PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD DEL ATLÁNTICO

OFICINA DE GESTIÓN TECNOLÓGICA E INFORMACIÓN

TABLA DE CONTENIDO

Contenido

INTRODUCCION

El Plan de seguridad y privacidad de la información es un documento estratégicos que aborda la necesidad de un sistema de gestión para la seguridad de la información en el proceso de Gestión Tecnológica y Comunicaciones en la Universidad del Atlántico. Para la mejora continua de esta gestión es necesario transmitir a la comunidad universitaria niveles de concientización, compromiso y prevención en el buen uso de los recursos públicos utilizados con base en la legislación y normatividad vigente referente a la Seguridad de la Información.

La Universidad del Atlántico implementa las mejores prácticas de la seguridad de la Información con base en el análisis de la misión, visión, metas institucionales y el manual de Seguridad y Políticas de la información con el fin de tomar acciones para el mejoramiento continuo, protección de los activos de información para minimizar riesgos que afecten la continuidad de la institución.

En el presente anexo se muestra la política de seguridad de la información.

1. DIRECTRIZ DE SEGURIDAD

La Alta dirección de la **UNIVERSIDAD DEL ATLÁNTICO**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un **Sistema de Gestión de Seguridad de la Información** buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de nuestra institución. Para la **UNIVERSIDAD DEL ATLÁNTICO** la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con el objeto de mantener un nivel de exposición que permita responder por altos niveles de confiabilidad, integridad y disponibilidad en los sistemas de información al servicio de la comunidad universitaria y grupos de interés, mediante la implementación de estándares internacionales de seguridad de información y buenas prácticas.

El establecimiento, implementación, mantenimiento y mejora continua de la Política de Seguridad de la Información garantiza un compromiso y concientización ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad logrando la mejora continua en los procesos acorde al Plan Estratégico Institucional.

La Política de Seguridad de la Información en el proceso de Gestión Tecnológica y Comunicaciones es la declaración general que representa la posición de la administración de la UNIVERSIDAD DEL ATLÁNTICO con respecto a la protección de los activos de información (personas, procesos y las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información apoyado las normativas vigentes, políticas y manuales para la seguridad de la información.

2. OBJETIVO

La Universidad del Atlántico, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a los valores institucionales, establece la función de Seguridad de la Información en la Institución, con el objetivo de:

- Brindar orientación y soporte, por parte de la alta dirección, para la seguridad de la información de acuerdo con los requisitos de la institución y con las leyes y reglamentos pertinentes

- Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la institución

- Asegurar que los funcionarios, contratistas y proveedores comprenden sus responsabilidades, sean idóneos en los roles asignados, cumplan sus compromisos de la seguridad de la información, protegiendo los intereses de la institución como parte del proceso de actualización o terminación de empleo o contrato

- Identificar y asegurar los activos de información organizacionales y definir las responsabilidades de protección apropiadas, de acuerdo con su importancia para la institución

- Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios

- Garantizar la seguridad de las operaciones controlando y documentando los cambios institucionales, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la seguridad de la información

- Mantener la seguridad de la información en el proceso de Gestión Tecnológica y de Comunicaciones, estableciendo políticas, procedimientos y controles de transferencia formales en la institución y las partes externas

- Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también

los requisitos para sistemas de información que prestan servicios sobre redes publicas

- Mantener el nivel acordado de seguridad en la información y protección de los activos de la institución con los proveedores

- Mantener e incrementar los niveles de confianza de la comunidad universitaria, clientes, proveedores y grupos de interés

- Garantizar la continuidad de la actividad de la institución frente a incidentes

- Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación, contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad

3. ALCANCE

El presente documento es de aplicación a toda la comunidad universitaria, dependencias que componen la institución, a sus recursos, a la totalidad de los procesos internos o externos vinculados al proceso de Gestión Tecnológica y de Comunicaciones, a través de contratos o acuerdos con terceros y a todo el personal de la Universidad del Atlántico y la ciudadanía en general, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Las responsabilidades frente a la seguridad de la información serán definidas, difundidas, publicadas y aceptadas por la comunidad universitaria.

La Universidad del Atlántico protegerá la información generada, procesada o resguardada por el proceso de Tecnología y Comunicaciones, Servicio TI y activos de información estableciendo controles a los riesgos que se generan de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

La Universidad del Atlántico protegerá la información creada, procesada, transmitida o resguardada por sus procesos de la organización, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La Universidad del Atlántico protegerá su información de las amenazas originadas por parte de las personas vinculadas (Administrativos, docentes, contratistas y otros) y con compromisos contractuales con la institución

- La Universidad del Atlántico protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos

- La Universidad del Atlántico controlará la operación de sus procesos institucionales garantizando la seguridad de los recursos tecnológicos y las redes de datos

- La Universidad del Atlántico implementará control de acceso a la información, sistemas y recursos de red

- La Universidad del Atlántico garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información

- La Universidad del Atlántico garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora continua y efectiva de su modelo de seguridad

- La Universidad del Atlántico garantizará la disponibilidad de sus procesos institucionales y la continuidad de su operación basada en el impacto que pueden generar los incidentes

- La Universidad del Atlántico garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

- La Universidad del Atlántico realizará seguimiento y actualización de la presente política y lineamientos cuando se identifiquen cambios de estructura, objetivos o alguna condición que afecte la política, con el fin de asegurar que se encuentren ajustadas a los requerimientos institucionales

4. MARCO NORMATIVO

Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. - Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. - Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1581 de 2012, Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente Ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento." - Ley 1581 de 2012, Artículo 17, ítem d: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"

Ley 1712 de 2014, "principio de transparencia": "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta Ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la Ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta Ley."

