RFC 2350 - Descripción del CSIRT de la ARIU

1. Información del Documento

1.1 Fecha de la última actualización

Esta es la versión 1.0 del 29 de Febrero de 2024.

1.2 Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de correo csirt@riu.edu.ar

2. Información de Contacto

2.1 Nombre del Equipo

Nombre del equipo: CSIRT-ARIU

2.3 Dirección Postal

Asociación de Redes de Interconexión Universitaria (ARIU)

Maipú 645

CP1006

CABA

Argentina

2.4 Información de Contacto

Correo Electrónico: csirt@riu.edu.ar

Horario de Atención: 9:00 - 17:00 (GMT -3), de lunes a viernes

2.5 Información de Otros Medios de Contacto

Sitio: https://riu.edu.ar/csirt-ciberseguridad/

2.6 Puntos de Contacto para Emergencias

Correo de Emergencia: csirt@riu.edu.ar

3. Constitución

3.1. Misión

El CSIRT-ARIU tiene como misión colaborar en la protección de la infraestructura de red de las instituciones miembro de la ARIU mediante la prevención, detección y respuesta a incidentes de seguridad informática.

3.2. Ámbito de Operación

El CSIRT-ARIU proporciona servicios a todas las universidades e instituciones educativas miembro de la ARIU.

3.3. Patrocinio y Afiliación

El CSIRT-ARIU es patrocinado por la Asociación de Redes de Interconexión Universitaria

3.4. Autoridad

El CSIRT-ARIU opera bajo la autoridad de la ARIU y tiene la capacidad de coordinar respuestas a incidentes en la comunidad objetivo.

4. Actividades y Servicios

4.1. Detección de Incidentes

El CSIRT de la ARIU monitorea la red de las instituciones miembro para detectar actividades sospechosas y posibles incidentes de seguridad.

4.2. Análisis de Incidentes

El equipo analiza los incidentes reportados para determinar su naturaleza, origen, impacto y medidas de mitigación necesarias.

4.3. Respuesta a Incidentes

El CSIRT colabora en la respuesta a incidentes de seguridad reportados, proporcionando asistencia técnica y orientación para contener, erradicar y recuperar los sistemas afectados.

4.4. Prevención y Concientización

El CSIRT promueve buenas prácticas de seguridad a través de programas de formación y concientización dirigidos a las instituciones miembro.

4.5. Coordinación y Cooperación

El CSIRT colabora con otros equipos de respuesta a incidentes a nivel nacional e internacional para intercambiar información y coordinar acciones conjuntas.

5. Políticas

5.1. Tipos de Incidentes y Nivel de Soporte

El CSIRT de la ARIU maneja incidentes de varios tipos, incluyendo pero no limitado a: Malware y virus, Ataques de phishing, Intrusiones y accesos no autorizados, Denegación de servicio (DoS/DDoS)

5.2. Procedimientos de Manejo de Incidentes

Recepción del Reporte: Recepción de notificaciones de incidentes a través del portal web.

Clasificación y Priorización: Evaluación inicial para determinar la gravedad y el impacto del incidente.

Análisis y Mitigación: Investigación detallada y desarrollo de una estrategia de mitigación.

Resolución y Recuperación: Implementación de medidas correctivas y restauración de servicios.

Documentación y Reporte: Registro detallado del incidente y las acciones tomadas.

5.3. Privacidad y Confidencialidad

El CSIRT de la ARIU se compromete a mantener la confidencialidad de la información recibida y solo compartirá detalles específicos con las partes autorizadas y pertinentes.

6. Infraestructura de Seguridad

6.1. Monitoreo y Detección

El CSIRT emplea diversas herramientas y tecnologías para la detección proactiva de amenazas y monitoreo continuo de la red.

6.2. Análisis de Vulnerabilidades

Realización de evaluaciones periódicas de vulnerabilidades para identificar y mitigar riesgos potenciales.

6.3. Capacitación Continua

El CSIRT trabaja en programas de capacitación y actualización continua para sus miembros y personal de las instituciones afiliadas.