacciones de usuarios, que mantengan niveles de seguridad apropiados.

8.3.2. La política de privacidad de la información en comercio electrónico debe ser fácil de ubicar y comprender; ser abierta, transparente y debe contar con información acerca de principios generalmente aceptados, cumpliendo en todos sus términos con la Ley de Protección de Datos y acción de Habeas Data (Ley 18331, Dec.414/2009).

8.3.3. OSE y sus socios de comercio electrónico deben cumplir con la legislación nacional referente al uso de información de usuarios o estadísticas derivadas, lo que incluye pero no se limita a lo siguiente:

- Indicar la información personal que se recaba, utiliza y revela
- Las opciones que el cliente tiene con respecto a la recopilación, uso y revelación de su información
- Si existen medidas de seguridad a efectos de proteger la información.

8.3.4. OSE debe adoptar prácticas de información que traten la información personal de clientes con sumo cuidado. Todos los sitios de comercio electrónico de OSE deben adherir a una política de privacidad basada en principios de información claros, adoptar medidas apropiadas para proveer la seguridad adecuada, y respetar las preferencias de los clientes en relación a la forma de envíos de información.

8.4. Difusión *de la información*

8.4.1. Todas las difusiones deben ser:

- claras, precisas y fáciles de encontrar y comprender;
- públicamente accesible (Por ej., en línea, con un link descriptivo);
- presentadas de tal forma que los usuarios puedan acceder y mantener registros adecuados;
- relativas a productos y servicios disponibles para la compra en línea o a la transacción en sí, y
- accesibles antes de que se cierre la transacción.

8.4.2. La información acerca de OSE debe comprender los siguientes datos de contacto, como mínimo:

- Nombre legal;
- Nombre bajo el cual se conduce el negocio;
- Dirección de contacto, incluyendo el país;
- Un método de contacto en línea (por ej., dirección de correo electrónico);
- Un punto de contacto dentro de la organización, es decir, el responsable por las preguntas de usuarios

8.4.3. OSE debe proveer información suficiente en relación a la transacción en línea, que permita a los usuarios involucrados tomar decisiones informadas acerca de si realizan o no dicha transacción.

La información puede incluir:

- Términos de la transacción;
- Disponibilidad del servicio o producto y versión (si aplica); y
- Precios y costos del cliente

OSE debe también dar al cliente oportunidad de:

- Revisar y aprobar la transacción; y
- Recibir una confirmación

8.4.4. OSE debe brindar información suficiente acerca de los productos y servicios disponibles en línea, para permitir a los clientes tomar decisiones informadas acerca de si los adquiere o no.

8.4.5. OSE debe revelar información referente al negocio, productos o servicios disponibles para ser comprados/contratados en línea por sus clientes para todas las transacciones.

8.5. Términos de Negocios

8.5.1. OSE y los socios de comercio electrónico deben publicar a los clientes sus términos de negocio. El uso de archivos de autoridades de

certificación y terceras partes confiables deben ser documentados de acuerdo con la Política de seguridad de la información de OSE.

OSE debe proveer los términos en los que se efectúa la transacción en línea, incluyendo pero no estando limitado a:

- Cualquier restricción o limitación impuesta a la venta de bienes o servicios;
- Mecanismos de pago fáciles de usar;
- Procedimientos y políticas de devolución de fondos;
- Términos y condiciones (por ej., garantías, limitaciones);
- Estándares de materiales, programas, honorarios, o cualquier información de esta naturaleza;
- Revelación de las reglas completas y términos para las competencias, concursos y otras promociones.
- Para transacciones y suscripciones en curso, la información acerca de la transacción aparecerá en el estado de cuenta, y puede ser accedida mediante mecanismos y procedimientos fáciles de entender, a efectos de efectuar la cancelación.

9. Cumplimiento.

9.1. Propósito y Alcance

Esta política define las acciones necesarias para mantener el cumplimiento con todas las regulaciones aplicables por ley.

Esta política se aplica para todos los funcionarios y Asociados de Negocio de OSE.

9.2. Declaración de la política

OSE debe cumplir con todas las regulaciones aplicables por ley. Esto incluye cualquier ley penal o civil, estatutaria, reguladora u obligaciones contractuales realizadas en nombre de OSE. Es esencial garantizar el cumplimiento de cualquier requerimiento de seguridad incorporado en estas leyes, incluyendo protección de datos privados personales, protección de la información propietaria así como los datos de clientes. Además el ambiente de seguridad y control está sujeto a revisiones periódicas y continuas.

9.3. Protección de datos y Privacidad de la información personal

La CPSI tendrá como uno de sus cometidos asegurar el cumplimiento de las regulaciones legales en lo referente a información personal.

