
digilogics

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. Términos y Definiciones

- **Incidente de Seguridad de la Información**: un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

4. Política

A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

- Se deberán planear campañas de difusión de los posibles incidentes de seguridad de la información, con alcance a toda la organización.
- Todo empleado debe reportar un incidente de seguridad de la información de acuerdo al numeral 5 del documento **Protocolo de acción contra incidentes al correo** alejandro.lopez@digilogics.com.mx.
- En casos de emergencia se puede localizar por teléfono empresarial al Administrador Técnico de Seguridad de la Información.
- El Administrador Técnico de Seguridad de la Información registrará el incidente en el **Reporte de incidentes de Seguridad de la Información**
- El Administrador Técnico de Seguridad de la Información deberá iniciar inmediatamente la instrucción **Protocolo de acción contra incidentes**
- El Oficial de Seguridad de la Información debe presentar el **Resumen de incidentes de seguridad de la información** a la Alta Dirección, solo en caso de existir incidente alguno.
- El administrador técnico de la Información dará seguimiento de avances a las acciones derivadas de los incidentes de seguridad de la información según aplique.

A.5.25 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 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 **Protocolo de acción contra incidentes.**

A.5.26 Respuestas a incidentes de seguridad de la información

Todos los colaboradores de DIGILOGICS deben de apegarse al **Protocolo de acción contra incidentes y en la política de Continuidad del negocio.**

A.5.27 Aprendizaje de incidentes de seguridad de la información

DIGILOGICS identifica dentro de **Protocolo de acción contra incidentes**, un apartado de lecciones aprendidas, que es gestionado por el Administrador Técnico de Seguridad de la Información, donde se analizan los incidentes hasta después de su cierre para aprender del mismo y mejorar o fortalecer los esquemas de seguridad de la organización, mediante el uso del mecanismo de acciones correctivas y planes de mejora, derivado del análisis de los incidentes.

A.5.28 Recolección 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 y **reporte de incidentes de seguridad de información** como el medio para recopilar dichas evidencias.