1. OBJETIVO

Identificar, evaluar y controlar los incidentes de seguridad digital, asegurando su gestión efectiva para dar una respuesta adecuada y minimizar los impactos adversos en la Unidad Administrativa Especial - Dirección de Impuestos y Aduanas Nacionales UAE DIAN y en sus operaciones de negocio, manteniendo los niveles de servicio y de disponibilidad.

2. ALCANCE

Aplica al procedimiento "*PR-IIT-0458 Gestión de incidentes*".

3. DEFINICIONES Y SIGLAS

- **Administrador de los sistemas de seguridad digital**. funcionario encargado de lograr la exactitud, integridad y protección de todos los procesos y recursos de los sistemas de información

  Fuente. https://es.wikipedia.org/wiki/Administraci%C3%B3n_de_seguridad

- **Confidencialidad**. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

  Fuente. NTC ISO/IEC 27000. Sistemas de Gestión de la Seguridad de la información. 2013

- **Contención de incidentes de seguridad digital**. Busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI.

  Fuente. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- **Correlación de eventos**. Nos permite descubrir y aplicar asociaciones lógicas entre eventos. Estos eventos pueden pertenecer a cualquier tipo de registro o recolección, incluso individuales o dispares.

  Fuente. Https://www.gb-advisors.com/es/correlacion-de-eventos-y-su-importancia-en-la-recoleccion-de-datos/

- **Disponibilidad**. Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

  Fuente: NTC ISO/IEC 27000. Sistemas de Gestión de la Seguridad de la información. 2013.

- **Endurecimiento del sistema (hardening)**. es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuantas más funciones desempeña.

  Fuente. Https://es.wikipedia.org/wiki/Endurecimiento_(inform%C3%A1tica)

- **Firewall (Cortafuegos)**. Es un dispositivo de seguridad de red, que monitorea el tráfico de red entrante y saliente, y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. Establecen una barrera entre las redes internas seguras y controladas que pueden ser confiables y no confiables fuera de las redes, como Internet.
  Fuente. https://www.cisco.com

- **Gestión de incidentes de seguridad de la información**. Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

  Fuente. Https://www.novasec.co/en/blog/62-gestion-integral-de-la-seguridad-de-la-informacion

- **Herramienta de seguridad digital**. Elemento de hardware y/o software utilizado para controlar los accesos a la red, proteger el flujo de información sensible y prevenir los ataques maliciosos dirigidos a sistemas de telecomunicaciones, de transporte de información y del contenido de las comunicaciones.

  Fuente. https://revista.seguridad.unam.mx/numero29/evolucion-herramientas-seguridad-ies

- **Incidente**. Interrupción no planificada de un Servicio de TI o reducción en la calidad de un servicio de TI. También lo es el fallo de un elemento de configuración que no ha impactado todavía en el servicio. Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción de este o una reducción de la calidad de dicho servicio.

  Fuente. ITIL® Glossary v01, 1 May 2006: Acronyms / Plan estratégico de tecnología de la información y comunicaciones – PETIC (2015-2018) UAE DIAN.

- **Incidente de seguridad digital**. un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

  Fuente. Norma Técnica Colombiana NTC-ISO/IEC 27001 2006-03-22

- **Incidentes de Alto Impacto**. El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Instituto. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

  Fuente. Https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- **Incidentes de Medio Impacto**. El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

  Fuente. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- **Incidentes de Bajo Impacto**. El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

  Fuente. Https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- **Integridad**. Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

  Fuente. NTC ISO/IEC 27000. Sistemas de Gestión de la Seguridad de la información. 2013

- **Mesa de servicio**. Es un equipo de trabajo, punto de contacto entre los usuarios de la empresa y las tecnologías estándares adoptadas por la misma, y cuyo objetivo principal será responder de una manera oportuna, eficiente y con alta calidad a las peticiones que dichos usuarios realicen, en relación con los diversos aspectos de la Tecnología de la Información.

  Fuente. Https://arandasoft.com/la-funcion-de-una-mesa-de-ayuda-dentro-de-la-organizacion/

- **Plataforma de seguridad digital**. Todos los aspectos y mecanismos que pueden emplearse para asegurar los datos privados que circulan a través de redes informáticas

  Fuente. Https://www.tecnologia-informatica.com/seguridad-informatica/

4. DESARROLLO DEL TEMA

4.1 Generalidades

- La Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, tendrá conocimiento total sobre los comportamientos de la infraestructura que está administrando, sobre las características normales a nivel de red y de los sistemas.