9.4. Identificación de legislación aplicable

La Oficina Jurídica Notarial debe documentar y definir, todos los requerimientos regulatorios, legales, estatutarios, o contractuales.

9.5. Prevención del uso inapropiado de las instalaciones de procesamiento de información

Las instalaciones para procesamiento electrónico de información de OSE, son solamente para uso del negocio.

9.6. Licencias de Software

9.6.1. La compra y uso de software de terceras partes debe cumplir con acuerdos de licenciamiento. Estos acuerdos deben detallar restricciones de usuario específicas (por ej.: número de licencias a instalar permitidas, número de máquinas en las que se puede instalar el software, o el número de usuarios concurrentes permitidos por el software en un mismo momento).

9.6.2. GTI debe llevar a cabo revisiones periódicas del uso de software en cualquier dispositivo electrónico y servidores de OSE y/o autorizados

por OSE, para asegurar que todos los recursos informáticos cumplen con los acuerdos de licenciamiento. Todo el software que viole estos acuerdos deberá ser desinstalado inmediatamente. Las partes responsables por instalar y/o utilizar el software no autorizado, estarán sujetas a acciones correctivas por parte de GTI.

9.6.3. Se debe licenciar todo el shareware y los usuarios deben acatar estrictamente las leyes de derecho de autor y las restricciones detalladas por el fabricante del software.

9.7. Software de terceras partes

9.7.1. GTI debe aprobar todo el shareware y freeware utilizado en las computadoras de OSE a efectos de evitar que el software contenga códigos maliciosos, sea inseguro o ineficiente.

9.7.2. Así mismo el usuario será responsable de dar estricto cumplimiento a las obligaciones establecidas en la presente política.

9.8. Chequeo de cumplimiento técnico

9.8.1. Los sistemas operacionales se deben chequear frecuentemente para revisar su cumplimiento técnico. Esto incluye el cumplimiento de todas las tecnologías, hardware y software, con las medidas de implementación de seguridad detalladas en la política de seguridad de OSE y la documentación de control técnica.

10. Administración de Comunicaciones y Operaciones

10.1. Propósito y alcance

El propósito de esta política es reducir el riesgo de errores ocurridos durante el procesamiento de información, a través de los controles de operaciones de sistemas. Esta política aplica a todos los Funcionarios, Proveedores y Asociados de Negocio de OSE, especialmente aquellos en funciones operativas relativas a los sistemas de información.

10.2. Declaración de la política

La administración de las comunicaciones y las operaciones de recursos de información y sistemas, son esenciales para mantener un alto nivel de servicio para los usuarios de OSE. Además, los requerimientos de seguridad se deben desarrollar e implementar a efectos de mantener el control sobre las comunicaciones y operaciones.

Los procedimientos operativos y las responsabilidades para mantener los accesos adecuados, el control y la disponibilidad de los sistemas de información deben ser incluidos en todas las funciones operativas. Todas las comunicaciones e intercambios de información, dentro o fuera de OSE, deben asegurarse de una manera adecuada, en relación al valor del activo de información.

10.3. Administración de instalaciones externas

A efectos de prevenir exposiciones y riesgos de seguridad, se deben analizar todos los procesos operativos llevados a cabo por terceras partes, y desarrollar procedimientos. El análisis debe incluir, pero no limitarse a:

- patrocinio y aprobación por los líderes de las Gerencias y Unidades de similar jerarquía que corresponda
- determinación de si la información sensible de OSE va a ser procesada o publicada en instalaciones externas
- determinación de la existencia de controles de seguridad
- cumplimiento de las medidas de seguridad de OSE
- respuesta ante cualquier contingencia operativa y planes de continuidad del negocio
- respuesta y manejo de todos los incidentes de seguridad
- determinación del cumplimiento de estándares de contratos con terceras partes

10.4. Control de cambios operativos

10.4.1. Todos los cambios en las redes de computación de OSE que no sean de emergencia deben seguir los estándares de Gestión de cambios de la Organización.

10.4.2. Sólo GTI podrán realizar cambios de emergencia en los sistemas de OSE. Estos cambios se deben documentar y aprobar dentro de las 48 hs. de resuelto el problema.

10.5. Administración de incidentes de seguridad física y ambiental

10.5.1. Una vez que los incidentes han sido reportados a las partes apropiadas, el incidente debe ser escalado para su investigación. Para determinar la gravedad de los mismos, los incidentes de seguridad física y ambiental serán investigados y se identificarán según los niveles definidos. Los métodos y procedimientos de investigación serán escalados en función del nivel de alerta.

10.5.2. La Unidad de Seguridad y Vigilancia es responsable por la coordinación de la respuesta a los incidentes de Seguridad física y/o ambiental coordinando y reportando, de manera rápida, eficiente y confidencial.

