RE: Reiteración Respuesta a Obervaciones invitación publica 019 de 2024

MARIA DEL PILAR DELGADO RODRIGUEZ <mdelgado@ucundinamarca.edu.co>

Mar 16/07/2024 11:58 AM

Para:JENIFFER CASTILLO FERNÁNDEZ <jcastillof@ucundinamarca.edu.co>;ÁREA DE SERVICIOS TECNOLÓGICOS <serviciostecnologicos@ucundinamarca.edu.co>
CC:ANA LUCIA HURTADO MESA <alhurtado@ucundinamarca.edu.co>;DIRECCIÓN DE SISTEMAS Y TECNOLOGIA <SISTEMASYTECNOLOGIA@ucundinamarca.edu.co>;Sistema de Gestión de Seguridad de la Informacion <sgsi@ucundinamarca.edu.co>

13.1

Fusagasugá, 2024-07-16

Ingeniera
JENIFFER CASTILLO FERNÁNDEZ
Profesional Director de Área I
Área de Servicios Tecnológicos
Dirección de Sistemas y Tecnología
Ciudad

Asunto: Respuesta “Observaciones invitación pública 019 de 2024”

Respetada Ingeniera Castillo:

En atención al correo que antecede, a continuación, se da respuesta de acuerdo con la observación allegada:

Observación No. 29

Solicitamos a la entidad validar cual es el alcance de la protección de datos ya que existen diversas políticas y artículos que solo están enfocados a la seguridad de la información, de esta manera solicitamos que nos permitan saber el alcance de la información necesaria que se debe custodiar ya que hasta el momento solo se ve reflejado en el pliego servicio de datos e internet y la seguridad perimetral de la Universidad de Cundinamarca.

Actualmente la Universidad de Cundinamarca, viene implementando el Sistema de Gestión de Seguridad de la Información -SGSI y la Ley de Protección de Datos Personales, siguiendo los lineamientos de la Norma ISO 27001 y la Ley 1581 de 2012 respectivamente, el control ***15 Relación con proveedores, 15.1 Seguridad en las relaciones con proveedore, 15.1.1 Política de seguridad de la información en las relaciones con los proveedores;*** *del* anexo A de la Norma ISO 27001.

Por lo tanto, la institución debe asegurar la confidencialidad, integridad y disponibilidad de la Información, que se encuentra alojada en sus repositorios y Bases de Datos, de igual forma, asegurar que los proveedores cuenten con las medidas de seguridad para asegurar la triada de la información, en consecuencia es importante que los proveedores cuenten con una política de seguridad de la información según lo expuesto en la Norma ISO 27001:2022 en el requisito **5.2 Política** y en la Guía N°2 del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia – MinTIC denominada *“Elaboración de la política general de seguridad y privacidad de la información”*

De igual forma, es importante que cuenten con una adecuada Política de Protección de Datos Personales, acorde a la Ley 1581 de 2012 ***“****Por la cual se dictan disposiciones generales para la protección de datos personales”*, y al Decreto Único 1074 de 2015 Artículo **2.2.2.25.3.1** ***Políticas del Tratamiento de la Información “****Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales* ***y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas****.”,* los proveedores pasan a ser encargados y tienen las mismos deberes que el responsable como se enuncia en el Titulo VI DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO, de la Ley 1581 de 2012.

Pendiente de sus sugerencias y/o comentarios

Cordialmente

Respuesta “URGENTE SOLICITUD RESPUESTA IDENTIFICADOR CONPPU 304 INTEGRADOC”

Sistema de Gestión de Seguridad de la Informacion <sgsi@ucundinamarca.edu.co>

Lun 22/07/2024 15:59

Para:Asesor Juridico Compras <apoyojuridico3@ucundinamarca.edu.co>
CC:COMPRAS UDEC <comprasudec@ucundinamarca.edu.co>;Bienes y Servicios <bienesyservicios@ucundinamarca.edu.co>;COORDINADOR JURIDICO COMPRAS <coordinadorjuridicocompras@ucundinamarca.edu.co>

3 archivos adjuntos (1 MB)

ESG-SSI-P09 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.pdf; ASIP16 DESARROLLO DE SISTEMAS DE INFORMACIÓN.pdf; ESG-SSI-M012 MANUAL POLÍTICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.pdf;

13.1

Fusagasugá 2024-07-22

Doctora
MONICA MARITZA SOTELO MORA
Asesora Jurídica
Oficina de Compras
Ciudad

Asunto: Respuesta “URGENTE SOLICITUD RESPUESTA IDENTIFICADOR CONPPU 304 INTEGRADOC”

Respetada Doctora Sotelo:

En atención al correo que antecede, me permito informar que se revisó el aplicativo *Integradoc* desde la cuenta de la Ingeniera María del Pilar Delgado Rodríguez y la del Sistema de Gestión de Seguridad de la Información – SGSI, y no se evidencia ninguna tarea en la bandeja de entrada.

Por lo anterior, se envía la respuesta a las observaciones por medio de correo electrónico para su conocimiento y fines pertinentes.

Observación No. 11 De acuerdo a lo solicitado por la entidad en el anexo MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS, solicitamos a la entidad aclare a los proponentes lo expuesto en el control A.15 Relación con Proveedores del Anexo A de la norma ISO / IEC 27001:2013.

El manual ESG-SSI-M013 MANUAL - LINEAMIENTO DE SEGURIDAD DE LA INFORMACION CON RELACION A LOS PROVEEDORES Y/O TERCEROS, está inspirado y fue construido de acuerdo con lo que solicita el control A.15 *Relación con los Proveedores* del Anexo A de la Norma ISO / IEC 27001:2013, por lo tanto, es un lineamento institucional que debe seguir cada proveedor que quiera contratar con la Universidad de Cundinamarca.

