A.16 Gestión de incidentes de seguridad de la información (POL-11)

A.16 Gestión de incidentes de seguridad de la información (POL-11)

1. Objetivo

Establecer las directrices para garantizar un enfoque consistente y eficaz para la administración de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

2. Alcance

Su alcance se dirige a toda persona que cuente con legítimo acceso a los sistemas de información de DIGILOGICS, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados, los incidentes pueden impactar activos físicos y lógicos.

3. Política

A.16 Gestión de incidentes de seguridad de información

A.16.1.1 Responsabilidades y procedimientos

- Todo incidente de seguridad de la información debe ser reportado al Oficial de Seguridad de la Información al correo electrónico: soporte.sgi@digilogics.com.mx.
- que quede registro del levantamiento, seguimiento y solución del incidente.

A.16.1.2 Reporte de eventos de seguridad de la información

- Todo empleado debe reportar un incidente de seguridad de la información de acuerdo al numeral 5 del documento **Protocolo de acción contra incidentes (INS-06).**
- El Oficial de Seguridad de la Información registrará el incidente en el **Reporte de incidentes de Seguridad de la Información (POL-11.FO-01).**
- El Oficial de Seguridad de la Información deberá iniciar inmediatamente la instrucción **Protocolo de acción contra incidentes (INS-06)**, comunicando el incidente a las áreas encargados que ayudaran en la atención del mismo.
- El Oficial de Seguridad de la Información en conjunto de las áreas responsables definirán acciones de contención.
- El Oficial de Seguridad de la Información debe presentar el **Resumen de incidentes de seguridad de la información (POL-11.FO-2)** a la Alta Dirección, solo en caso de existir incidente alguno.
- El Oficial de Seguridad de la Información dará seguimiento de avances a las acciones derivadas de los incidentes de seguridad de la información según aplique.
- El Oficial de Seguridad de la Información y la Alta Dirección realizarán un análisis de los incidentes en caso de existir, para definir acciones correctivas profundas derivadas de esta gestión.

A.16.1.3 Reporte de debilidades de seguridad de la información

- Las debilidades de seguridad de la información son reportadas bajo el mismo mecanismo definido en el punto A.16.1.2 Reporte de incidentes de seguridad de la información, la

diferencia es que no se genera una acción de contención, sino inmediatamente una acción correctiva.

A.16.1.4 Evaluación y decisión sobre eventos de seguridad de la información

- La Evaluación y decisión sobre eventos de seguridad de la información se llevará a cabo bajo los siguientes criterios:
  - El evento compromete los niveles de riesgo, pero no afecta la operación de la organización y sus objetivos de negocios. Por ejemplo, sería un evento cuando una persona tiene acceso a áreas que deberían estar restringidas. Esto genera un aumento temporal del riesgo, pero no impide que la organización alcance sus objetivos de negocio.
  - El incidente, a diferencia del evento, sí logra afectar negativamente a la organización e incluso a la información. Puede representar pérdida o corrupción de la información y ocasionar un retraso en las operaciones. Por ejemplo: un incendio en las instalaciones que vulnere el servidor.
- Dichos criterios también están establecidos en el Plan de continuidad del negocio (PLAN-03)

A.16.1.5 Respuestas a incidentes de seguridad de la información

- Todos los colaboradores de DIGILOGICS deben de apegarse al **Protocolo de acción contra incidentes (INS-06).** En caso de que no se dé el reporte, registro, seguimiento y cierre mediante la presente política, se considera que no es un incidente y una violación a las políticas de seguridad de la información.

A.16.1.7 Recopilación de evidencias

- Todo incidente no documentado es como si jamás hubiera ocurrido, por lo tanto, para que se haga el levantamiento, seguimiento y cierre del incidente se requieren de las evidencias que los sustenten, estás dependerán del tipo de incidente. El Administrador Técnico de Seguridad de la Información define el formato **DIGI-IT-02** como el medio para recopilar dichas evidencias.

4. Control de Versiones

Número de Versión	Fecha de Actualización	Descripción del Cambio
3	Abril, 2021	Actualización del documento de recopilación de evidencia: A.16.1.7