10.5.3. Se debe mantener un listado de los registros de incidentes a efectos de documentar los requerimientos financieros y gastos asociados, así como también la experiencia obtenida para prevenir casos futuros y establecer controles estadísticos a ser usados por la Dirección.

10.5.4. La CPSI debe mantener en una base de datos los registros que contengan información referente a violaciones de las políticas de seguridad de la información de la organización, reportando las que corresponda.

10.6. Protección contra software malicioso

10.6.1. Responsabilidades generales

10.6.1.1. Está prohibido poseer o desarrollar por parte de los usuarios, virus u otro software malicioso. El no cumplimiento de esta política puede resultar en una acción disciplinaria.

10.6.1.2. Se deben escanear, antes de su ejecución y con la herramienta antivirus corporativo disponible, los archivos adjuntos de correos o archivos bajados de Internet. Se deben escanear antes de su utilización, los medios de almacenamiento externos que han estado fuera del control del usuario (ej. Discos externos, pen drive, etc.).

10.6.1.3. Sera responsabilidad del usuario los danos ocasionados en los activos de información de OSE por el uso, sin previa autorización correspondiente, de dispositivos externos de almacenamiento o módems inalámbricos.

10.7. Medidas generales

10.7.1. En todos los dispositivos informáticos utilizados en OSE, se debe tener activado algún antivirus aceptado por GTI, que debe ser actualizado según las mejores prácticas, de la misma forma el sistema operativo que se utilice debe mantenerse actualizado (Fixes, service packs, etc). Esta responsabilidad es de GTI cuando los dispositivos son propiedad del Organismo y del usuario final cuando los dispositivos son de su propiedad.

10.7.2. Los programas de detección deben instalarse y/o activarse en todos los sistemas como parte del proceso de inicio. Estos programas se actualizarán regularmente a efectos de detectar nuevos virus o software malicioso.

10.7.3. Los PCs deben ser escaneados en cada inicio de sesión, y el software antivirus debe estar residente a través de toda la sesión. En caso de equipos que se reporten infectados, debe procederse a su control y seguimiento de acuerdo al procedimiento establecido.

10.8. Respaldo de información

10.8.1. Cada Gerencia debe procurar que toda la información en los servidores de OSE relacionada a su negocio, sea respaldada de forma consistente a los lineamientos corporativos. Cada Gerencia debe trabajar con el personal de GTI de OSE para asegurar que se respalda toda la información y que la misma se encuentra disponible para ser restaurada en caso de emergencia.

10.8.2. Cada Gerencia debe tener documentadas las solicitudes de respaldo y recuperación, con las correspondientes confirmaciones de GTI.

10.8.3. Los datos de los sistemas de información son considerados como datos normales si la falta de disponibilidad de esa información afecta de forma mínima a los usuarios y proveedores. La información clasificada como normal se respaldará periódicamente, según lo determine el responsable de la misma.

10.8.4. Los datos de los sistemas de información son considerados como datos esenciales si la falta de disponibilidad de la información interrumpe el negocio y el impacto es adverso. La información clasificada como esencial debe respaldarse y almacenarse en un lugar adecuado y en un local remoto.

10.8.5. Los Administradores de la información deben desarrollar programas de rotación y retención de respaldos para cada aplicación que soportan, basados en los requerimientos establecidos por los responsables de la información.

10.8.6. Los usuarios deben respaldar los archivos importantes en servidores centrales, cuando sea posible, los cual se respaldan de forma programada. Los archivos o aplicaciones personales no deben respaldarse en los servidores de la red.

10.9. Manipulación y seguridad de medios

10.9.1. Desecho de información

10.9.2. Todos los funcionarios deben utilizar métodos de destrucción apropiados cuando se desecha información de OSE. El método de destrucción adecuado para papeles con información de carácter Reservado o Confidencial es destruirlos en máquinas destructoras de papel. Es responsabilidad del usuario asegurar que se utilizan los métodos de destrucción adecuados.

10.9.3. Los dispositivos de almacenamiento de información electrónica (discos duros, cintas, CDs, DVD's, Pen Drives, etc.) deben desecharse de forma acorde a la clasificación de la información almacenada en ellos. Todos los dispositivos de almacenamiento electrónico deben "limpiarse" electrónicamente por medio de una herramienta aprobada por GTI, antes de desecharse.

10.10. Procedimientos de manipulación de la información

10.10.1. La información de OSE debe generarse en papel, sólo si éste es necesario para completar operaciones de negocio normales. Las copias de información deben ser mínimas para facilitar el control y la distribución. Cuando la información de carácter Reservado o Confidencial impresa no esté en uso, debe almacenarse en cajones con llave, armarios o salas diseñadas específicamente para ese propósito, y que sólo sean accesibles por el personal autorizado.