Observación No. 12 Pedimos a la entidad brinde información más específica de acerca de los protocolos de respuesta claros y efectivos en caso de que se produzcan violaciones de seguridad de la información y que tengan que ver con la matriz de escalamiento y política de seguridad de la Entidad. Agradecemos sea anexada a la respuesta a las presentes observaciones para conocimiento de los proponentes.

Los protocolos de respuesta en caso de que se produzcan violaciones de seguridad de la información están documentados en los documentos ESG-SSI-P09 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y el ESG-SSI-M012 MANUAL POLÍTICA DE GESTIÓN DE INCIDENTES los cuales se encuentran en adjunto.

Observación No. 13 De acuerdo a la página 9 del Manual – Lineamiento de Seguridad de la Información en el punto 6 donde establece que se deberá atender lo dispuesto en el ASIP16 DESARROLLO DE SISTEMAS DE INFORMACIÓN, solicitamos a la entidad suministrar el anexo para tener claro la información del documento.

En adjunto se encuentra el documento ASIP16 DESARROLLO DE SISTEMAS DE INFORMACIÓN.

Observación No. 14 Solicitamos a la entidad anexar el documento citado en la página 11 del Manual – Lineamiento de Seguridad de la Información ítem N° 3 ESG-SSI-P09 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN buscando así tener claridad de la información que tiene el documento.

En adjunto se encuentra el documento ESG-SSI-P09 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Pendiente de sus comentarios y/o sugerencias.

Cordialmente,

UDEC
UNIVERSIDAD DE CUNDINAMARCA

Más allá
de la universidad
tradicional

MARÍA DEL PILAR DELGADO RODRÍGUEZ
Coordinadora del Sistema de Gestión de Seguridad de la Información – SGSI
Sistema de Gestión de Seguridad de la Información – SGSI
sgsi@ucundinamarca.edu.co
Diagonal 18 No. 20-29
Fusagasugá, Cundinamarca - CO

www.ucundinamarca.edu.co

Este mensaje no es considerado spam porque su destinatario es usuario registrado a través del portal de la Universidad de Cundinamarca. Si usted recibió este correo por error o no quiere recibir más nuestros mensajes, puede responder a este correo solicitando su desvinculación de las bases de datos. La información transmitida por este medio no representa el pensamiento de la institución, cada información emitida es responsabilidad de su autor. Esta comunicación contiene información que es confidencial y también puede contener información privilegiada o de datos personales de titulares de la Universidad de Cundinamarca. Es para uso exclusivo del destinatario/s. Si usted no es el destinatario/s tenga en cuenta que cualquier distribución, copia o uso de esta comunicación o la información que contiene está estrictamente prohibida. Si usted ha recibido esta comunicación por error por favor notifíquelo por correo electrónico **sgsi@ucundinamarca.edu.co** y **protecciondedatos@ucundinamarca.edu.co.** Para mayor información consulte nuestra Política de Protección de Datos Personales. Piense en el medio ambiente. No imprima este mensaje de no ser absolutamente necesario.

De: Asesor Juridico Compras <apoyojuridico3@ucundinamarca.edu.co>
Enviado: lunes, 22 de julio de 2024 1:05 p. m.
Para: MARIA DEL PILAR DELGADO RODRIGUEZ <mdelgado@ucundinamarca.edu.co>; Sistema de Gestión de Seguridad de la Informacion <sgsi@ucundinamarca.edu.co>
Cc: COMPRAS UDEC <comprasudec@ucundinamarca.edu.co>; Bienes y Servicios <bienesyservicios@ucundinamarca.edu.co>; COORDINADOR JURIDICO COMPRAS <coordinadorjuridicocompras@ucundinamarca.edu.co>
Asunto: RE: URGENTE SOLICITUD RESPUESTA IDENTIFICADOR CONPPU 304 INTEGRADOC

Fusagasugá, 2024-07-22

Ingeniera
MARIA DEL PILAR DELGADO RODRIGUEZ
Coordinadora Sistema de Gestion de Seguridad de la Informacion
Universidad de Cundinamarca

Cordial Saludo,

Por medio de la presente me permito requerir de manera urgente la respuesta que fue asignada por aplicativo Integradoc la cual no fue realizada de acuerdo con la solicitud, por lo anterior que de manera atenta solicito dar rta a los puntos 11, 12, 13 y 14 de la observación que se adjunta.

OBJETIVO:	Realizar actividades de innovación, renovación y sostenimiento sobre los Sistemas de Información de la institución, contribuyendo al fortalecimiento de los servicios en línea ofrecidos a toda la comunidad universitaria, reduciendo los tiempos de respuesta en los trámites y proporcionando información de manera oportuna.
ALCANCE:	Innovación y renovación tecnológica de los Sistemas de Información administrados por la Dirección de Sistemas y Tecnología, dando alcance al contexto tecnológico de la institución a través de los procedimientos documentados en los sistemas de gestión. Aplica para nuevos desarrollos, actualizaciones de aplicativos existentes, adquisición de licencias para la gestión de procesos administrativos y desarrollo de software con externos.
LÍDER DE PROCEDIMIENTO:	Director de Sistemas y Tecnología.

DEFINICIONES

CONTEXTO TECNOLÓGICO: Grupo de variables que en conjunto reflejan el avance técnico de una entidad.

INNOVACIÓN TECNOLÓGICA: Creación o implementación de nuevos servicios tecnológicos para la optimización de los procesos de la institución.

MESA DE SERVICIOS A UN CLIC: Aplicación para la recepción y atención de solicitudes de los servicios de la Dirección de Sistemas y Tecnología.

