

**POLÍTICA SEGURIDAD FISICA
SISTESEG
BOGOTÁ
COLOMBIA**

Política Seguridad Física [BS 7799 Control A.7.1]

1.1 Audiencia

Esta política aplicará a todo el personal vinculado laboralmente con SISTESEG contratistas y terceros que tengan acceso a los recursos de información de la organización.

1.2 Introducción

La seguridad física identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al mantenimiento y procesamiento de la información, como por ejemplo activos de información, activos de software y activos físicos.

Se entiende por área donde se procesa la información los siguientes:

- Centros de Procesamiento normales o de emergencia
- Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación
- Áreas donde se almacenen formas continuas, membretadas, facturas sean propias de SISTESEG o procedentes de clientes o de otras de áreas.
- Áreas donde se encuentren concentrados dispositivos de información
- Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos Duros, Cintas etc.)
- Áreas donde se deposite salidas de impresoras o fax.

1.3 Definiciones

Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales.

Activos físicos: Se consideran activos físicos elementos tales como: Computadores, laptops, modems, impresoras, maquinas de fax, Equipos de Comunicaciones, PBX, cintas, discos, UPS, muebles etc.

1.4 Objetivo

Prevenir el acceso físico no autorizado, además de evitar daños o robo a los activos de la organización e interrupciones a las actividades del negocio de SISTESEG.

1.5 Enunciado de la Política

"Toda área o equipo informático, debe cumplir con todas las políticas funcionales y procedimientos de seguridad física, con el fin de evitar el acceso por personas no autorizadas, daño e interferencia a los recursos e infraestructura de información".

1.6 Elementos adicionales a la política general

Aspectos de la seguridad física a ser considerados en la definición de las políticas funcionales:

- Equipos de control del medio ambiente
- Almacenamiento de cintas de respaldo.
- Seguridad de las oficinas, salones y facilidades
- Reglas sobre el trabajo en áreas seguras
- Cableado, UPS, impresoras y Modems
- Seguridad de los equipos
- Control de los sistemas de potencia
 - Múltiples sistemas de alimentación
 - Sistemas de control de potencia (UPS)
 - Generadores de back up

1.7 Políticas relacionadas

Política de Control de Acceso
Política de Continuidad del Negocio.

1.8 Roles y responsabilidades

Esta política es responsabilidad de ser aprobada por las directivas de SISTESEG, con el fin de garantizar la continuidad del negocio en caso de un evento que afecte la operación normal de SISTESEG.

1.9 Violaciones a la política

Violaciones de la política de Seguridad Física, pueden resultar en acciones de tipo disciplinario, que pueden incluir, más no estar limitadas a:

- Acción de tipo disciplinario según los lineamientos establecidos por el Código Sustantivo del Trabajo, el Reglamento Interno de Trabajo, el Código de Comportamiento Empresarial SISTESEG, las Cláusulas Especiales que se establezcan con los empleados en sus Contratos Laborales y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias patronales.
- Reprimenda formal
- Suspensión o acceso restringido a las áreas de procesamiento de la información
- Reembolso por algún daño causado
- Suspensión sin pago de salario
- Terminación del contrato de trabajo o relación comercial (Basados en las disposiciones emitidas por las leyes colombianas en materia laboral).
- Demanda civil o penal

1.10 Revisión de la política

Esta política debe ser modificada si existieran cambios en la infraestructura física de SISTESEG, de no haber cambios, se debe realizar su revisión anualmente.

1.11 Referencias

N/A

1.12 Aspectos específicos sobre la política de Seguridad Física.

1.12.1 SEGURIDAD EN EL PERIMETRO FISICO (BS 7799-2 Control A 7.1.1)

El sitio escogido para colocar los sistemas de información, equipos de computo y comunicaciones, deben estar protegidos por barreras y controles físicos, para evitar intrusión física, inundaciones, y otro tipo de amenazas que afecten su normal operación.