10.10.2. El acceso físico a las bibliotecas de medios contenedores de información (por ej. discos) y documentación debe estar restringido a los funcionarios que requieran acceso por sus responsabilidades de trabajo. Debe revisarse periódicamente esta lista de accesos autorizados para asegurar que se encuentra actualizada.

10.10.3. Deben estar claramente identificados los receptores de los datos. Cualquier medio enviado a través del correo interno, externo, u otros medios, deben estar claramente etiquetados con los datos del receptor.

10.11. Manejo de medios de computación removibles

Todos los medios contenedores de información, incluyendo papeles y medios digitales, deben almacenarse de forma segura. Esto incluye medidas de seguridad física para prevenir robos, y controles ambientales para prevenir la degradación de los mismos. Todo medio informático que se saque de las instalaciones de OSE, debe estar autorizado por la gerencia correspondiente antes de salir de la organización. Si el contenido de los medios deja de ser requerido, debe borrarse antes de sacarlo del sitio.

10.12. Medidas generales de correo electrónico

10.12.1. Los sistemas de correo electrónico de la OSE no deben utilizarse para:

- enviar cadenas
- realizar propaganda política
- comprometerse en cualquier actividad ilegal, o reñidas con la moral y las buenas costumbres.
- realizar negocios que no sean relativos a OSE
- diseminar direcciones de correo interno a listas de correo externas.

10.12.2. Está prohibida la utilización de reglas de “re-envío automático” para enviar el correo electrónico del negocio de OSE a un servidor que no sea de OSE

10.13. Acuerdos de intercambio de información y software

10.13.1. Deben establecerse controles sobre el intercambio de información y software, para asegurar que:

- Se mantienen la confidencialidad e integridad de la información;
- La propiedad intelectual contenida en la información/software está protegida correctamente.

Para proteger la información, mientras ésta se encuentra fuera de las instalaciones seguras de OSE, se necesita considerar lo siguiente:

- Acuerdos de confidencialidad e intercambio de software;
- Seguridad de los medios en tránsito;
- Acceso a través de sistemas disponibles públicamente.

10.14. Otras formas de intercambio de información

10.14.1. Los funcionarios deben estar conscientes de los riesgos de divulgar información de carácter sensible en conversaciones u otras formas de comunicación. Esto incluye, pero no se limita a:

- No utilizar teléfonos inalámbricos o celulares para discutir información propietaria
- No discutir información sensible de OSE en lugares públicos
- No dejar información sensible en mensajes de voz.
- No transmitir información sensible a través de la red sin cifrarla.

11. Control de acceso

11.1. Propósito y alcance

Esta política define los requerimientos de control para acceder a los recursos vinculados al Sistema de Información de OSE. Esta política se aplica para los Funcionarios, Proveedores y Asociados de Negocio de OSE que acceden o administran el acceso a dichos recursos.

11.2. Declaración de la política

Los recursos vinculados al Sistema de Información de OSE son esenciales para el éxito de la organización. Por lo tanto, el acceso a todos los recursos de información será otorgado de manera controlada en base a los requerimientos de negocio. Se otorgarán explícitamente los accesos que correspondan a los Funcionarios, Proveedores y Asociados de Negocio de OSE.

No se otorgarán derechos de acceso por defecto.

El proceso para administrar el acceso a la información debe incluir, pero no limitarse a:

- documentación adecuada respecto a la administración y responsabilidades de todos los usuarios
- desarrollo e implementación de mecanismos de control de acceso
- realizar un seguimiento adecuado de los accesos exitosos e intentos fallidos y el uso de los recursos de información.
- Se deben desarrollar, implementar y mantener estos controles para prevenir que se comprometa la confidencialidad, disponibilidad e integridad de los recursos de información de OSE.

11.3. Requerimientos de negocio para el control de acceso

11.3.1. Política de control de acceso

11.3.1.1. Los usuarios deben obtener permisos del responsable de la información demostrando una causa de negocio justificada para acceder a los datos. La autorización debe estar documentada en el formulario de solicitud de acceso aprobada por el responsable de la información y/o el Jefe del Área a la cual pertenece el funcionario, o para la cual brinda el servicio. Este debe archivarse a efectos de mantener archivos históricos. Los responsables de la información

darán accesos en base a la “necesidad de conocer”, según se requiera por las funciones de trabajo esgrimidas por los solicitantes.

11.3.1.2. Las reglas de acceso deben estar documentadas explícitamente para los accesos opcionales u obligatorios. Si se utilizan perfiles, cada perfil debe incluir la documentación correspondiente.

11.3.1.3. Los controles de acceso deben establecer explícitamente las reglas y derechos de los usuarios. Todos los accesos de usuario se deben otorgar según los requerimientos del negocio. Los requerimientos de acceso deben asignarse y comunicarse a todas las personas involucradas. Todos los accesos deben ser consistentes con la clasificación de la información y los derechos, privilegios y tareas asignadas al usuario.