MICROSOFT PLANNER: Es una aplicación de la suite de Microsoft 365 que permite administrar planes de trabajo, de tal forma que facilita asignar de manera organizada diferentes actividades que se tendrán que realizar para cumplir con un plan, la fecha de entrega, así como el o los responsables de llevarla a cabo.

DEFINICIONES

MICROSOFT TEAMS: Microsoft Teams se basa en Grupos de Office 365 y permite la colaboración entre personas de un mismo equipo o el desarrollo de un proyecto concreto, compartiendo recursos y cuya función principal es la comunicación constante entre los miembros del equipo.

PLATAFORMA INSTITUCIONAL: Aplicación informática encargada de administrar la información académico – administrativa de la institución.

RENOVACION TECNOLÓGICA: Implementación de actualizaciones a los sistemas de información o infraestructura tecnológica institucional.

REQUERIMIENTOS FUNCIONALES: Un requisito funcional define claramente una función del sistema de software o sus componentes.

REQUERIMIENTOS NO FUNCIONALES: Son criterios específicos para evaluar las condiciones de un servicio a nivel operacional.

SERVICIOS EN LINEA: Servicio que puede ser prestado por medios electrónicos a través de la plataforma de una entidad.

SISTEMA DE INFORMACIÓN: Es un sistema electrónico de administración de información cuyas bondades favorecen a los trámites y servicios en línea.

TESTER: Un tester investiga un producto de software con el objetivo de obtener información acerca de su calidad y del valor que representa para quienes lo utilizan

VERSIONADOR DE CODIGO: Repositorio de códigos fuente

REQUISITOS Y CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

Todo sistema de información que se vaya a implementar dentro de la plataforma institucional de la Universidad de Cundinamarca debe articularse con el marco tecnológico de la entidad, obedecer mínimo a un procedimiento documentado y articularse con los actuales sistemas de información, además debe hacer uso de los datos e infraestructura tecnológica ya instalada. Su construcción debe tener en cuenta la metodología de desarrollo de software que permite realizar revisiones periódicas, en las que, dependiendo el alcance del proyecto, el área determinará la frecuencia de verificación y solicitud de ajustes, para el seguimiento y mejoramiento del producto a implementar.

El área de Desarrollo de Sistemas de Información debe gestionar el diligenciamiento del contrato cesión de derechos entre desarrolladores de Software y la Universidad de Cundinamarca, dependiendo el vínculo existente:

- Para proveedores, diligenciar el formato ASIF058.
- Para personal Termino Fijo, Orden de Prestación de Servicios, Personal Académico y Planta, diligenciar el formato ASIF057.
- Para pasantes y monitores, diligenciar el formato ASIF059.

Una vez culminada la prestación del servicio solicitado, el área de Desarrollo de Sistemas de información realizará la capacitación al usuario administrador del sistema entregado, a quien se le suministrará la Guía de Usuario o Manual de Usuario – ASIr020, con el fin de que la socialice con las partes interesadas.

Nota aclaratoria: Se habilitará el canal de **MICROSOFT TEAMS** para mantener una efectiva comunicación con el usuario durante todo el proceso. También se autoriza **MICROSOFT PLANNER** para realizar los seguimientos diarios de los desarrolladores del área de Desarrollo de Sistemas de Información.

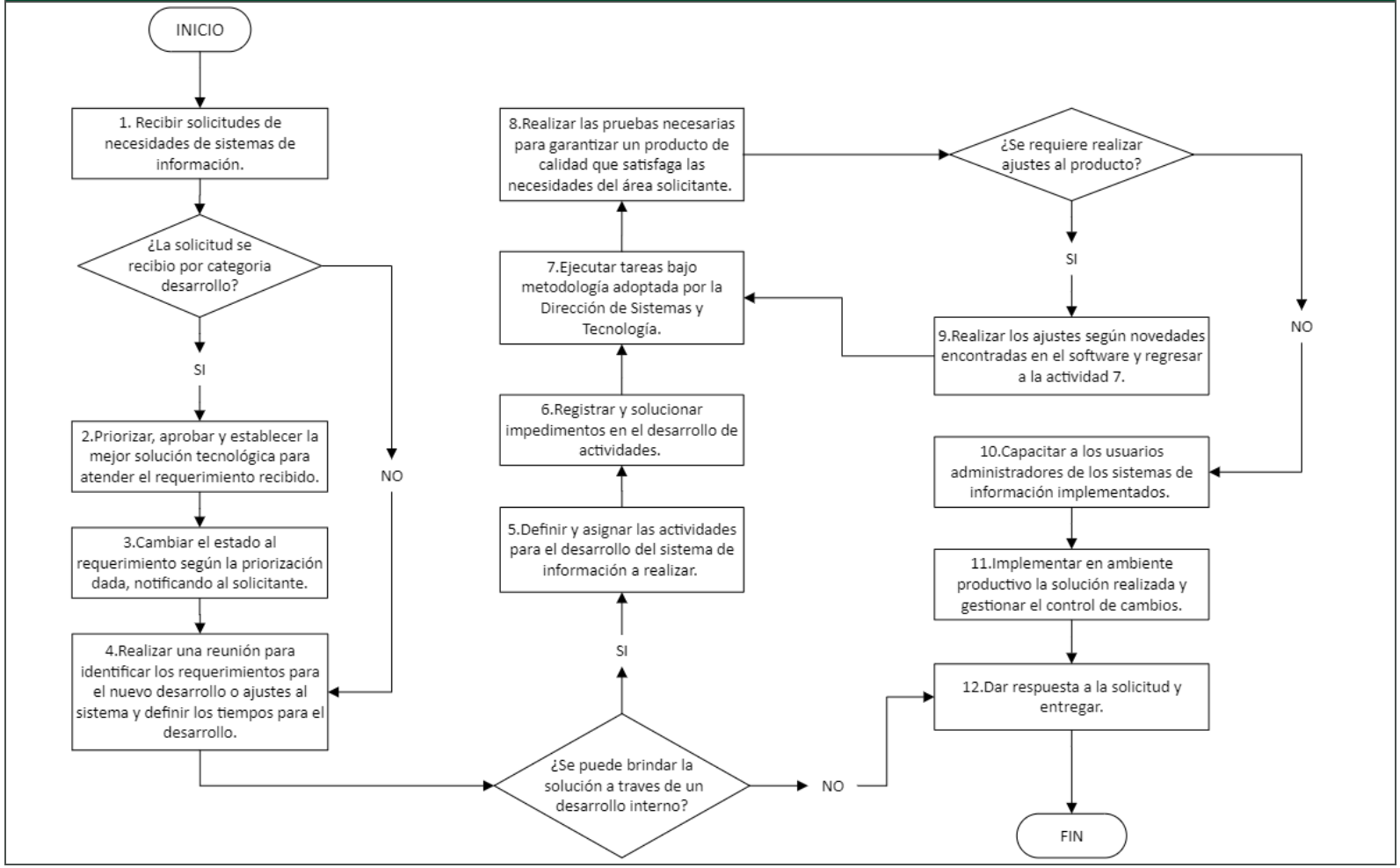
Nota Informativa: La Dirección de Sistemas y Tecnología informa a la comunidad universitaria que el ingreso de Usuarios al Área de Desarrollo de Sistemas de Información no se encuentra autorizado, por lo tanto, el soporte de primer nivel será proporcionado por los funcionarios del Área de Uso y Apropiación de Sistemas de Información.

