
digilogics

A.11 Seguridad física y ambiental (POL-07)

1. Objetivo

Preservar la seguridad de las instalaciones de procesamiento de la información de DIGILOGICS, ofreciendo dirección a las acciones para la prevención de los incidentes relacionados con el acceso físico no autorizado o la mala gestión de los activos de información durante su posicionamiento y manejo dentro o fuera de las instalaciones de la Organización.

2. Alcance

Es de aplicación general y su carácter es obligatorio, por lo que debe ser cumplida y respetada tanto por el personal interno de DIGILOGICS como por el externo que sea contratado o subcontratado.

3. Términos y Definiciones

- **CCTV:** se refiere al Circuito cerrado de televisión o CCTV (en inglés Closed Circuit Television) es una tecnología de video vigilancia diseñada para supervisar una diversidad de ambientes y actividades.
- **UPS:** Sistema de alimentación ininterrumpida (SAI), en inglés Uninterruptible Power Supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

4. Política

A.7.1 Perímetro de seguridad física

- DIGILOGICS cuenta con perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado para el correcto funcionamiento de los sistemas de información.
- Los perímetros de seguridad física incluyen sin ser limitativos: paredes, módulos de recepción, dispositivos de acceso controlados por biométricos y cerraduras de llave, estos mecanismos de acceso son utilizados para la protección de la información y los activos informáticos más sensibles e importantes para DIGILOGICS.
- Las áreas seguras están protegidas por mecanismos que garanticen la entrada exclusivamente al personal autorizado, obedeciendo lo establecido en el documento ***Control de Acceso de áreas seguras,*** donde se establece el área a que tiene acceso cada colaborador, este documento es gestionado por el Administrador Técnico de Seguridad de la Información

A.7.2 Controles físicos de entrada

- Para los controles físicos de entradas se consideran sin ser limitativo:

    a) Guardar registro de la fecha, hora de entrada y salida de las instalaciones de proveedores y visitantes, la evidencia de esta acción queda registrada en el ***Control de acceso de visitantes.***
    b) Todos los colaboradores deben registrar su entrada y salida en los mecanismos definidos por la organización (biométricos, bitácoras, etc.)
    c) Todos los terceros visitantes deben identificarse a través del gafete correspondiente, este gafete es proporcionado por el responsable de recepción.

d) Los terceros visitantes deben permanecer exclusivamente en área de visita asignada y escoltados siempre por la persona anfitrión.

- Todo colaborador o visitante que requiera ingresar con equipo de cómputo o herramienta ajena a la organización deberá registrarlo en la bitácora de ***Control de acceso equipo y herramienta***.
- Para las áreas de carga y descarga:
    a) Las zonas deben estar delimitadas.
    b) No se debe permitir el acceso a proveedores sin previa autorización de un representante de DIGILOGICS mismos que deberán de recibir al proveedor y asegurarse que:
        - Sea el personal identificado y autorizado por parte del proveedor y registrar su entrada y salida en las bitácoras correspondientes ***Control de acceso de visitantes.***
        - Validar que la cantidad de los insumos es la correcta, características y empaque acordado y que el proveedor presente la documentación necesaria dependiendo del tipo de entrega.
        - Cuando se trate de salida de mercancía deberá ser registrada en el formato ***Pase de Salida.***

A.7.3 Aseguramiento de oficinas, salas e instalaciones

- Se debe restringir el acceso a personal no autorizado a los documentos físicos que revelen información Confidencial y/o Restringida, esto mediante su clasificación y resguardo en archiveros cerrados y bajo llave dependiendo de su nivel de clasificación, incluyendo una identificación física de acuerdo a lo que ordena el documento **A.8 Gestión de Activos (POL-04)**, en relación al resguardo y etiquetado de los activos de información.

A.7.4 Supervisión de la seguridad física

- El CCTV registra los accesos y salidas de los colaboradores y es monitoreado por el área de administración; el CCTV respalda 7 días de grabación.
- Administrador debe reportar cualquier incidente siguiendo lo establecido en la política **A.16 Gestión de incidentes de seguridad de la información (POL-11)**.

