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

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 corporativa 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. Política

A.11.1 Áreas seguras

A.11.1.2 Controles físicos de entrada

- Las áreas seguras serán protegidas por mecanismos que garanticen la entrada exclusivamente al personal autorizado, obedeciendo lo establecido en el documento ***Control de Acceso de áreas seguras (POL-07.FO-01),*** donde se establece el área a que tiene acceso cada colaborador, éste documento es gestionado por el Oficial de Seguridad de la Información.
- Para los controles físicos de entradas debe considerarse sin ser limitativo:

  a) Guardar registro de la fecha, hora de entrada y salida de las instalaciones, proveedores y visitantes, la evidencia de esta acción queda registrada en el ***Control de acceso de visitantes (POL-07.FO-02).***
  b) Todo los colaboradores deben registrar su entrada y salida en los mecanismo definidos por la organización (biométricos, bitácoras, etc.)
  c) Todos los terceros visitantes deben identificarse a través del gafete correspondiente, éste 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.
  e) El acceso a terceros visitantes a las áreas seguras debe otorgarse únicamente si está justificado plenamente el acceso.

- Todo colaborador o visitante que requiera ingresar con equipo de cómputo o herramienta deberá registrarlo en la bitácora de ***Control de acceso equipo y herramienta (POL-07.FO.03)***.

A.11.1.3 Aseguramiento de oficinas, salas e instalaciones

- El CCTV registra los accesos y salidas de los colaboradores, éste sistema es monitoreado por el área de recursos materiales; el CCTV respalda 7 días de grabación, recursos materiales registra cualquier incidente siguiendo lo establecido en la política **A.16 Gestión de incidentes de seguridad de la información (POL-11)**.
- 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.11.1.4 Protección contra amenazas externas 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 la política **A17 Continuidad del negocio (POL-12).**

A.11.1.5 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 recursos materiales realizará un recorrido por las instalaciones para verificar que todas las puertas han sido cerradas.
    d) Los colaboradores deberán asegurarse al final de su horario laboral no dejar a la vista información considerada confidencial o restringida.

A.11.1.6 Áreas de entrega y carga

- Las áreas de carga y descarga de insumos deben estar delimitadas.
- 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:

    a) Sea el personal identificado y autorizado por parte del proveedor, registrar su entrada y salida en las bitácoras correspondientes ***Control de acceso de visitantes (POL-07.FO-02).***
    b) 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.
    c) Cuando se trate de salida de mercancía deberá ser registrada en el formato ***Pase de Salida (POL-07.FO-05)***

A.11.2 Equipo

A.11.2.1 Ubicación y protección del equipo

- El acceso al área del servidor se encuentra controlado mediante la ***Bitácora de acceso al servidor (POL-07.FO-06).***

- 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 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.11.2.4 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 recursos materiales en el **Programa de Mantenimiento (MAN-01.FO-04).**
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 (PRO-06.FO-01).***
d) Cuando el mantenimiento es realizado por personal externo, la Información sensible debe ser respaldado de acuerdo a la instrucción de ***Respaldo de información (INS-03)*** previa entrega al proveedor de servicio.
e) Los mantenimientos serán bajo supervisión del área de recursos materiales, esto dependerá del tipo de activo y el tipo de mantenimiento que se ejecutará.

A.11.2.5 Seguridad del equipo fuera del local

- Los equipos de cómputo propiedad de DIGILOGICS no tienen autorización para que salgan de las instalaciones, en caso de que por necesidad extraordinaria del trabajo o suceso inesperado sea indispensable llevárselos serán sometidos a controles de acuerdo a los riesgos a los que sean expuestos.

a) Todo equipo de cómputo o medio de almacenamiento que salga de las instalaciones deberá ser registrado sin excepción en el formato ***Pase de Salida (POL-07.FO-05).***
b) Los colaboradores que extraigan los equipos de las instalaciones deben conocer y respetar las especificaciones y cuidados a fin de evitar daños al equipo.

A.11.2.6. Seguridad de los equipos y activos fuera de las instalaciones

- En caso de que por necesidad extraordinaria del trabajo o suceso inesperado sea indispensable llevárselos deberán seguir las siguientes indicaciones:
- Dar aviso a recursos materiales de la salida del equipo.
- 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. DIGILOGICS no se hace responsable del equipo personal utilizado sin autorización.
- Mantener su información documentada en un entorno seguro y asegurando todo material confidencial, secretos comerciales, etc.

A.11.2.8 Equipo de usuario desatendido

- El equipo desatendido debe ser bloqueado o en su defecto se activará 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 éste tipo de información.

A.11.2.9 Pantalla y escritorio limpio

- 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.

4. Control de Versiones

Número de Versión	Fecha de Actualización	Descripción del Cambio
2	Marzo, 2020	Actualización de las políticas