1.12.1.1 Recomendaciones y controles adicionales

El tamaño del área será determinado por la cantidad de hardware necesitado para el procesamiento y almacenamiento de la información. Los requerimientos de tipo ambiental deben ser especificados por los diferentes fabricantes de los equipos. Las medidas de seguridad que se deban tomar, dependerán directamente del valor de los activos de información, su nivel de confidencialidad, y los valores requeridos de disponibilidad.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- El perímetro de seguridad debe ser claramente definido.
- El sitio donde es ubiqüen los recursos informáticos debe ser físicamente sólido, y protegido de accesos no autorizados factores naturales, usando mecanismos de control, barreras físicas, alarmas, barras metálicas etc.
- Debe existir un área de recepción que solo permita la entrada de personal autorizado.
- Todas las salidas de emergencia en el perímetro de seguridad deben tener alarmas sonoras y cierre automático.
- Comentario interno: Cumplimos con estas condiciones y aquellas donde se necesite inversión hasta donde vamos a hacer?

1.12.2 CONTROL DE ACCESO FISICO A AREAS SEGURAS (BS 7799-2 Control A 7.1.2-7.1.3)

Todos los sitios en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas.

- Comentario interno: Cumplimos con estas condiciones y aquellas donde se necesite inversión hasta donde vamos a hacer?

Se recomienda además tener separados físicamente la operación de terceros con las propias, en caso de existir actividades de terceros en SISTESEG, se deben establecer controles por la persona responsable en SISTESEG del Outsourcing.

1.12.2.1 Recomendaciones y controles Adicionales

Debido al posible robo, vandalismo y uso no autorizado de los sistemas de información, se debe considerar restringir el acceso de personas a las áreas consideradas seguras, según lo definido por SISTESEG.

Todo sistema de control de acceso debe considerar diferentes categorías de personal:

- 1) Operadores y usuarios que trabajan regularmente en las áreas seguras.
- 2) Personal de soporte que requiera acceso periódico.
- 3) Otros, que requieran acceder muy rara vez.

Aspectos de la seguridad de la información a ser considerados cuando se implementa la política de seguridad física son:

- Personal no autorizado puede llegar a tener acceso a las áreas restringidas, causando posibles fallas al sistema.
 - Personal de SISTESEG, visitantes o terceras personas, que ingresen a un área definida como segura por SISTESEG, deberán poseer una identificación a la vista que claramente los identifique como tal y estas identificaciones serán intransferibles. Se debe además hacer una revisión periódica de identificadores de acceso; una formal realizada con auditoría, al menos una vez al año, y las diferentes divisiones internamente realizarlas cada 3 meses.
 - No deberán existir señales, ni indicaciones de ningún tipo sobre la ubicación de los centros de procesamiento en la organización.
 - En caso de pérdidas de llaves, deberán existir procedimientos que garanticen que las mismas no podrán ser utilizadas por extraños.
- Equipos como fax, fotocopiadoras, impresoras deben estar en áreas definidas por SISTESEG como seguras, esto aplica también para equipos de comunicaciones como Switches, Enrutadores, firewalls, IDS, Concentradores VPN etc.
- Las puertas y ventanas deben estar cerradas, en caso de ser el primer piso se deben considerar controles adicionales.

1.12.3 USO DE MAQUINAS FAX O MODEMS (BS 7799-2 Control A 7.1.3)

La información sensible o confidencial solo puede ser enviada vía Fax o Modems cuando no existan otros medios que confieran una mejor seguridad, ambos el dueño y el receptor deben autorizar la transmisión de antemano.

Esta política considera las amenazas asociadas con el uso de maquinas de fax. El riesgo proviene principalmente de la relativa inseguridad del medio, dado que información confidencial puede ser revelada a personas no autorizadas.

1.12.4 USO DE IMPRESORAS (BS 7799-2 Control A 7.1.3)

La información clasificada como altamente confidencial no debe ser nunca enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión.