11.3.1.4. Cuando sea posible, el acceso del usuario debe estar incluido en un perfil basado en la descripción del trabajo, tareas o funciones. La utilización de perfiles ayuda en la administración del acceso de usuario y brinda consistencia a la tarea.

11.4. Gestión de acceso de usuarios

11.4.1. Registro de usuarios

11.4.1.1. Los procedimientos de alta y baja de usuarios deben incluir otorgar y cancelar los derechos de acceso a todos los sistemas y servicios de información que los usuarios requieran para desempeñar sus tareas.

Estos procedimientos deben documentarse e incluir, pero no limitarse a:

- la autorización adecuada de los responsables de la información para obtener el acceso a los sistemas y/o recursos de información;
- verificar y autorizar que los accesos otorgados son iguales a los solicitados;
- restringir y controlar la asignación y uso de privilegios
- brindar a los usuarios una política de uso aceptable y mantener una copia firmada de esa política archivada; y
- mantener un registro histórico de todos los usuarios.

11.4.2. Gestión de derechos y privilegios de las cuentas de usuarios

11.4.2.1. En caso de que los permisos de acceso a la información ya no sean necesarios, el responsable de la información debe notificar a

GTI. Es obligación del responsable de la información ver si los privilegios de acceso están alineados con el negocio y están asignados basados en la “necesidad de conocer” del mismo. Las listas de acceso se deben proporcionar en forma oportuna a los responsables de la administración de la información y GTI.

11.4.2.2. Una vez que un funcionario se desvincula de la Organización, cualquiera sea la causal, es responsabilidad del Área donde el funcionario prestaba servicio, revisar cualquier papel o archivo informático del funcionario. Si corresponde, el superior debe asignar un nuevo responsable de la información y desechar los registros que no son necesarios.

11.4.3. Administración de cuenta/contraseña de usuario

11.4.3.1. Las cuentas de usuario que no hayan sido accedidas por noventa días se inhabilitarán automáticamente.

11.4.3.2. Todos los accesos a sistemas informáticos que manejen información de Nivel pública o superior deben estar controlados por un método de autenticación que combine por lo menos usuario/contraseña.

11.4.3.3. El sistema forzará a los nuevos usuarios que acceden al sistema a cambiar la contraseña inicial por una que cumpla las recomendaciones de seguridad para el establecimiento de contraseñas.

11.4.3.4. Los usuarios deben ser forzados a cambiar las contraseñas periódicamente. Los Administradores de Sistemas deben forzar esto por medios automáticos estableciendo en el sistema la antigüedad de las contraseñas. Los usuarios no deben usar contraseñas cíclicas.

11.4.3.5. Los usuarios deben tener limitado el acceso a un único ID de usuario por sistema. Se deben seguir los estándares de nomenclatura de las cuentas de OSE para todos los sistemas.

11.4.3.6. El sistema no debe permitir que los usuarios tengan múltiples sesiones en el mismo sistema, a menos que el usuario esté autorizado.

11.4.4. Revisión de los derechos de acceso de los usuarios

11.4.4.1. Los responsables de la información deben revisar los privilegios de acceso otorgados periódicamente, y deben revocar todos aquellos que ya no son requeridos por los usuarios. Los Administradores de los sistemas son responsables de brindar reportes actualizados a los responsables de la información, y a GTI, en caso de ser solicitados, para revisar los accesos de los usuarios actuales.

11.4.4.2. Los derechos de acceso deben revisarse regularmente por los responsables de la información, para mantener un control de acceso efectivo.

11.5. Responsabilidades del usuario

11.5.1. Responsabilidades generales del usuario

11.5.1.1. Toda la actividad realizada bajo un ID de usuario es responsabilidad del funcionario asignado a ese ID de usuario. Por lo tanto, los usuarios no deben compartir sus cuentas con otros, o permitir a otros funcionarios utilizar sus cuentas. No se permite a los usuarios realizar actividades con un ID de usuario que no sea el propio.

11.5.1.2. Recomendaciones de seguridad en el uso de contraseñas de usuario

a) Los Administradores de Sistemas informáticos deben crear contraseñas iniciales que tengan un mínimo de ocho caracteres de largo y que contengan letras, números y caracteres especiales.

b) Siempre que el sistema lo permita, los usuarios de computadoras deben crear contraseñas de un largo mínimo de ocho caracteres que contengan letras, números y caracteres especiales.

c) El responsable de la información debe revisar por lo menos dos veces al año los derechos de acceso de los usuarios privilegiados para asegurar que el acceso a la información de OSE es apropiado.

d) Las contraseñas no deben poder asociarse fácilmente con la OSE o el usuario.

e) Las contraseñas nunca deben guardarse en textos visibles. Por lo tanto, los usuarios no deben poner nombres de usuario/contraseñas en scripts o archivos de texto, documentos de procesadores de texto o papel.