Decreto 1413 de 2017, "Seguridad de la información." "Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información

certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."

5. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

La Universidad del Atlántico garantiza el liderazgo y compromiso al cumplimientos de los requisitos según la norma ISO/IEC 27001:2013 en el proceso de establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada ***Comité Gestor de Seguridad de la Información*** cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- **Jefe de la Oficina de planeación o un delegado**
- **Jefe Talento Humano o un delegado**
- **Jefe de la Oficina de Gestión Tecnológica e Información**
- **Jefe de Jurídica o un delegado**
- **Jefe de control interno o un delegado**
- **Jefe de gestión ambiental o un delegado**
- **Equipo de trabajo Gestión tecnológica e información (Calidad, seguridad)**
- **Secretario General o un delegado – Gestión documental**
- **Jefe Calidad integral de docencia o un delegado**
- **Jefe de Gestión de compras y contratación o un delegado**
- **Oficial de seguridad de la información**

Este comité, deberá revisar y si se requiere actualizar anualmente la política de seguridad de la información, presentando las propuestas acordes al plan estratégico institucional. Las funciones del Comité Gestor de Seguridad de la Información son:

- Establecimiento, implementación, mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información

- Establecer la Política de seguridad de la información y los objetivos de la seguridad de la información

- Asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos del Sistema Integrado de Gestión SIG

- Asegurar los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles

- Asegurar que el sistema de gestión de la seguridad de la información logre los resultados previstos

- Comunicar la importancia de una gestión de seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de seguridad de la información

- Promover la mejora continua

6. RESPONSABILIDADES

Los propietarios de los riesgos.
Previa identificación y valoración de sus activos de información, hacen parte de los líderes de procesos que son responsables de Seguridad de la Información en sus dependencias, oficinas y entornos a su cargo, por lo tanto ***deben*** seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías, manuales y procedimientos recomendados por el Comité Gestor de Seguridad de la Información y aprobados por la Alta Dirección.
Son responsables de la clasificación, mantenimiento y actualización de los sistemas de información; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener acceso a la información de acuerdo a sus perfiles, funciones y competencia. En general, tienen la responsabilidad de mantener la integralidad, confidencialidad y disponibilidad de los activos de información durante su ciclo de vida

El **Coordinador del Comité de Seguridad de la Información.**
Será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política. Convocar y presidir las reuniones del Comité Gestor de Seguridad de la Información.

Equipo de Planificación de Seguridad de la Información.

Durante el establecimiento y creación del Comité Gestor de Seguridad de la Información se conformará un equipo de Líderes del SGSI y el CIO que trabajarán entre departamentos y resolverán conflictos relacionados con la seguridad de la información.

Los Líderes de Procesos.
Responsables de Seguridad Informática Responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité Gestor de Seguridad de la Información.
Cada jefatura determinará el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Jefe de Compras y Contratación y el Jefe de Infraestructura Física y Servicios Generales).

Jefe de Oficina de Planeación – Direccionamiento estratégico
Cumplirá las funciones de liderar y direccionar los planes estratégicos en el diseño, elaboración y coordinación asociados con las políticas de la seguridad de la información de la universidad del Atlántico, realizará seguimiento a los planes de acción implementados en las políticas de seguridad de la información.

Jefe de Talento Humano - Gestión del Talento Humano
Cumplirá la función de verificar la documentación aportada por el personal que será contratado, notificar a todo el personal que se vincula contractualmente con la Universidad del Atlántico, de las obligaciones, acuerdos y compromisos respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, instructivos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de las actualizaciones que en ella se produzcan a todo el personal, a través de acuerdos de *Confidencialidad* y de tareas de capacitación, sensibilización continua en materia de seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información, según lineamientos dictados por el Comité Gestor de Seguridad de la Información.

Jefe de la Oficina de Gestión tecnológica e información - Gestión tecnológica y comunicaciones
Debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración,

comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad.

Jefe de la Oficina Jurídica – Gestión jurídica
Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Así mismo, asesorará en materia legal a la entidad en lo que se refiere al cumplimiento de la normatividad nacional vigente con respecto a la seguridad de la información.

Oficina de Control Interno - Gestión de Control interno
Es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

Líder gestión Ambiental.
Interesado en motivar a otros individuos del entorno universitario, al objetivo de configurar una cultura ética institucional y hacer promoción de la Seguridad de la Información y proyectos integrales acordes al Plan de Acción Ético institucional.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

Equipo de trabajo de Gestión tecnológica e información
Será el encargado de dar apoyo en los conceptos técnicos concernientes a las decisiones tomadas en el comité gestor de seguridad de la información con respecto a cambios o actualizaciones en las políticas de la seguridad de la información.

Secretario General o un delegado – Gestión documental
Cumplirá la función de brindar las estrategias, velar y resguardar la gestión documental al mismo tiempo emitir y reguardar las actas generadas en el comité de seguridad de la información, haciendo el tratamiento de los mismo para evitar la divulgación a personal no autorizado, y realizando la gestión documental que requieran los integrantes del comité de seguridad de la información, realizar capacitación de manejo de información generada a los integrantes del comité.