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
1.Recibir solicitudes de necesidades de sistemas de información.	Directores, Jefes y/o coordinadores de Dependencias	Verificar que el requerimiento cumpla con los objetivos del proceso, Planes de Acción y Planes de Desarrollo	Plataforma / Sistema Institucional de Solicitudes (SIS) / Mesa de Servicios a un Clic.	Solicitud en la Mesa de Servicio
¿La solicitud se recibió por categoría Desarrollo de Sistemas de Información? Si la respuesta es afirmativa continúa a la Actividad 2, de lo contrario continúa a la Actividad 4.				
2.Priorizar, aprobar y establecer la mejor solución tecnológica para atender el requerimiento recibido.	Director de Sistemas y Tecnología, según gestión con la Alta Dirección o al Comité de Tecnología	Decidir la mejor solución que sea aprobada por Alta Dirección o comisión pertinente.	**ASIM001 ASIM006**	Solicitud en la Mesa de Servicios a un Clic
3.Cambiar el estado al requerimiento según la priorización dada, notificando al solicitante.	Gestor de Desarrollo de Sistemas de Información	Realizar el cambio de estado a la solicitud.	Plataforma / Sistema Institucional de Solicitudes (SIS) / Mesa de Servicios a un Clic.	Actualización de la solicitud en la mesa de servicios a un Clic
4.Realizar una reunión para identificar los requerimientos para el nuevo desarrollo o	Gestores de Uso y Apropiación Sistemas de Información,	Realizar reunión en la que deben participar gestores de la oficina solicitante, equipo de uso y	**ASIM006**	Actualización de la solicitud en la mesa de servicios a un Clic

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
ajustes al sistema y definir los tiempos para el desarrollo.	Desarrollo de Sistemas de Información	apropiación y equipo de desarrollo de sistemas de información.		
¿Se puede brindar solución a través de un desarrollo interno? Si la respuesta es afirmativa continúe con la actividad N°5, de lo contrario diríjase a la actividad N°12.				
5.Definir y asignar las actividades para el desarrollo del sistema de información a realizar.	Gestor de Desarrollo de Sistemas de Información	Diferenciar los artefactos según la metodología implementada.	Herramienta para la gestión de la metodología	Registro de actividades en la herramienta Microsoft Planner y en el **ASIF065** - Cronograma de necesidades de Sistemas de Información
6.Registrar y solucionar impedimentos en el desarrollo de actividades.	Gestor de Desarrollo de Sistemas de Información	Realizar seguimiento diario a la herramienta Microsoft Planner y verificar el cumplimiento de los desarrolladores	**ASIM006**	Registro de actividades en la herramienta Microsoft Planner, en el apartado de comentarios
7.Ejecutar tareas bajo metodología adoptada por la Dirección de Sistemas y Tecnología.	Gestor de Desarrollo de Sistemas de Información	Realizar revisiones diarias con el equipo de desarrollo	**ASIM006**	Registro de actividades en la herramienta Microsoft Planner Códigos Fuente registrados en el GitLab institucional
8.Realizar las pruebas necesarias para garantizar un producto de calidad que	Tester	Ejecutar las pruebas necesarias para satisfacer las necesidades del área solicitante	**ASIM006**	**ASIr019**

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
satisfaga las necesidades del área solicitante.				
¿Se requiere realizar ajustes al producto? Si la respuesta es afirmativa continúe con la actividad N°9, de lo contrario diríjase a la actividad N°10.				
9.Realizar los ajustes según novedades encontradas en el software y regresar a la actividad 7.	Gestor de Desarrollo de Sistemas de Información	Verificar los ajustes en el Versionador de Código	**ASIM006**	Códigos Fuente GitLab Institucional
10.Capacitar a los usuarios administradores de los sistemas de información implementados.	Gestores de Uso y Apropiación Sistemas de Información, Desarrollo de Sistemas de Información	Entregar guía de usuario (si el ajuste lo requiere)	**ASIr020**	**ESGr015**
11.Implementar en ambiente productivo la solución realizada y gestionar el control de cambios.	Gestor de Desarrollo de Sistemas de Información	Mesa de ayuda/versionamiento de aplicaciones	**ASIM006** Guía de despliegue en ambiente productivo	Sistema de Información Implementado Mesa de Ayuda
12.Dar respuesta a la solicitud y entregar.	Gestor de Desarrollo de Sistemas de Información	Brindar respuesta en Mesa de Servicios a un Clic	**ASIM001**	Actualización de la solicitud en la Mesa de Servicios a un clic