11.5.1.3. El ID del usuario debe estar explícitamente asignado a una persona. No están permitidas las cuentas compartidas ni de grupo. Las excepciones a esta medida deben estar aprobadas por GTI, como excepción a la Política.

11.6. Control de acceso a redes

11.6.1. Conectividad con redes externas

11.6.1.1. Todas las conexiones de red de OSE a Internet deben estar protegidas por firewalls filtrando el tráfico entrante para prevenir ingresos no autorizados a la red (WAN) de OSE. GTI debe aprobar todas las conexiones externas entrantes.

11.6.1.2. Todas las conexiones entre redes de OSE e Internet deben tener un Proxy. Sólo se permite a las conexiones salientes (que se originan desde dentro de las redes de OSE), salir a través de un firewall. Cierto tráfico entrante puede ser necesario para conexiones que se generan dentro de OSE debido a requerimientos técnicos. Estas conexiones deben justificarse por el servicio y deben estar aprobadas por GTI.

11.6.1.3. El esquema de numeración ip de la red interna de OSE no puede ser visible desde conexiones externas.

11.6.1.4. Para eliminar muchas de las vulnerabilidades inherentes a Internet con TCP/IP, routers, y firewalls no se deben aceptar conexiones externas que parezcan provenir de direcciones internas.

11.6.2. Medidas generales de acceso a redes

a) El acceso local a los recursos de información de OSE debe requerir como mínimo un ID de usuario único y una contraseña.

b) Los servidores con protocolos que permiten reenviar o re-rutear paquetes deben estar configurados para deshabilitar esta función. Por ejemplo, deben estar deshabilitadas las características “IP forwarding” y “passive” de FTP.

c) Para redes compartidas, especialmente las que se extienden más allá de los límites de la organización, debe restringirse la capacidad de conexión de los usuarios a la red, alineada con la política de control de acceso y los requisitos de las aplicaciones del negocio.

11.6.3. Políticas de uso se servicios de red

11.6.3.1. Todas las conexiones de red internas y externas deben cumplir con las políticas corporativas de uso de servicios de red y control de acceso. Por lo tanto, es responsabilidad de GTI determinar lo siguiente:

- Qué elementos de la red pueden ser accedidos;
- El procedimiento de autorización para obtener acceso; y
- Controles necesarios para proteger la red.

11.6.3.2. Debe controlarse el acceso físico y lógico a la configuración y diagnósticos de puertos.

11.6.3.3. Los servicios de red en los sistemas deben estar deshabilitados a menos que exista una razón de negocio específicamente documentada para tener el servicio. Los riesgos asociados con el servicio de red deben estar determinados y resueltos antes de la implementación del servicio.

11.6.4. Accesos remotos a redes

11.6.4.1. Los sistemas que brindan acceso remoto a los recursos de sistemas de OSE deben utilizar métodos más fuertes de autenticación. Para acceder, los usuarios remotos necesitarán un ID de usuario, una contraseña y otro método de autenticación.

11.6.4.2. No está permitido el acceso desde Internet hacia las redes de OSE sin algún mecanismo de autentificación, como mínimo considerar el uso de usuario y contraseña, para las aplicaciones que lo requieran, se deberá contar con un mecanismo de autenticación única (por ej. mecanismo de “token” one time password o una Smartcard).

11.6.4.3. El uso de módems no autorizados o soluciones de acceso remoto no aprobadas está prohibido y es una violación de la política de seguridad de OSE. Por lo tanto, no se pueden utilizar módems no autorizados o software de acceso remoto sin el consentimiento expreso por escrito de GTI.

11.6.5. Segregación de redes

11.6.5.1. No se permiten las conexiones irrestrictas a diferentes redes. Se debe implementar la separación de redes, dependiendo de las clases de información, para aumentar el nivel de seguridad durante el almacenamiento/transporte de información, incluyendo los puntos de acceso remoto. Cuando sea técnicamente posible, deben usarse arquitecturas de enrutamiento estrictas para limitar el acceso remoto a puntos específicos en la red.

11.6.5.2. Deben separarse en redes los grupos de servicios de información, usuarios y sistemas de información.

11.7. Control de acceso a sistemas operativos

11.7.1. Identificación y autenticación de usuarios

11.7.1.1. Los usuarios con accesos de super_usuarios o cuentas privilegiadas deben usar sus cuentas normales para ingresar a los sistemas. En caso de que estos requieran realizar tareas de administración, se cambiarán de la cuenta normal a la cuenta privilegiada.