- Todos los colaboradores DIAN y contratistas deben reportar a través de la herramienta de gestión de la mesa de servicio los siguientes eventos que inciden en la seguridad de la información de la entidad:

  a) Control de seguridad ineficaz;
  b) Incumplimiento de las expectativas de integridad, confidencialidad o disponibilidad de la información;
  c) Errores humanos;
  d) Incumplimiento de políticas o directrices;
  e) Incumplimientos de los acuerdos de seguridad física;
  f) Cambios incontrolados del sistema;
  g) Mal funcionamiento del software o hardware;
  h) Infracciones de acceso.

- La información necesaria para realizar el análisis de incidentes debe estar centralizada (Logs de servidores, redes, aplicaciones).

- El equipo de respuesta a incidentes de seguridad digital (Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces) atenderá en primera instancia todos los incidentes de seguridad digital detectados a través de las actividades de monitoreo y control de los servicios informáticos, las bases de datos, los sistemas de comunicaciones y demás infraestructura tecnológica que soporta las soluciones tecnológicas de la entidad.

- En segunda instancia este mismo equipo será el encargado de solucionar de fondo los incidentes contingentes que sean reportados por otras áreas o personas y que afecten la infraestructura tecnológica.

- Para la administración de las herramientas de seguridad digital se tendrán en cuenta los sistemas operativos, niveles de seguridad instalados, tipos y topologías de redes utilizadas, conexiones a redes externas a la entidad, servidores de uso interno y externo, configuración de los servicios, barreras de protección y su arquitectura.

- Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.

- El Oficial de Seguridad de la Información establece la frecuencia y tipo de reportes requeridos para el monitoreo, control, mantenimiento, alerta y gestión de incidentes de seguridad digital detectados e identificados por las herramientas de seguridad digital.

4.2 Descripción de actividades

4.2.1 Realizar monitoreo y mantenimiento a las herramientas de seguridad digital

El administrador de sistemas de seguridad digital monitorea las herramientas destinadas para este fin, con el fin de identificar y localizar debilidades, detectar software malicioso que puede ser transmitido mediante el uso de comunicaciones electrónicas, incidentes y/o problemas de seguridad digital, así como detectar oportunamente señales de ataque.

Los siguientes elementos se tienen en cuenta para el análisis en el funcionamiento de la herramienta y localización de incidentes:

- Caídas de servidores
- Software antivirus dando informes
- Logs de servidores.
- Logs de aplicaciones.
- Logs de herramientas de seguridad.
- Cualquier otra herramienta que permita la identificación de un incidente de
- seguridad.
- Reporte del oficial de seguridad
- Informes de mantenimiento

4.2.2 Detectar o recibir incidente de seguridad digital

Los incidentes pueden identificarse mediante monitoreo de las herramientas de seguridad digital o por los usuarios de los diferentes procesos con base en:

- Alertas en sistemas de seguridad.
- Reportes de usuarios en la herramienta de gestión de la mesa de servicio
- Gestión de la mesa de servicio.
- Otros funcionamientos fuera de lo normal del sistema.
- Reporte del oficial de seguridad remitidos por correo electrónico.

Se recolecta la evidencia del incidente tan pronto como sea posible después de la ocurrencia; cuando el incidente de seguridad digital es detectado por los usuarios, se debe adjuntar la evidencia en el registro del caso en la herramienta de gestión de la mesa de servicio.

4.2.3 Realizar contención del incidente

El administrador de sistemas de seguridad digital de la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, detiene el incidente con el fin de que no se propague y pueda generar daños a la información o a la arquitectura de TI, para facilitar esta tarea, la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, ha contemplado acciones inmediatas como, por ejemplo: apagar equipos, desconectar de la red el(los) equipo(s) afectado(s), deshabilitar servicios.

4.2.4 Analizar el incidente

El administrador de sistemas de seguridad digital de la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, tiene en cuenta las coincidencias con casos presentados anteriormente, realiza análisis forense de seguridad digital según sea necesario, se efectúa correlación de eventos para descubrir patrones de comportamiento anormal y poder identificar de manera más ágil la forma eliminar el incidente. A partir de la base de conocimiento, la información sobre nuevas vulnerabilidades, información de los servicios habilitados y experiencias con incidentes anteriores, se identifican causas del incidente con el fin prevenir su recurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios.