La variedad de la información que se envía a las impresoras puede alternar entre información pública e información confidencial, dado que información confidencial puede ser revelada a personas no autorizadas.

1.12.5 PRESENCIA DE EXTRAÑOS EN LAS INSTALACIONES (BS 7799-2 Control A 7.1.4)

Todos los empleados deben estar vigilantes a la presencia de personas extrañas sin identificación visible dentro de las instalaciones de SISTESEG y en ese caso reportar inmediatamente a seguridad.

Entre los controles adicionales tenemos:

- Todos los visitantes o extraños deben ser acompañados durante su estadía en SISTESEG, debido a la existencia de información confidencial o hurto.
- Equipos como videograbadoras, cámaras fotográficas, grabadoras, sniffers, analizadores de datos, (ej: hardware especial) etc, no debe ser permitidos su uso dentro de las instalaciones de SISTESEG a menos que exista una autorización formal por el oficial de seguridad o personal de seguridad del edificio.

1.12.6 AREAS DE DESCARGUE (BS 7799-2 Control A 7.1.5)

La carga y descarga de materiales en SISTESEG requerirá de un primer control (inspección rigurosa por seguridad) en recepción y luego de su respectiva autorización para ingresar, se entregará en el sitio respectivo. También debe ser cuidadosamente controlado su ingreso, y aislado de los centros de procesamiento de información.

Los siguientes controles deben ser considerados:

- Todo elemento que ingrese a SISTESEG, debe ser inspeccionado por la compañía de seguridad rigurosamente con el fin de identificar material peligroso y que coincida con su respectiva autorización de ingreso.
- Las áreas de descargue deben estar debidamente identificadas para evitar el acceso a las instalaciones por parte de terceros.
- Los materiales que deban entrar a SISTESEG deben ser inspeccionados debidamente en la zona de descargue, para evitar la entrada de elementos peligrosos a las áreas internas.
- El material entrante o saliente debe ser registrado, con el fin de mantener el listado de inventario actualizado.

1.12.7 SEGURIDAD DE LOS EQUIPOS (BS 7799-2 Control A 7.2)

En lo referente a la ubicación de computadores y hardware en general, se debe tener especial cuidado contra fallas del sistema de control del medio ambiente, y otras amenazas que puedan afectar la normal operación del sistema.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- Fallas en el control de la temperatura o humedad pueden afectar la operación del negocio, así que, se debe tener un estricto monitoreo sobre estas variables.
- Se deben adoptar o mantener al día, controles para minimizar el riesgo potencial de:
 - Robo

- Todos los visitantes o terceras personas, que ingresen a las instalaciones de SISTESEG deberán poseer una identificación a la vista que claramente los identifique como tal.
 - Fuego
 - En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses (cuanto tiempo se recomienda?) y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control del Manual de Seguridad Física.
 - Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.
 - Explosivos
 - Todos los visitantes o terceras personas, que ingresen a un área de procesamiento deberán poseer una identificación a la vista que claramente los identifique como tal, y por ninguna razón se debe tener material explosivo dentro, o en sitio cercano a áreas definidas como seguras por SISTESEG. (Por ejemplo químicos especiales, pólvora o gases explosivos)
 - Humo
 - En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo conato de incendio.
 - Inundación o falta de suministro
 - Las salas de procesamiento de la información deberán estar ubicadas en pisos a una altura superior al nivel de la calle a fin de evitar inundaciones.
 - Las cañerías de desagüe de dichas salas y ubicadas en el piso, deberán poseer válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación ante sobre-flujos
 - Interferencia Eléctrica y/o Radiación electromagnética.
 - El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
 - Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimento.
- El uso de elementos adicionales de protección (Contra Polvo o radiación) para los equipos informáticos debe ser considerado en ambientes de tipo industrial.
- Los equipos deben ser protegidos de fallas de potencia u otras anomalías de tipo eléctrico. Los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes de los equipos. Entre los controles adicionales tenemos:

- El correcto uso de UPS (Uninterruptable power supply), las cuales se deben probar según las recomendaciones del fabricante, de tal forma que garanticen el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.
- El Generador debe ser regularmente probado de acuerdo a las recomendaciones del fabricante, o por lo menos una vez al año.
- Se deben tener interruptores eléctricos adicionales, localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en caso de una falla o contingencia. Las luces de emergencia deben funcionar en caso de fallas en la potencia eléctrica.

