|  |  |  |
| --- | --- | --- |
| Programa de Contingencia  a los Riesgos |  | **MAAGTICSI** |

|  |  |
| --- | --- |
| Documentar las acciones y decisiones en caso de un evento o incidente que tenga un impacto potencial para el Instituto | **Proyecto:**  **ID:** |



**CONTENIDO**

1 ObjetivoS del Documento 3

2 Abreviaturas y definiciones 3

3 Referencias 3

4 Objetivo del Programa 4

5 Bitácora de Control de Cambios 8

1. ObjetivoS del Documento

*[Documentar las acciones y decisiones en caso de un evento o incidente que tenga un impacto potencial para el Instituto.]*

1. Abreviaturas y definiciones

|  |  |
| --- | --- |
| **Abreviación o definición** | **Descripción** |
|  |  |
|  |  |
|  |  |

1. Referencias

|  |  |
| --- | --- |
| **Nombre del documento** | **Descripción del documento** |
| *[Nombre del o los documentos a los que se hace referencia a lo largo del llenado de este formato].* | *[Escriba una breve descripción del documento, así como su ubicación física o lógica].* |
|  |  |
|  |  |

1. Objetivo del Programa

*[Documentar las acciones y decisiones en caso de un evento o incidente que tenga un impacto potencial para la Instituto.]*

**4.1 Eventos generadores**

*[Hasta el momento el mecanismo de activación del programa de contingencias contempla eventos como los siguientes:]*

|  |  |
| --- | --- |
| **EVENTOS** | **ACCIONES O MECANISMOS DE ACTIVACIÓN** |
| * *Nombre del evento generador aplicable a la STIC.* | * *Describir las acciones que se tomarán para contrarrestar al evento generador.* |

**4.2 Definición del Programa de contingencia y pruebas de viabilidad**

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Incidente** | **Actividades** | **Resultados Obtenidos** |
| *Riesgo 1* | *[Nombre del incidente]* | *[Describir acciones a realizar]* | *[Colocar los resultados obtenidos de cada actividad realizada]* |
| *Riesgo 2* |  |  |  |
| *Riesgo n* |  |  |  |

**4.3 Definición de la estructura del equipo de respuesta a la contingencia por el riesgo**

| **Puesto** | **Rol** |
| --- | --- |
| Subdirectora de Tecnologías de Información y Comunicaciones | Líder del ERISC |
| Jefe de Departamento de Gestión de Arquitectura e Infraestructura Tecnológica | Líder suplente del ERISC |
| Jefe del Departamento de Gestión y Operación de Servicios | Analista de Incidentes |
| Coordinador del Departamento de Gestión y Operación de Servicios |
| Coordinador del Departamento de Gestión y Operación de Servicios |
| Jefe del Departamento de Gestión y Desarrollo de Soluciones Tecnológicas |
| Coordinador del Departamento de Gestión y Desarrollo de Soluciones Tecnológicas |
| Coordinador del Departamento de Gestión y Desarrollo de Soluciones Tecnológicas |
| Coordinador de Infraestructura de Datos y Seguridad |
| Coordinador de Arquitectura Tecnológica |  |
| Coordinador de Infraestructura de Edificio Inteligente |
| Coordinador de Infraestructura de Voz y Cableado Estructurado |
| Coordinador de Incidentes |
| Coordinador de Mesa de Servicios de Infraestructura de Comunicaciones/Edificio Inteligente |
| Coordinador de Desarrollo de Soluciones Tecnológicas Administrativas |
| Coordinación de Desarrollo de Soluciones Tecnológicas Médicas |

