GESTIÓN DE CIBERINCIDENTES

APROBADO POR:	Nº DE REVISIÓN	FECHA	RESUMEN DE CAMBIOS/COMENTARIOS
	0.1	19/05/2015	Borrador
Comité de Seguridad	0.2	26/09/2017	Revisado por el Comité de Seguridad

Índice

1 OBJETO

El objeto de este procedimiento es definir la sistemática establecida por la Universidad de Granada para la gestión y notificación de incidentes y vulnerabilidades de seguridad con el propósito de asegurar que los incidentes de seguridad y las debilidades asociadas con los sistemas de información se comunican de tal manera que haya tiempo para tomar acciones correctoras y poder evitarlos en un futuro.

Además se pretende dar cumplimiento al artículo 90 del Real Decreto 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

Todo ello en cumplimiento de las medidas de seguridad establecidas en el Anexo II del R.D. 3/2010 por el que se regula el Esquema Nacional de Seguridad en al ámbito de la administración electrónica y de los objetivos de la entidad.

2 ALCANCE

Este procedimiento aplica a todos los sistemas y al personal que intervienen en la prestación de servicios de administración electrónica de la Universidad de Granada, así como a todos aquellos que tengan acceso a los mismos.

3 DOCUMENTACIÓN DE REFERENCIA

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

4 RESPONSABILIDADES

Será responsabilidad del Responsable de Seguridad velar por el cumplimiento del presente procedimiento, realizando un seguimiento de los incidentes ocurridos.

Será responsabilidad de todos los usuarios, internos o externos, notificar:

- Cualquier incidente de seguridad, real o sospechado, mediante los medios establecidos.
- Cualquier debilidad en el sistema aunque está todavía no haya dado lugar a un fallo de seguridad.

5 DESARROLLO

5.1 NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

En el registro de incidentes (herramienta GIA) se reflejarán todos aquellos incidentes de seguridad que se detecten, entendiéndose por incidente de seguridad o ciberincidente cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos o servicios así como a la infraestructura que le da soporte. Asimismo se notificará si se detecta una vulnerabilidad o debilidad que pueda afectar a la seguridad de la información o de los servicios.

Todo usuario que detecte un incidente de seguridad o debilidad en los sistemas de información deberá notificarlo al CSIRC:

- La aplicación GIA http://csirc.ugr.es/informatica/destacados/Incidencias/GIA.
- El correo electrónico seguridadinformatica@ugr.es
- El número telefónico 36000.

El técnico que recibe la notificación deberá proceder a registrar el incidente en la herramienta GIA.

5.2 CLASIFICACIÓN DE LOS CIBERINCIDENTES

La clasificación de incidentes aplicada por la Universidad de Granada, se muestra en la siguiente tabla:

Clase de incidente	Descripción	Tipo de incidente
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas	• Virus • Gusanos • Troyanos • Spyware • Rootkit • Ransomware (secuestro informático) • Herramientas para acceso remoto (RAT)
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas	• DoS / DDoS • Fallo (HW o SW) • Error humano • Sabotaje
Obtención de información	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	• Compromiso de cuentas de usuario • Defacement • Cross Site Scripting (XSS) • Cross Site Request Forgery (CSRF) • Falsificación de petición entre sitios cruzados • Inyección SQL • Spear Phising • Pharming • Ataque de fuerza bruta • Inyección de ficheros remota • Explotación de vulnerabilidad software • Explotación de vulnerabilidad hardware

Clase de incidente	Descripción	Tipo de incidente
Compromiso de la información	Incidentes relacionados con el acceso y fuga, modificación o borrado de información no pública	• Acceso no autorizado a la información • Modificación y borrado no autorizada de información • Publicación no autorizada de información • Exfiltración de información
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	• Suplantación / Spoofing • Uso de recursos no autorizado • Uso ilegítimo de credenciales • Violaciones de derechos de propiedad intelectual o industrial
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general, la ciberdelincuencia).	• Spam • Acoso / extorsión / mensajes ofensivos • Pederastia / racismo / apología de la violencia / delito, etc…
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización	• Abuso de privilegio por usuarios • Acceso a servicios no autorizados
Seguridad Física	Incidentes relacionados con la violación de las políticas y normas de seguridad física establecidas por la organización	• Acceso no autorizado a áreas seguras • Daños en las instalaciones
Documentación	Incidentes relacionados con la información impresa	• Documentación extraviada • Contenedores de documentación manipulados • Acceso no autorizado a documentación
Otros	Otros incidentes no incluidos en los apartados anteriores	•

5.3 PELIGROSIDAD DE LOS CIBERINCIDENTES

En la siguiente tabla se muestran los niveles de peligrosidad establecidos y los criterios para la determinación del nivel de peligrosidad de un incidente de seguridad:

Nivel	Vector de ataque	Características potenciales del incidente
Crítico	• APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc…	• Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. • Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.
Muy Alto	• Códigos dañinos confirmados de alto impacto (RAT, troyanos enviando datos, rootkit, etc.). • Ataques externos con éxito.	• Capacidad para exfiltrar información valiosa, en cantidad apreciable. • Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
Alto	• Códigos dañinos de medio impacto (virus, gusanos, troyanos). • Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). • Tráfico DNS con dominios relacionados con APTs o campañas de malware. • Accesos no autorizados, suplantación o sabotaje. • Cross-Site Scripting, inyección SQL. • Spear phising / Pharming.	• Capacidad para exfiltrar información valiosa. • Capacidad para tomar el control de ciertos sistemas.
Medio	• Descargas de archivos sospechosos. • Contactos con dominios o direcciones IP sospechosas. • Escáneres de vulnerabilidades. • Códigos dañinos de bajo impacto (adware, spyware, etc…). • Sniffing o ingeniería social.	• Capacidad para exfiltrar un volumen apreciable de información. • Capacidad para tomar el control de algún sistema.

Nivel	Vector de ataque	Características potenciales del incidente
Bajo	• Políticas. • Spam sin adjuntos. • Software desactualizado. • Acoso, coacción, comentarios ofensivos. • Error humanos, Fallo HW o SW.	• Escasa capacidad para exfiltrar un volumen apreciable de información. • Nula o escasa capacidad para tomar el control de sistemas.

5.4 NIVEL DE IMPACTO DEL CIBERINCIDENTE

Se define impacto potencial como una estimación del daño que podría causar un incidente de seguridad. Se aplican los siguientes criterios para evaluar el impacto potencial de los incidentes de seguridad:

Nivel	Criterios
Nulo	• Ningún sistema de información afectado llega a categoría BAJA. • No hay daños reputacionales apreciables.
Bajo	• La categoría más alta de los sistemas de información afectados es BAJA. • Daños reputaciones puntuales, sin eco mediático
Medio	• La categoría más alta de los sistemas de información afectados es MEDIA. • Más de 10 servidores afectados con información cuya máxima categoría es BAJA. • Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
Alto	• La categoría más alta de los sistemas de información afectados es ALTA. • Más de 50 servidores afectados con información cuya máxima categoría es BAJA. • Más de 10 servidores afectados con información cuya máxima categoría es MEDIA. • Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
Muy Alto	• Más de 100 servidores afectados con información cuya máxima categoría es BAJA. • Más de 50 servidores afectados con información cuya máxima categoría es MEDIA. • Más de 10 servidores afectados con información cuya máxima categoría es ALTA. • Daños reputacionales a la imagen del país (marca España). • Afecta apreciablemente a actividades oficiales o misiones en el extranjero. • Afecta apreciablemente a una infraestructura crítica.
Crítico	• Más de 100 servidores afectados con información cuya máxima categoría es MEDIA. • Más de 50 servidores afectados con información cuya máxima categoría es ALTA. • Afecta a la seguridad nacional. • Destruye una infraestructura crítica.

5.5 GESTIÓN Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

Actualmente el Área de Seguridad del CSIRC de la Universidad de Granada en la ISO 9001 en el procedimiento **<PE02-08-INSE >**utiliza un software de gestión de incidentes donde se registran los incidentes. Registrará como mínimo la siguiente información:

- Clasificación del incidente, en base a la clasificación establecida en el presente procedimiento.
- Fecha y hora de la detección del incidente.
- Fecha y hora de la notificación.
- Persona que recibe la notificación.
- Estado: Abierta, cerrada, pendiente de confirmar, etc…
- Dimensiones de seguridad afectadas: Confidencialidad, Disponibilidad e Integridad (si las dimensiones trazabilidad y autenticidad se ven afectadas, se considerará como un caso en que se encuentra afectada la integridad de la información).
- Fecha y hora de la resolución y cierre.
- Acciones llevadas a cabo para solucionarla
- Los efectos que se hubieran derivado de la misma.
- Proceso de recuperación (si aplica)

Cuando el incidente guarde relación con sistemas de nivel medio, se debe registrar también:

- Peligrosidad, en base a los criterios establecidos en el presente procedimiento.
- Impacto potencial, en base a los criterios establecidos en el presente procedimiento.
- Impacto o consecuencias.
- El número y tipología de los sistemas afectados.
- Nivel de degradación de los activos afectados: alta, media o baja.

Todos aquellos **ciberincidentes** con un **Nivel de Peligrosidad Alto, Muy Alto o Crítico**, deben ser notificados por el equipo de respuesta a incidentes de la Universidad de Granada al CCN-CERT a través del correo electrónico incidentes@ccn-cert.cni.es (o a través de la herramienta LUCIA en caso de estar implantada).