DIAGRAMA DE FLUJO



SISTEMAS DE INFORMACIÓN			
SISTEMA DE INFORMACIÓN	**DESCRIPCIÓN**	**FRECUENCIA**	**UBICACIÓN**
Mesa de Servicios a un Clic	Aplicación para la atención de solicitudes de requerimientos para desarrollos nuevos o actualizaciones de sistemas de información institucionales.	Diario	Plataforma Institucional / Sistema Institucional de Solicitudes / Mesa de Servicios
Mesa de Ayuda	Aplicación para gestionar y controlar las versiones de las aplicaciones propias	Según necesidad	Plataforma Institucional / Mesa de Ayuda
GitLab	Herramienta para el control de versiones de códigos fuentes	Según necesidad	Servidores institucionales

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA DE APROBACIÓN**			**DESCRIPCIÓN DEL CAMBIO**
	AAAA	**MM**	**DD**	
1	2018	02	13	Emisión del Documento.
2	2018	08	11	Se inactiva el instructivo y se crea el manual Política de Desarrollo de Software.
3	2019	02	08	Corrección de los documentos de referencia
4	2019	04	04	Inclusión de los documentos de referencia ASIr033 y ASIr035
5	2020	10	19	Ajustes en algunos campos, se modifican los documentos referencia y otras modificaciones para cumplir con la Resolución 000158 del 29 de octubre de 2019, "POR LA CUAL SE ADOPTA LA IMAGEN CORPORATIVA Y SE DICTAN LAS POLÍTICAS DE IDENTIDAD CORPORATIVA DE LA UNIVERSIDAD DE CUNDINAMARCA"
6	2022	12	06	Se realizan correcciones, teniendo en cuenta las observaciones de la auditoría interna vigencia 2021, así como mejoras propias del proceso. Se agregaron definiciones de algunos términos, se modificaron los requisitos y condiciones

				del procedimiento, también se realizaron ajustes a las actividades y al diagrama de flujo.
7	2023	07	21	Se realiza la inclusión de los formatos ASIF057, ASIF058 Y ASI059 en los requisitos y condiciones del procedimiento.
8	2023	10	23	Se realiza el cambio en las actividades del procedimiento y se agregan requisitos y condiciones.
9	2024	02	16	Se realizan ajustes a las actividades y diagrama de flujo del procedimiento.
10	2024	06	20	Se incluye la herramienta Microsoft Planner, para los seguimientos a los desarrolladores, asimismo se incluye el formato ASIF065 - Cronograma de necesidades de Sistemas de Información.

ELABORÓ	
NOMBRES Y APELLIDOS	**CARGO**
Yohan Sebastián Moreno Lesmes	Técnico IV
Maria Alejandra Guerrero Martínez	Técnico IV
Yamid Santiago Montañez Monroy	Técnico

REVISÓ	
NOMBRES Y APELLIDOS	**CARGO**
Ana Lucia Hurtado Mesa	Directora de Sistemas y Tecnología

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	**CARGO**	**FECHA**		
		AAAA	**MM**	**DD**
Ana Lucia Hurtado Mesa	Directora de Sistemas y Tecnología	2024	06	20

UNIVERSIDAD DE CUNDINAMARCA

MANUAL - POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

FUSAGASUGÁ
2022

UNIVERSIDAD DE CUNDINAMARCA

MANUAL - POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

FUSAGASUGÁ
2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO GENERAL 5
2.1. OBJETIVO GENERAL 5
2.2. OBJETIVOS ESPECÍFICOS 5
3. ALCANCE 6
4. DEFINICIONES 6
5. NORMATIVIDAD 8
6. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 8
7. CONTEXTO GENERAL 8
8. MODELO PARA LA GESTIÓN DE INCIDENTES 11
9. PREPARACION 12
9.1. Detección y reporte 13
9.2. Reporte de eventos y/o incidentes de seguridad de la información… 13
9.3. Evaluación y decisiones 14
9.4. Clasificación de incidentes 14
9.5. Priorización de incidentes de seguridad según su impacto 17
9.6. Respuesta, contención, erradicación y recuperación. 18
9.7. Contención, erradicación y recuperación 19
9.8. Lecciones aprendidas 25
10. BIBLIOGRAFÍA Y WEBGRAFÍA 26

1. INTRODUCCIÓN

En la actualidad, la información en las organizaciones es el activo más importante que pueden poseer, dado que, en el ejercicio de sus actividades estratégicas, misionales, y/o comerciales, logran producir, almacenar, transferir y procesar gran cantidad de datos indispensables para su funcionamiento, en otras palabras, a esto se le conoce como activos de información. Este tipo de elementos pueden ser archivos (físicos y/o digitales), bases de datos, contratos, acuerdos, manuales de usuarios, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, instalaciones, servicios informáticos, servicios de comunicaciones, entre otros. Por lo tanto, es necesario que las organizaciones implementen medidas y técnicas para salvaguardar los activos de información.

Algunas técnicas para la protección de la información, están relacionadas a la aplicación de controles basados en estándares internacionales, como la norma ISO/IEC 27001, donde se establece los lineamientos para la implementación de un sistema de gestión de seguridad de la información que garantice proteger los principios de confidencialidad, integridad y disponibilidad, sin embargo la implementación de controles dentro de una organización, no es suficiente ya que estos por si solos, no garantizan que no se vulneren las políticas de seguridad de la información que se hayan establecido previamente. De esta forma, dentro de los procedimientos para la aplicación de los controles de seguridad, en ocasiones se puede propiciar los riesgos residuales en las organizaciones, que podrían generar impactos en la seguridad de la información y, por consiguiente, estos generarían la posibilidad de incidentes de seguridad de la información.