Jefe Calidad integral de docencia o un delegado – Gestión docencia

Apoyar en la planeación, metodología y estrategia de la divulgación de los temas concernientes a las políticas de seguridad de la información de la universidad del Atlántico en la comunidad universitaria.
Apoyar con estrategias de promuevan la constante actualización de las políticas de seguridad de la información de la universidad del Atlántico e identificar riesgos que puedan afectar el logro del proceso.

Gestión de compras y contratación o un delegado – Gestión de Bienes y servicios
Sera encargado de llevar el inventario de equipos tecnológicos y de comunicaciones propios de la Universidad del Atlántico, de su actualización y llevar el control de equipos retirados o dados de baja.
Llevar el control de la salida e ingreso de los equipos que se encuentran en el inventario de equipos tecnológicos y de comunicaciones.

Personal de la Universidad.
Todo el personal de la Universidad del Atlántico, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional. Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por la **Oficina de Gestión Tecnológica e Información**, en cuanto a la información y **la red de datos** , en cuanto a los dispositivos hardware y los elementos de software.

Estudiantes.
Para poder usar los recursos de TI de la Universidad del Atlántico, los estudiantes deben poseer matricula financiera y académica, conocer y aceptar en cada matrícula de semestre un acuerdo con los términos y condiciones en cuanto a seguridad y política de protección de datos personales sensibles. **El Departamento de Admisiones y Registro** deben asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros.

Usuarios Externos.
Todos los usuarios externos y personal de empresas externas que deban ingresar a los centros de cableado o utilicen bases de datos deben estar autorizados por La Oficina de Gestión Tecnológica e Información, quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales, los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las credenciales de acceso al sistema (usuarios externos) cuales deben ser de perfiles específicos y tener caducidad no superior a ***la vigencia contractual***, renovables de acuerdo a la naturaleza del usuario.

7. SEGURIDAD INSTITUCIONAL

Toda persona que ingresa como usuario nuevo a la Universidad del Atlántico para utilizar equipos de cómputo y emplear servicios informáticos debe aceptar las condiciones de confidencialidad, del buen uso de los recursos tecnológicos y de información, así como cumplir los lineamientos y compromisos consignados en esta política y en el Manual de Seguridad y Políticas de Informática.

1.1 **Usuarios Nuevos.** Todo el personal nuevo de la Institución, deberá ser reportado por su jefe inmediato, interventor o supervisor del contrato al Departamento de Talento Humano quien es el ente facultado para reportar novedades y actualizaciones del personal (administrativo, contratistas, docentes tiempo completo/ocasional, monitores y otros) vinculado a la Universidad del Atlántico, debe reportar a la Oficina de Informática, para que asigne las herramientas y derechos correspondientes para el buen desarrollo de su objeto contractual (equipo de cómputo, recursos tecnológicos, cuentas de usuario y/o credenciales para acceder a los sistemas de información) o en el caso de cambio o retiro del cargo, revocar las credenciales de acceso al sistema.

1.2 **Comunicación o información en Seguridad Información y Manual de Funciones.** Todo servidor o funcionario nuevo en la Universidad del Atlántico deberá informarse sobre las Políticas, Estándares y el **Manual de Seguridad y Políticas de Informática**, donde se dan a conocer los compromisos, responsabilidades, obligaciones para los usuarios y las sanciones que pueda incurrir en caso de incumplimiento.

8. PLAN DE IMPLEMENTACIÓN DEL MSPI

Basado en el diagrama presentado en el MSPI (Modelo de seguridad y privacidad de la información) publicado por el MINTIC, se elabora el plan de implementación que se muestra a continuación.

Gestión	Actividades	Tareas	Responsable
Activos de información	Definir formato para levantamiento de los activos de información de las dependencias	Creación de la metodología y del instrumento para el levantamiento de activos de información de los procesos de cada dependencia	Jefe de la Oficina de Gestión tecnológica e información o un delegado, gestión documental y gestión de bienes y servicios

		Identificar y citar a los gestores de proceso de cada dependencia y realizar un acta	Jefe de la Oficina de Gestión tecnológica e información o un delegado
	Realizar el levantamiento de los activos de información	Registro o actualización de los activos mediante el uso del formato creado en la actividad anterior, para su identificación y valoración	Jefe de cada dependencia o personas delegadas por los mismos
		Identificar o actualizar los activos de información de las dependencias.	Jefe de cada dependencia o personas delegadas por los mismos
		Compilar, validar y aceptar los activos de información para su publicación a cargo de cada líder de proceso (análisis cualitativo) (publicación y registro según ley 1712 de 2014)	Jefe de cada dependencia o personas delegadas por los mismos con el aval de la oficina jurídica y la oficina de Gestión tecnológica e información
	Revisión de datos personales	Reportar al líder de la oficina de Gestión tecnológica e información o al encargado de la seguridad de la información, los activos recolectados en el formato que correspondan a base de datos	Jefe de cada dependencia o personas delegadas por los mismos
	Publicación y registros de los activos de información según ley 1712 de 2014	Publicar los instrumentos de activos de la información consolidados (análisis cuantitativo)	