A.7.5 Protección contra amenazas físicas y ambientales

- Se cuenta con un programa de protección civil donde se establece las actividades mínimas para la actuación en caso de desastres.
- En caso de desastres naturales y contingencias se debe observar el **Plan de Continuidad del negocio.**

A.7.6 Trabajo en áreas seguras

- El trabajo dentro de las instalaciones se debe apegar a mecanismos de seguridad de la información; en un área segura se deberá seguir los siguientes lineamientos:

    a) Los visitantes deben estar siempre escoltados por un representante de DIGILOGICS.
    b) Los proveedores con acceso autorizado para mantenimiento u otro tipo de actividades, deben estar perfectamente controlados por los responsables del acceso

físico, los proveedores se deben registrar en la bitácora correspondiente y describir los motivos de su visita.

c) Al finalizar el horario laboral el vigilante realizará un recorrido por las instalaciones para verificar que todas las puertas han sido cerradas.
d) Las áreas seguras no deben emplearse como almacenes.
e) Los colaboradores deberán asegurarse al final de su horario laboral no dejar a la vista información considerada confidencial o restringida.
f) Las áreas que se encuentren vacantes deben cerrarse con llave, en la medida de lo posible, e inspeccionarse periódicamente.

A.7.7 Escritorio y pantalla despejados

- El equipo desatendido debe ser bloqueado o en su defecto debe tener activado el bloqueo automático del equipo, el tiempo de bloqueo debe quedar configurado con un máximo de 1 minuto.
- No se deben dejar a la vista del público documentos impresos que revelen información confidencial y/o restringida esto incluye notas, pegatinas, cuadernos, agendas, entre otros que revelen en su contenido este tipo de información.
- Los colaboradores deben aplicar reglas de pantalla y escritorio limpio en las áreas de trabajo, la pantalla de escritorio no debe observarse iconos que revelen o mantengan acceso directo a información confidencial y/o restringida.

A.7.8 Ubicación y protección del equipo

- El acceso al área del servidor se encuentra controlado mediante la ***Bitácora de acceso al servidor.***
- Se debe evitar comer en las áreas donde se procese información, solo se permitirán bebidas que estén contenidas en recipientes con tapas.
- En caso de reubicación física o instalación de equipos nuevos es necesario considerar:
    a) Instalar los equipos en sitios donde se minimicen los accesos innecesarios.
    b) Los equipos destinados para el almacenamiento de Información sensible no se deben colocar donde se corra el riesgo de que personal no autorizado tenga acceso.
    c) Los activos que requieran condiciones especiales deben aislarse del resto y mantener el acceso restringido.
    d) Se deben tomar las medidas adecuadas e implementarse los controles necesarios para minimizar los riesgos de daño de los activos causados por robo, incendio, agua, fallas en suministros de energía, vandalismo, daños con químicos, etc.
    e) Se debe mantener controlado el ambiente (temperatura y humedad) de acuerdo a las especificaciones del proveedor a fin de evitar que estos factores dañen los activos.

A.7.9 Seguridad de los equipos y activos fuera de las instalaciones

- En caso de que por necesidad del trabajo o suceso inesperado sea indispensable sacar equipos de las instalaciones se deberán seguir las siguientes indicaciones:
    - ✓ Dar aviso al administrador de la salida del equipo.
    - ✓ Dejar evidencia de su salida mediante el formato ***Pase de Salida.***
    - ✓ No dejar el equipo desatendido en lugares públicos o en lugares donde pueda ser sustraído o dañado con relativa facilidad, como autos, maletas de viaje, cerca de ventanas, en el piso, mesas de comida o bebida, etc.

- ✓ En la manera de lo posible cumplir con los elementos de seguridad que son aplicables en una oficina, esto significa tener un entorno seguro de trabajo libre de perturbación eléctrica, exposición a cableado, superficies sucias, derrames de alimento y líquidos, etc.
- ✓ Ser responsable del equipo asignado por la compañía cuando se utiliza en una ubicación de trabajo externa. El colaborador es responsable del costo de reparación o reemplazo de cualquier equipo si es manejado inadecuadamente.
- ✓ Los colaboradores que saquen los equipos de las instalaciones deben conocer y respetar las especificaciones y cuidados a fin de evitar daños al equipo.