Por lo anterior, la Universidad de Cundinamarca busca salvaguardar los activos de información dentro de la institución, aplicando los controles necesarios en articulación con las áreas involucradas, sin embargo, entendiendo la posibilidad de la materialización de un incidente, el Sistema de Gestión de Seguridad de la Información – SGSI presenta este Manual - Política, donde se establecen los lineamientos para la gestión de incidentes de seguridad de la información basados en estándares nacionales e internacionales.

2. OBJETIVO GENERAL

2.1. OBJETIVO GENERAL

Establecer los lineamientos para la gestión de incidentes de seguridad de la información, a fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Universidad de Cundinamarca, tomando como referencia la norma internacional ISO27001 y las políticas públicas nacionales, permitiendo la mitigación del impacto negativo ante la materialización de los incidentes de seguridad de la información.

2.2. OBJETIVOS ESPECÍFICOS

- Definir las actividades para monitoreo, el reporte y escalamiento de incidentes de seguridad de la información a las áreas encargadas, permitiendo evidenciar la trazabilidad y el avance del evento.

- Establecer las acciones necesarias para la detección, monitoreo y reporte brindando una respuesta oportuna y apropiada, cuando se presente un evento o incidente de seguridad de la información en la Universidad de Cundinamarca y a sus partes interesadas.

- Establecer el mecanismo que permita consolidar las lecciones aprendidas tras los incidentes de seguridad de la información que se presenten en la institución, a fin de evitar la probabilidad de ocurrencia, mediante la documentación necesaria.

- Socializar los lineamientos que permitan reducir y contener los impactos negativos que los incidentes puedan generar a la Universidad mediante la divulgación de los procedimientos internos y la implementación de las técnicas adecuadas.

3. ALCANCE

El presente Manual- Política aplica para todos los procesos, servicios, sistemas y/o redes de información con los que la Universidad de Cundinamarca cuenta y en donde los funcionarios que, en sus diferentes modalidades de contratación, en el cumplimiento de sus funciones contractuales tiene acceso autorizado a los activos de información de la institución. Este Manual – Política para la gestión de incidentes de Seguridad de la Información involucra las etapas de detección, análisis, contención, erradicación de incidentes y finaliza con la consolidación de lecciones aprendidas.

4. DEFINICIONES

ACTIVO DE INFORMACIÓN: Se refiere a cualquier información o elemento en físico y/o digital para el procesamiento, almacenamiento, comunicaciones, procesos, procedimientos y recursos humanos asociados con el manejo y uso de los datos para llevar a cabo las actividades estratégicas, misionales, de apoyo y seguimiento de la institución.[1]

CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados según sea requerida.[2]

CSIRT: Cyber Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad de la Información y Seguridad Informática), el cual se encarga de gestionar de forma eficiente el daño resultante de incidentes, así como también proveer de respuesta y recuperación efectiva, ante estos.[3]

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.[4]

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia o cambio de circunstancias identificadas en un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, falla de los controles o una situación desconocida.[5]

---

[1] DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3854 de 2016 [sitio web]. Bogotá D.C. [Consultado: 25 de octubre de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[2] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p.

[3] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Incidentes de Seguridad de la Información, Conceptos Básicos. ISO/IEC 27035. Bogotá D.C.: El Instituto, 2014. 2 p.

[4] Ibid, p. 2.

[5] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Políticas del Sistema de Gestión de Seguridad de la Información – SGSI [sitio web]. Bogotá D.C. [Consultado: 10 de octubre de 2022]. Disponible en: https://sigi.sic.gov.co/SIGI/files/mod_documentos/documentos/GS02-I06/versiones/POL%CDTICAS%20DEL%20SISTEMA%20DE%20GESTI%D3N%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%D3N%20-%20SGSI_V2.doc

EVIDENCIA: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.[6]

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos o fases para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.[7]

IMPACTO: Consecuencias que produce un incidente de seguridad sobre la organización.[8]

INCIDENTE O VIOLACIÓN DE SEGURIDAD DE LA INFORMACIÓN: Uno o varios eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer la confidencialidad, integridad y/o disponibilidad de la información.[9]

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.[10]

MODELO PARA LA GESTIÓN DE INCIDENTES: Estrategias enfocadas a orientar de forma estructurada la gestión de incidentes de seguridad en las organizaciones.[11]

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.[12]

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.[13]

---

[6] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Definiciones. ISO/IEC 27000. Bogotá D.C.: El Instituto, 2014. 2 p.
[7] Seguridad de la Información e Informática. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 25 de octubre2022] Disponible en: https://www.mineducacion.gov.co/1759/articles 322548_Manual__Gestion_de_Incidentes_de_Seguridad_de_la_Informacion_e_Informatica_.pdf
[8] Guía para la gestión de incidentes. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 25 de octubre2022] Disponible en: http://www.idep.edu.co/sites/default/files/Guia.pdf
[9] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Definiciones. ISO/IEC 27000. Bogotá D.C.: El Instituto, 2014. 2 p.
[10] Ibid, p.2.
[11] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Incidentes de Seguridad de la Información, Conceptos Básicos. ISO/IEC 27035. Bogotá D.C.: El Instituto, 2014. 4 p.
[12] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Definiciones. ISO/IEC 27000. Bogotá D.C.: El Instituto, 2014. 7 p.
[13] Ibid p.11.

5. NORMATIVIDAD

El presente Manual-Política se realiza en cumplimiento del Decreto 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

La Resolución 500 del 10 de marzo de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital".