Gestión	Actividades	Tareas	Responsable
Gestión de riesgos	Revisión de lineamientos de riesgos	Revisar política y metodología, declaración de aplicabilidad de gestión de riesgos	Equipo de planificación de seguridad de la información
	Socialización	Socialización plan, Modelo de Seguridad y privacidad de la Información y plan de Continuidad de la operación	Jefe de la oficina Gestión tecnológica e información o un delegado
	Identificación de riesgos de seguridad y privacidad de la información	Convocar gestores de los procesos a reunión de análisis de riesgos y realizar el acta	Jefe de la oficina de Gestión tecnológica e información o un delegado
		Identificación, análisis, aceptación, aprobación y evaluación de riesgos - seguridad y privacidad de la información y realizar plan de tratamiento, si aplica	Jefe de cada dependencia o personas delegadas por los mismos
	Seguimiento a la fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Jefe de cada dependencia o personas delegadas por los mismos
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Jefe de cada dependencia o personas delegadas por los mismos
	Plan de mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Jefe de cada dependencia o personas delegadas por los mismos
		Actualización guía gestión de Riesgos Seguridad de la información, de acuerdo a los cambios que sean solicitados	Equipo de planificación de seguridad de la información
	Monitoreo y revisión	Seguimiento de indicadores	Equipo de planificación de seguridad de la información

Gestión	Actividades	Tareas	Responsable
Gestión de incidentes de	Seguimiento de incidentes de seguridad de la información	Seguimiento de incidentes de seguridad de la información	Jefe de cada dependencia o personas delegadas por los mismos

seguridad de la información		Socializar incidentes	Jefe de cada dependencia o personas delegadas por los mismos
	Gestionar los incidentes de seguridad de la información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Jefe de cada dependencia o personas delegadas por los mismos
Acciones correctivas y oportunidades de mejora SGSI	Reporte del estado de las acciones correctivas y oportunidades de mejora	Seguimiento de las acciones correctivas y oportunidades de mejora	Jefe de cada dependencia o personas delegadas por los mismos
Planeación	Revisión de políticas de seguridad de la información	Actualizar Manual Políticas de Seguridad de la Información	Equipo de planificación de seguridad de la información
Gobierno digital	Gobierno digital	Actualizar el Plan de Seguridad y Privacidad de la Información.	Jefe de la oficina de Gestión tecnológica e información o un delegado
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Equipo de planificación de seguridad de la información
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Equipo de planificación de seguridad de la información

9. CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes se clasifican según la naturaleza de la amenaza y el impacto potencial en los sistemas, datos o usuarios de la institución educativa.
continuación te muestro una tabla con las categorías principales y ejemplos para cada una. Luego, tú me dirás con cuáles quieres trabajar más a fondo:

Categoría de Incidente	Descripción	Ejemplos en un entorno educativo
Malware / Ransomware	Software malicioso que compromete sistemas, bloquea archivos o roba información.	Ransomware en servidores de notas; virus en PCs del laboratorio.
Phishing / Ingeniería social	Engaños dirigidos a usuarios para robar credenciales u obtener acceso.	Correos falsos pidiendo ingresar al LMS (Moodle, Canvas, etc.).
Acceso no autorizado	Ingreso a sistemas sin permiso, por ataque externo o abuso interno.	Un alumno accede al sistema de calificaciones de otro estudiante.

Fuga o pérdida de información	Exposición de datos personales, académicos o administrativos.	Filtración de bases de datos con nombres, calificaciones o direcciones de correo.
Denegación de servicio (DoS/DDoS)	Ataques que hacen caer o vuelven inaccesibles los servicios digitales.	DDoS al sitio web institucional o portal de estudiantes.
Explotación de vulnerabilidades	Uso de fallas técnicas para comprometer sistemas.	Ataques a servidores desactualizados o sin parches.
Abuso de privilegios / cuentas internas	Uso indebido de accesos legítimos por parte de personal o alumnos.	Un docente modifica notas sin autorización.

Categoría Malware / Ransomware

Este es uno de los ataques más comunes y peligrosos en instituciones educativas, especialmente en servidores, PCs de laboratorios o laptops del personal.

Detección del incidente

¿Qué buscar?

- Computadoras que muestran mensajes de bloqueo o cifrado.
- Archivos renombrados con extensiones extrañas (.locky, .encrypted, etc.).
- Equipos lentos o con procesos sospechosos.
- Alertas del antivirus o del sistema de monitoreo (SIEM, EDR).

¿Quién puede detectarlo?

- Usuarios finales (docentes, estudiantes, TI).
- Sistemas automáticos de detección (antivirus, EDR, SIEM).
- Soporte técnico al recibir quejas.

Acciones iniciales:

- Registrar la hora y fecha del comportamiento extraño.
- Notificar al equipo de soporte TI o al CSIRT (si existe).
- No apagar el equipo (puede perderse evidencia).

- Análisis y validación

Objetivo: Confirmar si realmente hay una infección y qué tipo es.

Pasos:

- Revisar alertas de antivirus y logs del sistema.
- Verificar si el malware está activo o si ya cifró datos.
- Determinar si el incidente es aislado o afecta a más dispositivos.
- Identificar cómo se propagó (correo, USB, red).

Herramientas útiles:

- Antivirus/EDR (Ej: SentinelOne, Windows Defender).
- SIEM para correlación de eventos.
- Análisis manual del tráfico de red.

Contención del incidente

Objetivo: Detener la propagación del malware.

Acciones inmediatas:

- **Desconectar el equipo afectado de la red (WiFi o cable).**
- Bloquear puertos USB si el contagio fue por medios físicos.
- Restringir el acceso a carpetas compartidas o servidores infectados.
- Revisar otros dispositivos en la misma red.