A.7.10 Medios de almacenamiento

- Bajo ninguna circunstancia se dejará sin vigilancia o seguridad los medios de almacenamiento o copias de seguridad de los sistemas de información.
- Todo medio de almacenamiento deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la red de la empresa.
- Se prohíbe el uso de medios almacenamiento en lugares de acceso al público que contengan información reservada o confidencial de la empresa.
- El uso de medios de almacenamiento para transferencia de información debe responder a una necesidad del negocio y se hará única y exclusivamente a través de los entregados por la empresa de acuerdo a los siguientes pasos:
  1.- Solicitarlo a través de correo electrónico al administrador (gustavo.munoz@digilogics.com.mx), indicando el motivo de su uso.
  2.- El administrador elaborará el ***Resguardo*** respectivo para su entrega.
  3.- El administrador actualizará el **control del Inventario de Activo**
- Todo dispositivo de almacenamiento removible en uso debe guardarse en un ambiente seguro acorde al tipo y sensibilidad de la información contenida

A.7.11 Servicios de apoyo

- Las instalaciones de apoyo (eléctricas, suministros de agua, etc.) deben ser revisados periódicamente para comprobar su correcto funcionamiento, esto de acuerdo al ***programa de mantenimiento.***
- Se cuenta con UPS, que protegen los equipos de cómputo contra variaciones de voltaje, fallas en el suministro de energía y anomalías.
- El uso de los UPS quedará sujeto a prioridades y presupuestos autorizados, y al nivel de riesgo de cada equipo, mismo que deben revisarse periódicamente para garantizar su funcionamiento adecuado.
- Se cuenta con un interruptor de energía eléctrica de emergencia cerca de la salida para facilitar la desconexión de los equipos en caso de emergencia, el área de administración debe gestionar su correcto funcionamiento.
- Los equipos de telecomunicación deben contar con conexiones redundantes y ser probados continuamente por el Administrador Técnico de Seguridad para garantizar que la operación no será interrumpida por fallas en este servicio.
- Las instalaciones generales (inmueble) deben contar con mantenimiento preventivo y correctivo que garanticen la vida útil. En caso de requerir servicio de mantenimiento se debe seguir el procedimiento de **mantenimiento preventivo y correctivo**.

A.7.12 Seguridad en el cableado

- El cableado de red y del suministro eléctrico debe encontrarse protegido contra intercepciones y daños físicos.
- Para garantizar la seguridad en el cableado se debe considerar:

    a) Contar con la topología o diagrama de cableado de las instalaciones.
    b) Proteger el cableado de red contra intercepciones o daños, usando ductos especiales y evitando que sean visibles en las áreas públicas.
    c) Los cables de alimentación de energía y los cables de red se encontrarán separados para evitar interferencias.
    d) El cableado se encontrará debidamente rotulado e identificado minimizando riesgo de errores como conexiones incorrectas.
    e) La identificación y rotulación del cableado debe darse por medios de identificación visual sencilla y práctica, (rótulos, colores, estructura, etc.), donde sea posible.

A.7.13 Mantenimiento de equipo

- Los equipos de cómputo y comunicaciones deben seguir programas de mantenimiento adecuados para garantizar su continua disponibilidad e integridad.
- En el mantenimiento de equipos se considerará:
    a) Elaborar planes de mantenimiento de acuerdo a las especificaciones del proveedor y/o la definida por el área de administración en el **Programa de Mantenimiento.**
    b) El mantenimiento debe realizarse exclusivamente por personal capacitado y autorizado.
    c) Se debe mantener un registro de los mantenimientos preventivos y correctivos que presenten los equipos, estos registros deben contener la fecha y acciones de los mantenimientos preventivo y correctivo a los que sea sometido, ***Control de mantenimiento.***
    d) Cuando el mantenimiento es realizado por personal externo, la Información sensible debe ser respaldado de acuerdo a la instrucción de ***Respaldo de información*** previa entrega al proveedor de servicio.
    e) Los mantenimientos serán bajo supervisión del área de administración, esto dependerá del tipo de activo y el tipo de mantenimiento que se ejecutará.

A.7.14 Seguridad en la eliminación o reutilización de equipos

- Todos los equipos que se descarten para su uso deben ser revisados para garantizar que cualquier dato sensible, licencias y software hayan sido removidos de forma definitiva como medida de seguridad antes de la eliminación, desecho o re uso, esta actividad deberá ser coordinada por el área de administración y el administrador técnico de seguridad.
- Los dispositivos dañados que contienen Información sensible deben ser sometidos a evaluación para decidir si se destruirán físicamente, serán reparados o recuperados por parte del administrador técnico de seguridad.
- Todo respaldo de información realizada a equipos que se eliminen o reutilicen deberán seguir lo establecido en el documento **Respaldo y Borrado de Activos de Información.**
- Si algún equipo es declarado como inservible por daño físico u obsolescencia, debe ser actualizado su estado en el **Inventario de Activo**.