En cumplimiento de la Norma ISO 27001:2013 y del ítem 16 de la Tabla 1 de los controles del Anexo A del estándar ISO/IEC 27001 y del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.

También se realiza en cumplimiento de la Norma ISO 27035:2020 Gestión de Incidentes de Seguridad de la Información.

6. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de Cundinamarca, entiende la importancia de gestionar los incidentes del Sistema de Gestión de Seguridad de la información - SGSI, por lo tanto, establece los lineamientos y acciones necesarias para la protección de la información a nivel institucional, articulado al esquema de Gestión de Incidentes del “Modelo de Seguridad y Privacidad de la información –MSPI” del MinTic, partiendo del monitoreo, reporte de eventos y/o incidentes que se presenten en los procesos que conforman el Modelo de Operación Digital de la Universidad de Cundinamarca, con el propósito de eliminar las causas que los generan y responder de forma eficiente a cada uno de ellos, logrando minimizar el impacto que estos puedan generar, como también erradicarlos y evitar que conlleven a la materialización de los riesgos de los activos de la información de la institución.

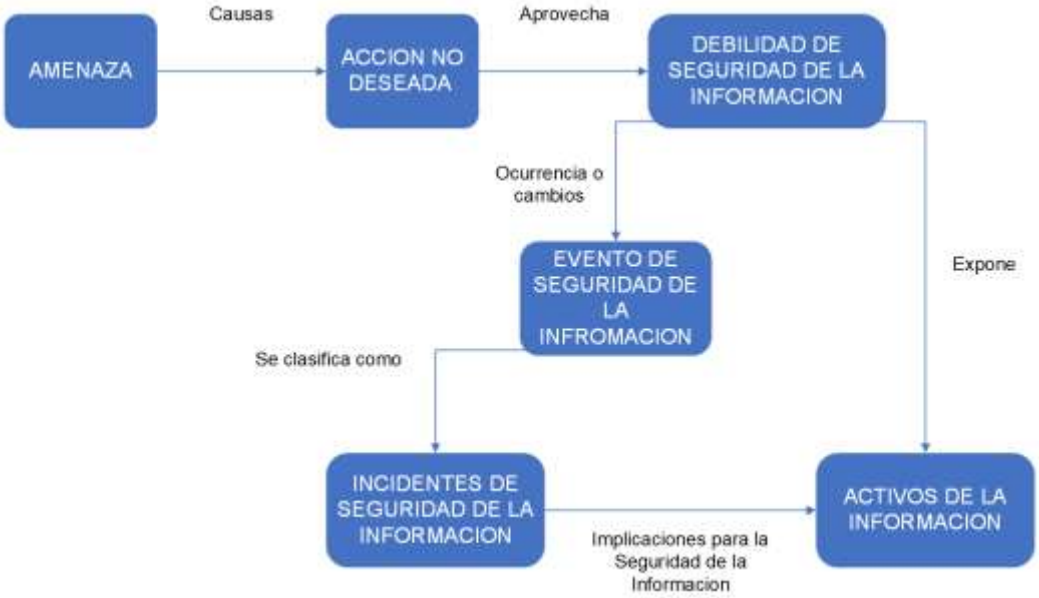
7. CONTEXTO GENERAL

Un evento de seguridad de la información es la posible representación de una circunstancia en un sistema y/o activo de información en el que se pueda evidenciar la violación a las políticas de seguridad de la información o una brecha en los controles a los activos de información dentro de la organización, sin embargo, estos eventos no necesariamente pueden comprometer o violar los principios de la seguridad de la información ya que no colocan en riesgo las operaciones de las organizaciones, ni tampoco la continuidad de estas, así como tampoco generan impacto de tipo legal y/o económico, por otra parte los incidentes de seguridad de la información en su gran

mayoría son posibles amenazas a los activos de información, ya que estos ocurren en sistemas, servicios o redes de información con debilidades y/o vulnerabilidades, por lo que son aprovechadas para la explotación y generación de un riesgo en la continuidad del negocio.

De acuerdo a lo expuesto anteriormente, dentro del contexto de la seguridad de la información, en la Universidad de Cundinamarca se pueden encontrar vulnerabilidades que no se hayan identificado en los sistemas, servicios o redes de información que se cuentan al interior de esta, propiciando que una amenaza pueda explotar una debilidad y/o vulnerabilidad e ir en contra del Manual de Políticas de Seguridad y Privacidad de la Información ESG-SSI-M001, sin embargo, en la institución se han venido aplicando los controles necesarios de acuerdo a la norma ISO/IEC 27001 y su Anexo A, con el objetivo de mitigar los riesgos ocasionados por la explotación de estas vulnerabilidades.

Figura 1. Relación de objetos en cadena de incidentes de seguridad de la información.



Fuente: GTC-ISO/ IEC 27035 - Guía Gestión de incidentes – MINTIC

En seguridad de la información, cuando un riesgo es tratado mediante la implementación de una técnica, se puede generar un riego residual, este tipo riesgos hacen alegoría a posibles eventos o incidentes que ocurren en los activos de información, que se han identificado al interior de la institución y donde el Procedimiento Gestión de Activos de Información ESG-SSI-P001, traza la ruta precisa que se tiene para identificación, clasificación, registro y consolidado de estos activos. Es por tal razón que en la figura 1, se describe la relación de objetos de una cadena de incidentes de seguridad que afecta los activos de información.