4.2.5 Clasificar el incidente

El administrador de sistemas de seguridad digital de la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, clasifica el incidente con el fin de darle un tratamiento adecuado y contenerlo en el menor tiempo posible, los incidentes de seguridad digital se clasifican como incidentes de alto impacto, incidentes de medio impacto o incidentes de bajo impacto. Esta clasificación se efectúa evaluando la criticidad, la cobertura del incidente y la afectación de la operación normal de un sistema de información que tenga relación con el contribuyente.

La criticidad del incidente se establece considerando los riesgos generados en relación con el cumplimiento de la misión de la entidad. La cobertura se determina considerando la afectación en las bases de datos, en la red de comunicaciones y los sistemas de información, así como evaluando el impacto a nivel de proceso y a nivel de direcciones seccionales.

- Si el incidente se clasifica de **bajo impacto**, se establece un tiempo máximo de atención, dejando registro de este en la herramienta de gestión de la mesa de servicio y se escala al responsable técnico respectivo.

- Si el incidente se clasifica de **medio impacto**, se define la posible solución según la falla identificada, apoyándose en los especialistas correspondientes de acuerdo con su competencia: bases de datos, sistemas operativos, construcción de los sistemas de información, estabilización o estabilización básica. Se registra la solución en la herramienta de gestión de la mesa de servicio, y se estima el tiempo máximo de respuesta.

- Si el incidente se clasifica de **alto impacto**, se informa al Director de Gestión de Innovación y Proyectos o quien haga sus veces, a los Directores de Gestión, Directores seccionales,

Subdirectores de Gestión, Oficina de Seguridad de la Información, Jefes de Coordinaciones, Jefes de Divisiones, Jefes de GIT, sobre la ocurrencia del incidente y el impacto que tendrá en los diferentes procesos, mediante mensaje institucional (correo electrónico, chat institucional). Dependiendo del impacto del incidente a nivel Software si se prevén medidas de protección al usuario por la no disponibilidad de las soluciones tecnológicas, se informa al Director de Gestión de Innovación y Proyectos o quien haga sus veces y se genera el reporte de inconvenientes técnicos en las soluciones tecnológicas. Se define la posible solución (descrita en el impacto medio) y se estima el tiempo máximo de respuesta.

4.2.6 Erradicar el incidente

Se realiza una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso o accesos no autorizados, registrando la acción en la herramienta de gestión de la mesa de servicio. Se informa la realización de la actividad al administrador de la herramienta de seguridad digital.

4.2.7 Recuperar el servicio

Se restablece la funcionalidad de las soluciones tecnológicas y/o servicios afectados y se realiza un endurecimiento del sistema que permita prevenir incidentes similares en el futuro. Se describe la solución generada al incidente de seguridad digital reportado en la herramienta de gestión de solicitudes de la mesa de servicio, se cierra el caso informando la normalización del servicio.

Se documentan las lecciones aprendidas después de un incidente de alto impacto, y periódicamente después de los incidentes impacto medio y bajo, alimentando la base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados y experiencias con incidentes anteriores, con el fin de la mejora de las medidas de seguridad y el proceso de gestión de incidentes.

4.2.8 Comunicar a las partes interesadas

A través de medios de comunicación como intranet, la página web o mediante correos electrónicos y/o dando respuesta al incidente en la herramienta de gestión de la mesa de servicio, se mantienen informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad digital.

5. CONTROL DE CAMBIOS

Versión	Vigencia Desde	Hasta	Descripción de Cambios
1	10/09/2021		Versión inicial.

Elaboró:	Yenny Paola Ostos Mendivelso **Elaboración técnica**	Analista II de tecnología	Subdirección de Innovación y Proyectos
	Juan Pablo Serna Botero **Elaboración técnica**	Gestor IV de tecnología	Subdirección de Innovación y Proyectos

	Juan Carlos Vizcaino Novoa **Elaboración técnica**	Inspector IV	Subdirección de Infraestructura Tecnológica y de Operaciones
	Alfredo Antonio Ahumada Ahumada **Elaboración Metodológica**	Gestor II del Sistema de Gestión	Coordinación de Organización y Gestión de Calidad
	Tito Alejandro Menjura Murcia **Elaboración Metodológica**	Gestor II del Sistema de Gestión	Coordinación de Organización y Gestión de Calidad
Revisó:	Héctor Leonel Mesa Lara	Subdirector de Infraestructura Tecnológica y de Operaciones	Subdirección de Infraestructura Tecnológica y de Operaciones
Aprobó:	Diana Parra Silva	Directora de Gestión de Innovación y Proyectos	Dirección de Gestión de Innovación y Proyectos