1.12.8 INSTALACION Y MANTENIMIENTO DEL CABLEADO (BS 7799-2 Control A 7.2.3)

El cableado de la red debe ser instalado y mantenido por ingenieros calificados con el fin de garantizar su integridad. Conectores de pared no utilizados deben ser sellados y su estado debe ser formalmente notificado.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- Un daño malicioso a la red puede causar un grave disturbio a los sistemas de procesamiento y comunicaciones.
- Una incursión ilegal puede comprometer la seguridad de los datos, nombres y contraseñas.
- Las conexiones de potencia deben tener su respectivo polo a tierra.
- El cableado de la red debe ser protegido de interceptación o daño, por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de acuerdo a las normas técnicas, de los de comunicaciones.
- Para el caso de conexiones muy críticas (Transporte de mucha información o aplicaciones especiales) se debe considerar el uso de fibra óptica.
- Considerar el uso de enlaces redundantes.

1.12.9 MANTENIMIENTO DE LOS EQUIPOS (BS 7799-2 Control A 7.2.4)

Se deberán realizar mantenimientos sobre los equipos de acuerdo a las recomendaciones del fabricante y ser realizados únicamente por personal autorizado, considerando el hecho que si se tuviera que enviar fuera de las instalaciones, se debe tener en cuenta la información sensible y los requerimientos de las pólizas de aseguramiento.

1.12.10 EQUIPOS FUERA DE LAS INSTALACIONES (BS 7799-2 Control A 7.2.5)

El uso de equipos de procesamiento de la información o software, fuera de las instalaciones de SISTESEG, debe ser autorizado por el jefe o director del área donde el empleado dependa. Esto aplica para Computadores personales, Agendas electrónicas, teléfonos móviles, etc.

Las siguientes recomendaciones deben ser consideradas:

- No dejar los equipos desatendidos en zonas publicas. Los computadores personales deben evitar su apariencia y ser llevados como equipaje de mano.
- Las especificaciones del fabricante deben ser consideradas.
- El trabajo remoto debe estar sujeto a controles especiales, considerando las recomendaciones aplicadas cuando su uso es de tipo interno.
- Se debe considerar el uso de seguros contra robo, perdida etc.

1.12.11 DESTRUCCION DE EQUIPOS Y RE-USO (BS 7799-2 Control A 7.2.6)

Los equipos de almacenamiento de información deben ser destruidos físicamente o escritos de manera segura a través del uso de herramientas especiales que garanticen y verifiquen que no quede información remanente, evitando además el uso de comandos de borrado usados en su operación normal.

1.12.12 POLITICA DE ESCRITORIOS Y PANTALLA LIMPIA (BS 7799-2 Control A 7.3)

SISTESEG debe adoptar una política de escritorios limpios para papeles, y medios de información, junto con una política de pantalla limpia, con el fin de reducir los riesgos por pérdida, daño a la información durante o fuera de las horas de trabajo.

Los siguientes controles deben ser considerados:

- Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.
- Información confidencial y crítica para la organización debe ser asegurada preferiblemente en armarios resistentes a impacto, fuego e inundación. Los computadores personales no se deben dejar dentro de sesión, se recomienda el uso de llaves físicas, contraseñas, y otro tipo de controles cuando no estén en uso.
- Puntos de envío y recepción del correo, Maquinas de fax, deben ser protegidos de acceso no autorizado.
- Las fotocopiadoras deben estar protegidas de uso no autorizado.