Si hay más equipos comprometidos:

- Aislar la subred completa o el segmento del laboratorio.
- Bloquear dominios o IPs relacionados con el malware.

Erradicación

Objetivo: Eliminar por completo el malware.

Pasos:

- Ejecutar antivirus actualizado en modo seguro.
- Eliminar archivos infectados o sospechosos.
- Cambiar contraseñas asociadas a cuentas en el equipo.
- Si el sistema está muy comprometido: formatear y reinstalar.

Revisión:

- Verificar si hay scripts persistentes en el inicio.
- Revisar si el malware dejó puertas traseras (backdoors).

Recuperación

Objetivo: Volver a operaciones normales, asegurando el entorno.

Pasos:

- Restaurar archivos desde backups seguros (previos al ataque).
- Validar integridad del sistema operativo y software.
- Reconectar el equipo a la red de forma controlada.
- Monitorear comportamiento por al menos 48 horas.

Lecciones aprendidas

Objetivo: Evitar que vuelva a ocurrir el mismo incidente.

Análisis post-incidente:

- ¿Cómo se introdujo el malware?
- ¿Qué controles fallaron?
- ¿Qué impacto tuvo?

Medidas de mejora:

- Capacitación a usuarios sobre archivos sospechosos.
- Actualización de antivirus en todos los equipos.
- Refuerzo de políticas de backups regulares.
- Bloqueo de correos o dominios maliciosos conocidos

.

Categoria : Phishing / Ingeniería Social

Este tipo de ataque busca engañar a usuarios (estudiantes, docentes, administrativos) para que entreguen sus credenciales, descarguen malware o den acceso a sistemas sensibles. Es una de las causas más comunes de incidentes en instituciones educativas.

Detección del incidente

¿Qué buscar?

- Correos sospechosos que aparentan ser de la institución (suplantación).
- Enlaces o archivos adjuntos desconocidos.
- Páginas falsas que imitan el login del correo, LMS o sistema de notas.
- Usuarios que reportan haber entregado su contraseña.

¿Quién puede detectarlo?

- Usuarios que reciben correos extraños.
- Soporte técnico al recibir múltiples reportes.
- Sistemas de correo con filtros (Microsoft 365, Gmail, etc.).

Acciones iniciales:

- No hacer clic en enlaces ni descargar archivos.
- Tomar captura del correo y encabezados.
- Reportar inmediatamente a TI / seguridad.

Análisis y validación

Objetivo: Confirmar que se trata de un ataque y no de un falso positivo.

Pasos:

- Verificar si el correo proviene de un dominio falso (ej. @univer5idad.edu en lugar de @universidad.edu).
- Revisar el enlace: ¿lleva a una página legítima o a una copia falsa?
- Confirmar si otros usuarios recibieron el mismo mensaje.
- Validar si hay registros de accesos extraños a cuentas institucionales.

Herramientas útiles:

- Analizadores de encabezados de correo.

- Verificadores de reputación de dominios (VirusTotal, etc.).
- SIEM o logs de correo.

Contención del incidente

Objetivo: Limitar el daño y evitar que más usuarios sean engañados.

Acciones inmediatas:

- Bloquear el remitente y los enlaces en el servidor de correo.
- Enviar un aviso masivo alertando sobre el mensaje falso.
- Forzar cambio de contraseña a usuarios que hicieron clic o entregaron credenciales.
- Bloquear IPs o sesiones sospechosas desde donde se accedió a las cuentas.

Erradicación

Objetivo: Eliminar la amenaza y evitar su persistencia.

Pasos:

- Eliminar los correos maliciosos aún no abiertos desde el servidor.
- Revocar tokens de sesión activos para cuentas comprometidas.
- Cambiar preguntas de seguridad, activar MFA (autenticación multifactor) si es posible.
- Revisar si las cuentas comprometidas fueron usadas para enviar más phishing.

Recuperación

Objetivo: Restaurar el acceso seguro a los servicios y corregir configuraciones afectadas.

Pasos:

- Restaurar configuraciones de seguridad en cuentas afectadas.
- Reestablecer el acceso de forma segura a plataformas educativas.
- Reforzar filtros de correo para prevenir nuevos ataques.
- Verificar si hubo movimiento lateral (acceso a otras áreas o datos internos).

Lecciones aprendidas

Objetivo: Prevenir incidentes similares en el futuro.

Acciones recomendadas:

- Campañas de concienciación en ciberseguridad para toda la comunidad educativa.
- Simulacros de phishing para entrenar a los usuarios.
- Configuración avanzada de filtros anti-phishing.
- Revisión de políticas de seguridad en el correo institucional**.**

Categoría: Acceso no autorizado / Intrusión

Este tipo de incidente ocurre cuando una persona (interna o externa) logra ingresar a un sistema o recurso sin los permisos necesarios. Puede comprometer datos sensibles o alterar sistemas críticos (como el sistema de notas o el portal de estudiantes).

Detección del incidente

¿Qué buscar?

- Accesos desde ubicaciones geográficas inusuales.
- Cambios no autorizados en sistemas (notas, cuentas, archivos).
- Ingresos fuera de horario habitual (por ejemplo, de madrugada).
- Múltiples intentos fallidos de inicio de sesión.
- Usuarios que reportan que sus cuentas fueron "usadas sin ellos".

¿Quién puede detectarlo?

- Administradores de sistemas (revisión de logs).
- Usuarios que reportan actividad no reconocida.
- Herramientas de monitoreo (SIEM, autenticación con alertas).