11.7.1.2. Los usuarios que tienen accesos a líneas de comando de sistemas, deben estar limitados al acceso o servicio necesario. Esto puede incluir shells restringidos, restricción en los menús de aplicaciones, etc.

11.7.1.3. Todos los usuarios deben tener una única identificación de usuario. El uso de cuentas compartidas y “guest” (invitado), debe estar sujeto a autorización. Cada cuenta de usuario debe tener una clave asociada conocida solamente por el responsable. Se puede agregar seguridad adicional al proceso, por ejemplo, mediante el uso de tarjetas inteligentes o medidas biométricas.

11.7.2. Limitaciones en la conexión

11.7.2.1. Para ambientes de alta seguridad puede ser necesario limitar el inicio de sesión a terminales en ubicaciones específicas. En este caso, se deben asociar identificadores de dispositivos únicos con los puntos de conexión aprobados o conexiones directas a un servidor.

11.7.3. Sistemas de administración de contraseñas

11.7.3.1. GTI debe realizar pruebas aleatorias sobre las contraseñas cuando lo considere necesario, para asegurarse que se utilizan contraseñas adecuadas. Esto puede incluir el uso de herramientas de “cracking” de contraseñas. Este proceso se controlará de manera estricta y estará sujeto a supervisión de la CPSI para que sea realizado con las debidas garantías respecto a la privacidad de la información de los usuarios.

11.7.3.2. Todas las computadoras, bases de datos, o aplicaciones que almacenan información de cuentas de usuarios y contraseñas deben asegurarse. Se debe restringir y revisar periódicamente el acceso a la base de datos de cuentas de usuarios, solamente a los administradores autorizados.

11.7.4. Inactividad de sistemas

11.7.4.1. Las sesiones de sistemas que estén inactivas por diez minutos, se deben desconectar automáticamente. En los sistemas en los que las conexiones no se puedan terminar automáticamente, se deben activar protectores de pantalla con contraseñas, o bloqueo de terminales. Los usuarios no deben deshabilitar estos controles.

11.7.4.2. Los PCs/notebooks/Smartphones y servidores se deben configurar con un protector de pantalla protegido con contraseña. El protector de pantalla debe requerir el ingreso de una contraseña luego de que el equipo haya estado inactivo.

11.7.5. Medidas de seguridad de ingreso al sistema

11.7.5.1. Luego de tres fallas de autenticación consecutivas, los usuarios se bloquearán en el sistema al cual intentan acceder y su cuenta se restablecerá sólo manualmente.

11.7.5.2. Antes de ingresar a una sesión de trabajo, se desplegará a los usuarios un anuncio de ingreso.

11.7.5.3. En cada ingreso a una sesión de trabajo en sistemas sensibles de OSE, se debe incluir un aviso especial indicando:

- el sistema solo podrá ser utilizado por usuarios autorizados
- si se continúa con el uso del sistema, significa que el usuario está autorizado

- el uso del sistema implica el conocimiento por parte del usuario que las actividades realizadas podrán ser registradas (logs).

11.7.5.4. La identificación de la compañía, red, ubicación o servidor, no deben aparecer antes de un ingreso exitoso.

11.7.5.5. Los sistemas se deben configurar a efectos de no dar información ante un ingreso fallido. Esto incluye la identificación de qué parte de los datos de la secuencia de ingreso (usuario o contraseña) fue incorrecto.

11.7.6. Uso de utilitarios del sistema

11.7.6.1. Cualquier utilitario que permita a los Administradores de Sistema llevar a cabo tareas de mantenimiento en un sistema debe:

- Estar almacenado fuera de línea si no se necesita diariamente;
- Dar acceso restringido a un grupo limitado de usuarios autorizados;
- Incluir facilidades para registrar su uso.

11.8. Control de acceso a la información y a las aplicaciones

11.8.1. Restricción de acceso a la información

11.8.1.1. Se debe dar a los usuarios el nivel mínimo de accesos requerido para llevar a cabo sus tareas. Esto será logrado utilizando una combinación de:

- Seguridad lógica dentro de una aplicación
- Limitación de la disponibilidad de opciones no autorizadas
- Restricción del acceso a líneas de comando
- Restricción del contenido y funcionalidad de la aplicación
- Limitación de permisos sobre archivos, por ej. sólo lectura
- Control de distribución de salida

11.8.2. Aislamiento de sistemas sensibles

Basados en la clasificación de la información, las redes pueden requerir cierta segregación. Cuando la información procesada es sensible, el sistema debe estar físicamente segregado y no tener conexión directa con otras redes o sistemas que tengan datos menos críticos.

11.9. Seguimiento de acceso a sistemas y uso

11.9.1. Sincronización de relojes

Se deben sincronizar los relojes de los sistemas bajo un estándar acordado, para asegurar la exactitud de los registros de auditoria. Se debe implementar un procedimiento para asegurar que cualquier variación sea corregida.