Una vez registrado, los propios técnicos del equipo de sistemas del CSIRC intentarán dar solución al incidente. Si consiguen solucionarlo, introducirán una descripción de las acciones realizadas y procederán a cambiar el estado a resuelto o cerrado en la herramienta de gestión de incidentes.

Si desde el CSIRC no pudiese resolverse el incidente, este será escalado/notificado al proveedor correspondiente, para que proceda a su resolución, y quedando constancia de este hecho en la herramienta de gestión de incidentes.

En este punto, la gestión del incidente o la vulnerabilidad se iniciará con la identificación de las causas o posibles causas que dan lugar a los mismos, así como de los efectos por éstos producidos.

El tratamiento de los incidentes y vulnerabilidades se llevará a cabo en dos frentes: corrector y preventivo. El tratamiento corrector tratará de resolver la problemática causada por el incidente de una manera inmediata. El preventivo establecerá los medios y o métodos precisos con el fin de evitar la repetición del mismo o la reducción de la vulnerabilidad. Así, cuando un incidente, a criterio del Responsable de Seguridad o del Responsable de Sistemas sea repetitivo o con un impacto grave como para tomar acciones, se abrirá una Acción Correctiva de acuerdo a lo descrito en el presente procedimiento.

Si el tratamiento correctivo del incidente da lugar a otro tipo de registro (recuperación de datos, destrucción de soportes, etc.) deberá indicarse el código y fecha de los registros correspondientes.

Para reducir los riesgos que resultan de la explotación de vulnerabilidades técnicas publicadas, el CSIRC, hará un seguimiento para identificar nuevas vulnerabilidades en los activos definidos en el inventario, y determinarán qué parches o modificaciones hay que aplicarles.

Se llevará a cabo el seguimiento de todos los incidentes detectados hasta su resolución.

Se conservarán los registros asociados a los incidentes de, al menos, los dos últimos años.

5.6 RECOLECCIÓN Y CUSTODIA DE EVIDENCIAS

El equipo del CSIRC registrará las tareas de análisis de los incidentes, las evidencias obtenidas durante los análisis y los resultados de éstos.

Los Servicios Universitarios implicados deberán recoger y mantener las evidencias que se recaben durante los análisis de forma que se asegure su precisión y completitud.

Adicionalmente, cuando se sospeche que los incidentes han sido consecuencia de actos maliciosos, a fin de garantizar su admisibilidad en juicio en caso de que se decidiese ejercitar acciones contra los responsables de los incidentes, en la recolección de las evidencias se tomarán las siguientes precauciones:

- Se archivarán los originales de las evidencias en papel usando medios que eviten cualquier posibilidad de que sean modificados, reemplazados, sustraídos o destruidos de forma intencionada o no deseada, registrando:
    - La identidad y los datos de contacto de quienes los recogieron.
    - El lugar en que fueron encontrados.
    - La fecha y hora en la que fueron recogidos.
    - Los accesos autorizados que sean realizados dejando constancia de la identidad de quienes acceden a las evidencias, además de la fecha, hora y demás datos relevantes sobre los accesos realizados.

- Para la recopilación de evidencias de los sistemas informáticos se asegurará que:
  - Se realicen copias de los discos duros, memorias y soportes removibles de información en los que se hallen almacenadas las evidencias electrónicas.
  - Se recaben los registros de monitorización generados por los sistemas durante la realización de las copias.
  - Se archiven los registros originales de forma tal que se evite todo acceso que pudiera comprometer su integridad o disponibilidad.
  - Se realicen todas las actividades necesarias para determinar la causa y los responsables de los incidentes exclusivamente sobre las copias realizadas a partir de los originales, registrando la identidad y los datos de contacto de las personas que realicen y presencien las mismas, todos los pasos dados y los recursos empleados.

5.7 GESTIÓN DE ACCIONES CORRECTIVAS.

Las acciones correctivas permitirán actuar sobre problemas (presentes o futuros) de cierta importancia, según el criterio del Responsable de Seguridad o del Responsable de Sistemas.

Localizado un problema debe determinarse la relación causa-efecto, considerando todas las causas posibles. Conocidas las causas, se analiza su importancia relativa y el coste de las posibles soluciones para eliminarlas. El Responsable de Seguridad, en colaboración con otro personal del CSIRC, tomará la decisión sobre las acciones a tomar y asignará responsables y plazos para su ejecución.

Asimismo será el encargado de controlar la ejecución y cierre de la acción correctiva, verificando que se han obtenido los resultados deseados.

Las acciones correctivas serán registradas y archivadas por el Responsable de Seguridad de acuerdo al formato FO.PS07-01 Acción correctiva.

6 REGISTROS

- Incidentes de seguridad registrados

7 ANEXOS

- FO.PS07-01 Acción correctiva