Acciones iniciales:

- Documentar los síntomas y cuándo empezaron.
- Notificar al equipo de TI o CSIRT.
- No cerrar la sesión sin antes recopilar evidencia.

Análisis y validación

Objetivo: Confirmar que hubo acceso indebido, y determinar su alcance.

Pasos:

- Revisar logs de acceso (direcciones IP, horas, dispositivos).
- Verificar actividad reciente del usuario (archivos abiertos, cambios realizados).
- Validar si las credenciales fueron robadas o adivinadas.
- Determinar si el acceso se extendió a otras cuentas o sistemas.

Herramientas útiles:

- Logs del sistema (servidores, LMS, correo).
- SIEM / UBA (User Behavior Analytics).
- Correlación de eventos y patrones de comportamiento.

Contención del incidente

Objetivo: Detener el acceso indebido y evitar su expansión.

Acciones inmediatas:

- Deshabilitar temporalmente las cuentas comprometidas.
- Bloquear direcciones IP o dispositivos sospechosos.
- Cambiar contraseñas y revocar tokens de sesión.
- Revisar permisos y roles asignados al usuario comprometido.

Erradicación

Objetivo: Eliminar cualquier persistencia del atacante y cerrar las brechas utilizadas.

Pasos:

- Identificar y cerrar la vulnerabilidad usada para ingresar (contraseña débil, brecha técnica...).

- Eliminar scripts o accesos creados por el intruso.
- Cambiar credenciales de administradores si fueron afectadas.
- Revisar otras cuentas con privilegios similares.

Recuperación

Objetivo: Restaurar acceso legítimo y corregir posibles daños.

Pasos:

- Restablecer el acceso a las cuentas de forma segura.
- Corregir configuraciones alteradas por el intruso.
- Notificar a los usuarios afectados (si procede).
- Monitorear la cuenta durante un periodo de observación.

Lecciones aprendidas

Objetivo: Fortalecer la seguridad y evitar futuras intrusiones.

Medidas recomendadas:

- Implementar MFA (autenticación multifactor) si aún no está.
- Revisar políticas de contraseñas (longitud, caducidad).
- Auditar regularmente cuentas privilegiadas.
- Capacitar al personal sobre buenas prácticas de acceso.

Categoría: Fuga o Pérdida de Información

Una fuga o pérdida de información ocurre cuando **datos sensibles son expuestos, accedidos o eliminados sin autorización**. Puede ser por error humano, negligencia, fallas técnicas o ataques maliciosos.

Detección del incidente

¿Qué buscar?

- Publicación no autorizada de datos en internet o redes.
- Archivos confidenciales encontrados fuera del entorno institucional (Google Drive personal, correos no autorizados).
- Usuarios que reportan pérdida o acceso indebido a información.
- Alertas del DLP (Data Loss Prevention) o SIEM.
- Dispositivos extraviados (pendrives, laptops) con datos sensibles.

¿Quién puede detectarlo?

- Usuarios (docentes, administrativos, estudiantes).
- Equipo de TI o seguridad.
- Auditores internos o externos.
- Herramientas automáticas (antivirus, DLP, SIEM).

Acciones iniciales:

- Documentar el incidente: fecha, tipo de datos, cómo fue detectado.
- No divulgar el hecho innecesariamente (evitar pánico).
- Notificar al equipo de seguridad o TI.

Análisis y validación

Objetivo: Determinar qué información se ha visto comprometida, cómo y por quién.

Pasos:

- Confirmar qué tipo de información fue expuesta: personal, académica, administrativa, financiera, etc.
- Determinar si la fuga fue interna (por accidente o abuso) o externa (por ataque).
- Verificar alcance del incidente: número de usuarios afectados, cantidad de archivos.
- Revisar logs, correos enviados, respaldos y accesos a carpetas compartidas.

Herramientas útiles:

- Logs de servidores y sistemas en la nube.
- Revisión de permisos en archivos compartidos.
- Herramientas de DLP (si se usan).
- Forense digital (si es necesario).

Contención del incidente

Objetivo: Detener la exposición de datos y evitar que se siga propagando.

Acciones inmediatas:

- Revocar enlaces compartidos o accesos a los archivos filtrados.
- Cambiar contraseñas de sistemas afectados.
- Eliminar archivos publicados de manera incorrecta (de servidores o la nube).
- Aislar dispositivos si hubo una filtración por malware o infección.

Erradicación

Objetivo: Eliminar la causa raíz y prevenir que vuelva a ocurrir.

Pasos:

- Corregir configuraciones inseguras en sistemas y carpetas.
- Actualizar políticas de uso de datos y acceso compartido.
- Establecer reglas de cifrado y almacenamiento seguro.
- Investigar al responsable si fue por negligencia o intencional.

Recuperación

Objetivo: Restaurar la seguridad y mitigar el impacto.

Pasos:

- Informar a los usuarios afectados si es necesario (ej. si sus datos personales fueron expuestos).
- Restaurar copias seguras de la información, si fue eliminada.
- Fortalecer medidas de control sobre los sistemas implicados.
- Supervisar durante los días siguientes posibles nuevas filtraciones.

Lecciones aprendidas

Objetivo: Reducir el riesgo de futuras fugas de información.

Medidas recomendadas:

- Capacitación regular en manejo seguro de datos.
- Política clara de uso de dispositivos externos y almacenamiento en la nube.
- Clasificación de la información institucional según su sensibilidad.
- Auditorías regulares de accesos a información crítica.
- Implementación de cifrado obligatorio en dispositivos y backups.