11.9.2. Responsabilidades Generales

Los Administradores de sistemas deben realizar el seguimiento de los sistemas, como parte de su rutina de trabajo. Esto incluye pero no está limitado a, verificar el correcto uso, procesamiento, accesos de usuarios y servicios generales de sistemas. Pueden utilizarse herramientas automáticas en el caso que éstas hayan sido probadas extensivamente y sean aceptadas por GTI.

11.9.3. Registros de eventos de sistema

11.9.3.1. Todos los eventos de seguridad relevantes en cualquier sistema que maneje información de carácter Reservado o Confidencial se deben registrar, incluyendo pero no limitándose a:

- inicios fallidos,
- modificación de datos,
- uso de cuentas privilegiadas,
- cambios a los modelos de acceso o permisos de archivos,
- modificación de software instalado o sistema operativo,
- cambios a los permisos de usuarios o privilegios de cualquier función del sistema.

11.9.3.2. Se deben en retener los registros de seguridad por un mínimo de seis meses. El acceso a estos registros durante este tiempo solo debe darse a las personas autorizadas. Los registros deben ser retenidos como de sólo lectura.

11.10. Acceso móviles y redes de telecomunicaciones

11.10.1. Responsabilidades Generales

Los usuarios que trabajan con información de OSE desde sus casas o ubicaciones remotas, deben comprender las amenazas adicionales de seguridad que existen en dichos ambientes y tomar las medidas apropiadas para garantizar la seguridad de la información de OSE.

11.10.2. Medidas Generales

Todas las políticas de OSE aplicables a las operaciones realizadas en las oficinas de OSE, aplican también a las operaciones realizadas desde ubicaciones remotas.

11.10.3. Acceso remoto

Se deben implementar medidas adicionales de seguridad para proteger los datos mantenidos o accedidos vía dispositivos remotos, por .ej. notebooks o dispositivos de comunicación remotos. Todos los dispositivos móviles (ej. Notebooks) deben incluir:

- Cifrado de los datos almacenados (cuando sea necesario)
- Claves de encendido
- Dispositivos de aseguramiento físico para equipamientos móviles
- Protección de los datos durante la conexión y transmisión (por ej. VPN, SSL)
- Controles adicionales de autenticación lógica para obtener acceso a redes (Por ej. Uso de tokens de autenticación robusta)
- Adicionalmente, los usuarios remotos o móviles deben ser capacitados específicamente en las medidas de seguridad a ser tomadas en los accesos remotos.

Los usuarios deben usar las computadoras de OSE para acceder o conectarse a las redes de OSE. Solo aquellos usuarios que cuenten con la debida autorización, los elementos de seguridad necesarios y cumplan con los requisitos de seguridad para un acceso remoto seguro, podrán acceder o conectarse a las redes de OSE en forma remota desde computadoras ajenas a OSE.

Sólo los usuarios que tengan una causa de negocio justificada para acceder remotamente, serán autorizados a tener dicho acceso por el Responsable de la información en coordinación con GTI.

12. Excepciones a la Política

12.1. Propósito y alcance

Esta política define los procedimientos que seguirá el personal para identificar cualquier excepción a las políticas que pueda ocurrir para cumplir con los objetivos de negocio exitosamente. Define la documentación que debe completarse así como las aprobaciones que deben realizarse antes de permitir cualquier excepción a la política de Seguridad.

12.2. Excepciones a la declaración de la política

En los casos donde exista una necesidad de negocio justificable de realizar acciones que estén en conflicto con las medidas establecidas en la política de Seguridad de OSE, la CPSI deberá realizar las consideraciones necesarias.

Se pueden registrar excepciones para facilitar nuevos negocios de OSE, o las que estén dirigidas a áreas donde los cambios tecnológicos no están cubiertos por las políticas actuales. Sin embargo, es responsabilidad la CPSI entender y mitigar los riesgos.

12.3. Procedimientos para solicitar excepciones a las políticas

12.3.1. Lineamientos

12.3.1.1. Las solicitudes de excepciones a las políticas deben estar justificadas por un caso de negocio documentado, y deben tener las aprobaciones necesarias para considerarse válidas. Las excepciones deben estar aprobadas y firmadas por el responsable de la información involucrada, su Superior y por la CPSI. Una vez aprobadas, las excepciones a la política serán válidas, como máximo, por el período de un año al cabo del cual la excepción debe re-evaluarse y re-aprobarse.

12.3.1.2. Si las excepciones a la política evaden los controles internos existentes, se deben implementar y hacer el seguimiento de controles mitigantes o compensatorios. La CPSI debe estar involucrada en todas las instancias donde se pasen por alto los controles de seguridad interna.