*De acuerdo a la estructura de la STIC.*

**4.4 Responsabilidades**

| **ROL** | **RESPONSABILIDADES** |
| --- | --- |
| **Líder del**  **ERISC** | * Establecer los mecanismos de comunicación del Equipo. * Informar periódicamente al Responsable de la Seguridad en la STIC, sobre los incidentes de seguridad y su correspondiente atención y solución. * Definir el Procedimiento de movilización de las partes involucradas, describiendo las medidas técnicas, organizativas y humanas a realizar para la solución del incidente de manera pronta y eficiente. * Transmitir por los medios de comunicación acordados, al personal y áreas afectadas la contingencia de que se trata y la estimación de solución |
| **Líder suplente del ERISC** | * Apoyar en las actividades asignadas al Líder del ERISC. * Sustituir al Líder del ERISC, en la toma de decisiones, en caso de ausencia. * Realizar el cierre de incidentes, en caso de ausencia del Líder del equipo. * Establecer los mecanismos y medidas para que la respuesta inicial sea de forma * Definir el Procedimiento de movilización de las partes involucradas, describiendo las medidas técnicas, organizativas y humanas a realizar para la solución del incidente de manera pronta y eficiente. * Elaborar un informe describiendo los daños generados por el incidente, el alcance de reparación obtenido y acciones de mejora. * Definir las tareas a realizar para poder identificar y evaluar el nivel de contingencia que se presenta indicando el grado de daño de los activos afectados por los incidentes. |
| **Analista de Incidentes** | * Realizar la detección y atención de incidentes de acuerdo al Procedimiento definido. * Elaborar un informe de daños generados por el incidente, el alcance de reparación obtenido y acciones de mejora. * Identificar los las empresas, direcciones y áreas externas involucradas * Describir las tareas necesarias a realizar por cada una de las áreas involucradas para la solución de los incidentes. * Realizar un matriz de pruebas indicando las actividades y resultados obtenidos para la solución de los incidentes. |

**4.5 Aseguramiento de respuesta a la contingencia**

*[Los integrantes del ERISC establecerán el mecanismo de registro de incidentes de seguridad de la información.*

*Se definirán turnos de guardia, así como permisos y accesos a las instalaciones del Instituto.]*

**4.6 Evaluación preliminar del daño**

*[Actualizar en el monto en que se implemente el SGSI.]*

**4.7 Informar a los usuarios afectados por la contingencia**

*[Los responsables de la detección de incidentes de seguridad notificarán inmediatamente al Líder del ERISC y/o al Líder suplente del ERISC por medio de correo electrónico, teléfono celular o voceo solo para localización.*

*El líder del ERISC informará periódicamente al Responsable de la Seguridad de la Información de la STIC acerca de los incidentes ocurridos en el periodo (en caso de ocurrencia).*

*El Líder del Equipo, o su Suplente en caso de ausencia será el único autorizado para realizar el cierre de los incidentes detectados en la operación de TIC.*

*El cierre de los incidentes solo podrá ser realizado por el Líder del Equipo o Suplente de Respuesta a Incidentes de Seguridad de la Información de TIC.]*

**4.8 Procedimiento de respuesta**

*[El procedimiento de respuesta y movilización de las partes involucradas se adecuara considerando: Medidas Técnicas, Organizacionales y Humanas para la solución de incidentes:*

**4.9 Medidas técnicas:**

*Extintores contra incendios.*

*Detectores de humo.*

*Salidas de emergencia.*

*Equipos informáticos de respaldo.*

*Plan de respaldo:*

*Revisión de extintores.*

*Simulacros de incendio.*

*Realización de copias de respaldo.*

*Revisión de las copias de respaldo.*

*Plan de emergencia:*

*Aplicación del contrato de arrendamiento de equipos de TI.*

*Restauración de las copias de respaldo.*

*Reanudación de operaciones.*

**10. Medidas organizativas:**

*Aplicaciones de seguros y garantías.*

*Procedimiento de copia de respaldo.*

*Procedimiento de actuación en caso de incendio.*

**10.1 Medidas humanas:**

*Capacitación para actuar en caso de incendio.*

*Asignación de roles y responsabilidades para la operación de respaldos.*

**10.2 Ejecución**

*Actualmente los analistas de incidentes de las áreas de la STIC están definiendo las tareas a realizar para la gestión y solución de incidentes que estén al alcance de sus responsabilidades.*

**10.3 Evaluación**

*No se ha realizado ningún análisis de resultados de daños generados por incidentes ni se tienen acciones de mejora dado que el programa de contingencias de riesgos no se ha ejecutado.]*

**10.4 Lista de contactos externos**

|  |  |  |
| --- | --- | --- |
| **Nombre de empresa, dirección o área externa** | **Personal de contacto** | **Medios de contacto** |
| *[Nombre de la empresa y/o institución externa de soporte a la STIC]* | *[Nombre de la persona responsable de contactar a los proveedores]* | *[Colocar el medio de contacto: correo electrónico, teléfono, etc.]* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. 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 Imagen Institucional | DIC 20 | M. en I. María Isabel Garrido Galindo | Aceptado | DIC 20 |