Cagtegoría: Ataques de Denegación de Servicio (DDoS)

Un ataque DDoS (Distributed Denial of Service) busca **interrumpir un servicio, red o sistema** enviando un volumen masivo de tráfico desde múltiples fuentes. En instituciones educativas, esto puede afectar el sitio web institucional, servidores de autenticación, portales académicos y LMS.

Detección del incidente

¿Qué buscar?

- Lentitud o inaccesibilidad repentina en servicios en línea.
- Saturación inusual del ancho de banda.
- Caída de servidores o servicios web sin causa técnica aparente.
- Alertas del firewall, balanceadores de carga o IDS/IPS.
- Muchos intentos de conexión desde múltiples IPs en muy poco tiempo.

¿Quién puede detectarlo?

- Equipo de TI / red.
- Proveedor de servicios de hosting o internet.
- Usuarios que reportan caída del servicio.

Acciones iniciales:

- Confirmar si la caída es general o localizada.
- Verificar consumo de ancho de banda y logs del servidor.
- Notificar al equipo de infraestructura/red o al proveedor.

Análisis y validación

Objetivo: Confirmar que se trata de un DDoS, y no de un problema técnico común.

Pasos:

- Revisar los logs de red: número de peticiones, IPs repetidas o inusuales.
- Identificar patrones de tráfico (volumen, origen, frecuencia).
- Comparar contra el comportamiento normal del sistema (¿coincide con temporada de matrículas?).
- Consultar con el proveedor de internet o del servicio en la nube.

Herramientas útiles:

- Monitores de red (Zabbix, PRTG, NetFlow).
- Firewalls o balanceadores de carga con capacidades de DDoS detection.
- Plataformas de protección en la nube (Cloudflare, AWS Shield).

Contención del incidente

Objetivo: Minimizar el impacto y mantener operativos los servicios esenciales.

Acciones inmediatas:

- Aplicar reglas en el firewall para filtrar tráfico malicioso (por IP, geolocalización, user-agent).
- Activar mitigación de DDoS en el proveedor (si está contratado).
- Redirigir tráfico a servicios externos de protección como Cloudflare o Akamai.
- Limitar temporalmente accesos desde ubicaciones no prioritarias.

Erradicación

Objetivo: Restaurar el estado normal del servicio y asegurar los puntos de entrada.

Pasos:

- Identificar y bloquear permanentemente las fuentes del ataque (si es posible).
- Reforzar las configuraciones de red y firewall.
- Validar que no se hayan abierto vulnerabilidades aprovechadas durante el ataque.
- Notificar a autoridades o CERT nacionales si el ataque es masivo.

Recuperación

Objetivo: Restablecer completamente los servicios afectados y validar su estabilidad.

Pasos:

- Levantar servicios afectados de manera progresiva.
- Verificar la integridad de sistemas y bases de datos.
- Informar a la comunidad educativa sobre el restablecimiento.
- Monitorear activamente durante las horas siguientes.

Lecciones aprendidas

Objetivo: Mejorar la resiliencia ante futuros ataques DDoS.

Medidas recomendadas:

- Contratar servicios de mitigación DDoS en la nube (CDN, firewall avanzado).
- Configurar alertas tempranas de consumo de recursos.
- Segmentar los sistemas críticos (evitar punto único de falla).
- Diseñar un plan de contingencia para continuidad operativa ante caída de servicios.

Categoría: Explotación de Vulnerabilidades

Este tipo de incidente ocurre cuando un atacante detecta y aprovecha una **vulnerabilidad técnica** (como una versión antigua de software, una mala configuración o una brecha en una aplicación web) para ejecutar acciones maliciosas: acceso no autorizado, ejecución remota de código, robo de información o manipulación de sistemas.

Detección del incidente

¿Qué buscar?

- Comportamientos anómalos en servidores o aplicaciones.
- Alertas del sistema de detección de intrusos (IDS/IPS).
- Actividad inusual en los logs: comandos extraños, errores 500 repetidos, etc.
- Informes de pruebas de penetración (internas o externas).
- Anuncios públicos de vulnerabilidades (CVE) que afecten software usado por la institución.

¿Quién puede detectarlo?

- Administradores de sistemas.
- Auditores de seguridad (internos o externos).
- Sistemas automáticos de escaneo (Nessus, OpenVAS).
- Usuarios que detectan fallos inusuales en aplicaciones.

Acciones iniciales:

- Registrar el evento y recolectar información básica (fecha, sistema afectado, síntomas).
- Notificar al área de TI/seguridad.
- No reiniciar el servidor sin autorización (puede perderse evidencia).

Análisis y validación

Objetivo: Confirmar si se está explotando una vulnerabilidad real y determinar su criticidad.

Pasos:

- Verificar si el sistema está expuesto a una vulnerabilidad conocida (revisar CVEs).
- Comparar con información de bases de datos de seguridad (NIST, Mitre).
- Revisar logs de acceso, comandos ejecutados, cargas en URLs o formularios web.
- Identificar si hubo explotación exitosa (acceso, cambio, extracción de datos).

Herramientas útiles:

- Escáneres de vulnerabilidades (Nessus, Qualys, OpenVAS).
- Logs del sistema operativo, aplicaciones y servicios web.
- Plataformas de threat intelligence.

