|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Directriz Rectora de Respuesta a Incidentes | |  | **MAAGTICSI** | | Establecer la línea a seguir para planear, realizar, analizar y evaluar incidentes de seguridad en la STIC del INR. | **Proyecto:**  **ID:** | | | |  | | | |

|  |  |  |
| --- | --- | --- |
|  | **DIRECCIÓN GENERAL** | logo siglas autorizado curvas |
| **SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES** |
| **Directriz Rectora de Respuesta a Incidentes** |

**CONTENIDO**

[1 OBJETIVO DEL DOCUMENTO 2](#_Toc383085661)

[2 ABREVIATURAS Y DEFINICIONES 2](#_Toc383085662)

[3 Referencias 2](#_Toc383085663)

[4 OBJETIVO DE LA DIRECTRIZ 3](#_Toc383085664)

[5 ALCANCE 3](#_Toc383085665)

[6 JUSTIFICACIÓN 3](#_Toc383085666)

[7 ROLES Y RESPONSABILIDADES 4](#_Toc383085667)

[8 DIRECTRICES DE RESPUESTA A INCIDENTES 6](#_Toc383085668)

[9 MECANISMO DE DIFUSIÓN 7](#_Toc383085669)

[10 MECANISMO DE REVISIÓN DEL CUMPLIMIENTO DE LA DIRECTRIZ 7](#_Toc383085670)

[11 BITÁCORA DE CONTROL DE CAMBIOS 7](#_Toc383085671)

# OBJETIVO DEL DOCUMENTO

Establecer la línea a seguir para planear, realizar, analizar y evaluar incidentes de seguridad en la STIC del INR.

# ABREVIATURAS Y DEFINICIONES

|  |  |
| --- | --- |
| **Abreviación o definición** | **Descripción** |
| INRLGII | Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra |
| MAAGTICSI | Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y Seguridad de la Información |
| SGSI | Sistema de Gestión de Seguridad de la Información |

# Referencias

|  |  |
| --- | --- |
| **Descripción del documento** | **Nombre del archivo** |
|  |  |
|  |  |
|  |  |

# OBJETIVO DE LA DIRECTRIZ

Establecer la línea a seguir para planear, realizar, analizar y evaluar incidentes de seguridad en la STIC del INR, sensibilizando al personal en identificar y planear las medidas adecuadas para su tratamiento, con los mecanismos, elementos, herramientas y todos aquellos apoyos que permitan a la Subdirección reaccionar ante incidentes que se presentan y mitigarlos con los menores daños y costos posibles.

# ALCANCE

El presente documento aplica a cualquier incidente que ponga en riesgo la Confidencialidad, Integridad y/o Disponibilidad de la información y activos críticos dela STIC.

# JUSTIFICACIÓN

La presente directriz nos permitirá describir los elementos internos y externos que obligan al establecimiento de la Respuesta a Incidentes, logrando tomar como base para esto experiencias pasadas que hayan impactado alas TIC, para así evitar impactos negativos al Instituto en sus bienes y servicios, logrando así beneficios significativos.