Contención del incidente

Objetivo: Detener la explotación y aislar los sistemas afectados.

Acciones inmediatas:

- Desconectar el sistema afectado de la red si hay evidencia de compromiso activo.
- Bloquear temporalmente accesos al servicio vulnerable.
- Revocar sesiones y accesos a datos sensibles.
- Aislar redes o servicios relacionados que puedan estar en riesgo.

Erradicación

Objetivo: Corregir la vulnerabilidad y eliminar el vector de ataque.

Pasos:

- Aplicar parches y actualizaciones del software afectado.
- Corregir configuraciones inseguras (por ejemplo: puertos abiertos, contraseñas por defecto).
- Eliminar cuentas o accesos creados por el atacante (si existieron).
- Realizar pruebas de validación para asegurar que la vulnerabilidad ya no es explotable.

Recuperación

Objetivo: Restaurar el sistema de forma segura y confiable.

Pasos:

- Validar que el sistema funciona correctamente luego de las correcciones.
- Reincorporar el sistema a la red bajo monitoreo.
- Verificar la integridad de los datos y el sistema (checksum, revisión de logs).
- Restaurar servicios afectados, si hubo interrupciones.

Lecciones aprendidas

Objetivo: Fortalecer el entorno técnico y prevenir futuras explotaciones.

Medidas recomendadas:

- Implementar un programa continuo de gestión de vulnerabilidades.
- Mantener todos los sistemas actualizados con parches de seguridad.
- Limitar exposición pública de servicios (uso de VPN, firewalls, segmentación).
- Realizar auditorías y pruebas de penetración regularmente.
- Fomentar la cultura de "cero confianza" en la arquitectura de red (Zero Trust).

- e información sensible.
- Creación o modificación de cuentas sin autorización.

- Reportes de usuarios sobre comportamientos sospechosos.

Categoría : Abuso de Privilegios Internos

Detección del incidente

¿Qué buscar?

- Acceso o modificación de datos fuera de horarios o funciones habituales.
- Uso de cuentas administrativas para tareas no autorizadas.
- Descarga o copia masiva de información sensible.
- Creación o modificación de cuentas sin autorización.
- Reportes de usuarios sobre comportamientos sospechosos.

¿Quién puede detectarlo?

- Equipos de auditoría y monitoreo.
- Sistemas de gestión de accesos (IAM) y registros (logs).
- Usuarios que notan irregularidades.
- Herramientas de análisis de comportamiento (UEBA).

Acciones iniciales:

- Documentar actividades sospechosas.
- Avisar a seguridad informática y a Recursos Humanos según el caso.
- Mantener discreción para no alertar al sospechoso.

Análisis y validación

Objetivo: Confirmar el abuso y determinar su alcance.

Pasos:

- Revisar logs detalladamente para identificar acciones realizadas.
- Corroborar si las acciones violan políticas de uso o seguridad.
- Identificar qué datos o sistemas fueron afectados.
- Entrevistar al personal involucrado si es necesario.

Herramientas útiles:

- Sistemas de monitoreo de actividad.
- Logs de auditoría.
- Software UEBA (User and Entity Behavior Analytics).

- Contención del incidente

Objetivo: Detener el abuso y proteger los activos.

Acciones inmediatas:

- Revocar permisos o acceso temporalmente al usuario sospechoso.
- Cambiar credenciales relacionadas.
- Restringir accesos a sistemas críticos.
- Notificar a la gerencia y recursos humanos.

Erradicación

Objetivo: Eliminar las acciones maliciosas o erróneas y restaurar controles.

Pasos:

- Revertir cambios no autorizados.
- Revisar y corregir permisos y roles asignados.
- Implementar controles adicionales si se identifican brechas.
- Documentar el incidente para seguimiento legal o disciplinario.

Recuperación

Objetivo: Restaurar la confianza y operatividad segura.

Pasos:

- Restablecer accesos correctos según roles.
- Comunicar a los equipos afectados las acciones realizadas.
- Supervisar la actividad del usuario tras el incidente.
- Actualizar políticas de seguridad y formación para evitar repetición.

Lecciones aprendidas

Objetivo: Fortalecer la gestión de accesos y cultura organizacional.

Medidas recomendadas:

- Implementar principio de mínimo privilegio (solo lo necesario).
- Revisar periódicamente permisos y accesos.
- Capacitar sobre ética y seguridad para todo el personal.
- Implementar monitoreo continuo de actividades críticas.
- Establecer protocolos claros para reportar y manejar abusos.

10. REFERENCIAS BIBLIOGRAFICAS

- Guía emitida por el MINTIC.
- Modelo de seguridad y privacidad de la información v3.0.2.

11. CONTROL DE CAMBIOS

VER.	FECHA	ELABORÓ	REVISÓ Y APROBÓ	DESCRIPCIÓN
0	01/11/2020			VERSIÓN ORIGINAL
1	30/09/2022	Carlos Gomez		ACTUALIZACIÓN Item 4 marconormativo Item 5 Organización para la seguridad de la información Item 6 responsables
2	3/07/2025	Olga Marin	Alberto Redondo	Actualización de membrete institucional y nombre de la Oficina de Gestión Tecnológica e Información
3	9/09/2025	Olga Marin	Alberto Redondo	Actualización de los nombres de oficinas y departamentos actuales, adición de párrafo en el alcance acerca del seguimiento y revisión de la política
		Carlos Gómez		Adición del capítulo “Clasificación de incidentes de seguridad de la Información”