# ROLES Y RESPONSABILIDADES

| **Rol** | **Descripción** | **Responsabilidades** |
| --- | --- | --- |
| ERISC | Equipo de Respuesta a Incidentes de Seguridad de TIC. | Bajo la coordinación y supervisión del GI-TIC, elaborar y mantener actualizada una Directriz rectora de respuesta a incidentes.  En coordinación con el GI-TIC y de acuerdo a lo establecido en la Directriz rectora de respuesta a incidentes: Definir acciones de resolución de incidentes e integrar una Guía técnica de atención a Incidentes de acuerdo a la criticidad de los activos de TIC afectados.  Dar seguimiento a los incidentes registrados en la Herramienta de Mesa de Servicios, así como a la Base de Conocimientos de la misma.  Reportar al Responsable de seguridad de la información, los incidentes que se presenten y el resultado de su gestión.  Ejecutar las acciones necesarias para atender un incidente de seguridad de la información de impacto y prioridad alta para la STIC y/o el Instituto, cuando no sea posible atenderse por segundo y tercer nivel de la mesa de servicios, así como dar seguimiento a las acciones tomadas en la gestión de incidentes en la Herramienta de Mesa de Servicios.  El ERISC, en coordinación con el Responsable del GI-TIC, deberá:   * Definir las acciones de atención a los incidentes con apoyo de la Guía técnica, respecto del Incidente que se haya presentado. * Ejecutar la solución necesaria. * Registrar los datos del Incidente y su solución. * Asegurar que se comunique el Incidente y su solución, al GI-TIC y a los Responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados. * Integrar los datos del Incidente y su solución a la base de conocimientos. |
| RSII | Responsable de la Seguridad de la Información | Coordinar los trabajos del equipo en la identificación, documentación, revisión periódica de los Procesos Críticos de la STIC, así como de las Infraestructuras Críticas y Activos de Información.  Impulsar la participación de los integrantes del equipo.  Vigilar el desarrollo y cumplimiento de los trabajos desarrollados por el equipo de trabajo.  Elaborar el Documento de Definición, implantación, Evaluación y Mejora del SGSI.  Asegurar que los controles de seguridad se hayan implantado de acuerdo a lo previsto en el Documento de Definición, implantación, Evaluación y Mejora del SGSI.  Elaborar los informes correspondientes a las desviaciones en la implantación y/o en la operación de los controles de seguridad tomando para esto el Documento de Definición, implantación, Evaluación y Mejora del SGSI.  Enviar el Documento de Definición, implantación, Evaluación y Mejora del SGSI al GI-TIC.  Obtener los datos necesarios para verificar la eficiencia y eficacia de los controles implementados.  Medir la efectividad de los controles de seguridad implantados.  Efectuar evaluación del SGSI mediante el Documento de Definición, implantación, Evaluación y Mejora del SGSI.  Registrar la información de los intentos, exitosos y no exitosos, de violaciones e incidentes de seguridad, así como efectuar el análisis y evaluación de dicha información.  Documentar las acciones de revisión del SGSI que hayan resultado de los factores críticos anteriores, mediante la elaboración y/o actualización del Documento de Definición, implantación, Evaluación y Mejora del SGSI.  Verificar el contenido del Documento de Definición, implantación, Evaluación y Mejora del SGSI; actualizar y enviarlos al GI-TIC. |

# DIRECTRICES DE RESPUESTA A INCIDENTES

|  |  |  |  |
| --- | --- | --- | --- |
| **Necesidad** | **Directriz de respuesta a incidentes** | **Escenario** | **Impacto** |
| Tecnológica | Detección y  Registro del  Incidente | * Actores * Tiempo * Recursos * Tipo de incidente | Alto |
| Operativa | Clasificación y Apoyo | * Actores * Tiempo * Recursos * Tipo de incidente | Alto |
| Administrativa | Solicitud de Servicio | * Actores * Tiempo * Recursos * Tipo de incidente | Alto |
| Financiera | Investigación y Diagnostico | * Actores * Tiempo * Recursos * Tipo de incidente | Alto |
| Humana | Resolución y Recuperación | * Actores * Tiempo * Recursos * Tipo de incidente | Alto |
| Política | Cierre del Incidente | * Actores * Tiempo * Recursos * Tipo de incidente | Alto |

# MECANISMO DE DIFUSIÓN

La STIC del INR establecerá el mecanismo y sus elementos para asegurar la difusión de la Directriz rectora y procurará su entendimiento en la totalidad de los involucrados e instancias externas para los aspectos que les atañan.

# MECANISMO DE REVISIÓN DEL CUMPLIMIENTO DE LA DIRECTRIZ

Los periodos de revisión y evaluación del mecanismo y sus elementos para asegurar el cumplimiento de la Directriz por parte de los involucrados y/o responsables de la procuración de su seguimiento se ha acordado con las áreas involucradas en periodos anuales (al menos una veces al año). Si fuera necesario, se revisará por medio deuna petición formal de los responsables de su implementación y monitoreo.

# BITÁCORA DE CONTROL DE CAMBIOS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Revisión** | **Descripción del Cambio** | **Fecha de evaluación** | **Aprobador** | **Aceptado /Rechazado** | **Fecha de aplicación** |
| 01 | Actualización de la Imagen Institucional | JUN 15 | Mtra. Ma. De Lourdes Zaldívar Martínez | Aceptado | JUN 15 |
| 02 | Transición del SGC de la Norma ISO 9001:2008 a la Norma ISO 9001:2015  Revisión de contenidos y actualización de encabezados | MAY 18 | M. en I. María Isabel Garrido Galindo | Aceptado | MAY 18 |
| 03 | Actualización de ImagenInstitucional | DIC 20 | M. en I. María Isabel Garrido Galindo | Aceptado | DIC 20 |