Una vez entendida la relación de todos los objetos que condicionan a la ocurrencia de un incidente de seguridad, la Universidad de Cundinamarca, a través del Sistema de Gestión de Seguridad de la Información-SGSI plantea la metodología para la gestión de incidentes desde el ciclo de vida y las fases en la atención, atendiendo la norma internacional ISO/ IEC 27035 y la Guía Gestión de incidentes del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, ya que se establece la pauta precisa, para seguir los parámetros más adecuados en el tratamiento de este tipo de eventos y/o incidentes. Como parte de las estrategias a seguir se deben tener en cuenta las siguientes acciones:

- Se deberán acoger los mecanismos necesarios para brindar protección a los activos de información en la institución.

- Cualquier funcionario de la institución, en sus diferentes modalidades de contratación, que evidencie un evento que atente contra los principios de seguridad de la información, deberá realizar el respectivo reporte al Sistema de Gestión de Seguridad de la Información – SGSI y/o el Área de Servicios Tecnológicos.

- Se deberá realizar el respectivo análisis a los eventos y/o incidentes de seguridad de la información, por medio de las estrategias adecuadas para identificar la presencia de estos.

- Verificar la respectiva ejecución de las acciones definidas en las fases de contención y mitigación a los incidentes que se presenten, con el fin de evaluar la eficacia de las soluciones implementadas.

- Se deberán documentar y clasificar los incidentes de seguridad de la información que se presenten en la Universidad de Cundinamarca.

- Se deberá realizar la respectiva documentación de las lecciones aprendidas durante el ciclo de vida del incidente.

- Comprobar que las consecuencias de los incidentes presentados hayan sido subsanadas con las partes involucradas al interior de la institución.

- Iniciar acciones post-incidentes con el propósito de efectuar mejoras a las actividades descritas en el procedimiento de gestión de incidentes de seguridad de la información

8. MODELO PARA LA GESTIÓN DE INCIDENTES

El modelo para la gestión de incidentes de seguridad de la información en la Universidad de Cundinamarca se desglosa por etapas, las cuales constan de preparación, detección y reporte, evaluación y decisiones, respuestas y por último lecciones aprendidas, como se observa a continuación:

Figura 2. Ciclo de la gestión de incidentes de seguridad de la información.

Fuente: GTC-ISO/ IEC 27035 - Guía Gestión de incidentes – MINTIC

9. PREPARACION

Dentro del Modelo de Gestión Integral de Seguridad de la Información, adoptado por la Universidad de Cundinamarca, se establece la etapa de gestión de incidentes, en donde, se cuenta con la fase de preparación, la cual es la más importante, ya que busca la planificación y revisión de todos los procesos, personas y acciones que se deben tener presente en la gestión de eventos y/o incidentes, con el propósito de eliminar las causas que los generan y responder de forma eficiente a cada uno de ellos, logrando minimizar el impacto que estos puedan generar, como también erradicarlos y evitar que conlleven en riesgo los activos de la información.

En esta fase se referencian todas las directivas y/o acciones que se tienen al interior de la institución para gestionar los eventos y/o incidentes de seguridad de la información con todas las partes de interés, razón por la cual, con el apoyo de la Dirección de Sistemas y Tecnología desde el Área de Servicios Tecnológicos y el área de Sistemas de Información, el Sistema de Gestión de Seguridad de la Información – SGSI ha establecido los siguientes procedimientos necesarios para dar cumplimiento a esta primera fase, los cuales se listan a continuación:

- Manual de Políticas de Seguridad y Privacidad de la Información - ESG-SSI-M001, donde se da a conocer las políticas del SGSI, así mismo el Programa Integral de Gestión de Datos Personales – PIGDP.
- Procedimiento de Gestión de incidentes de Seguridad de la Información - ESG-SSI-P009, en donde se establecen los requisitos y las actividades necesarias para la gestión de eventos y/o incidentes de seguridad.
- Procedimiento de Gestión de Riesgos de Seguridad y Privacidad de la Información - ESG-SSI-P12, en donde se establecen la metodología para la identificación, valoración y tratamiento de los riesgos relacionados a los activos de información.
- Manual de Roles y Responsabilidades en Seguridad y Privacidad de la Información - ESG-SSI-M004, donde se establece el Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información en su numeral 6.6.
- Plan Institucional de Sensibilización y Entrenamiento en Seguridad y privacidad de la Información - ESG-SSI-PL01, en donde se establece los lineamientos y directrices que a nivel institucional se deben adoptar para realizar la sensibilización y entrenamiento en seguridad y privacidad de la información de los funcionarios administrativos y docentes.
- Sistemas de Información - ASIP16, en donde se establece la innovación y renovación tecnológica a los Sistemas de Información de la institución y los servicios administrativos prestados a usuarios finales.
- Soporte, Mantenimiento y Monitoreo a la Infraestructura de Red y Recursos Tecnológicos -ASIP18, donde se establece la identificación, la gestión y el soporte la Infraestructura de Red y los Recursos Tecnológicos de la Universidad.

- Gestión de Acceso a los Sistemas de Información, Recursos Y Servicios Tecnológicos - ASIP20, donde se establece gestionar el acceso de usuarios a los Sistemas de Información, Recursos y Servicios Tecnológicos de la Institución.
- Copia de Seguridad de la Información - ASIP25, en donde se establece las actividades para la ejecución de copias de seguridad (proceso, seguimiento y recuperación de copias de seguridad) en los Activos de la Información de la Institución.
- Manual – Política de Uso Aceptable de Activos de Información - ESG-SSI-M011, donde se establece los lineamientos y directrices institucionales para el uso aceptable de los activos de información que pertenecen a la Universidad.

9.1. Detección y reporte

Esta fase consiste en la identificación de los cambios o eventos de seguridad en los sistemas, servicios o redes de información y la recolección de estos datos observados mediante el formato de registro que se tenga para tal fin (Reporte de eventos incidentes de seguridad de la información ESG-SSI-F036). En algunos casos no todos los eventos tienen la capacidad significativa de convertirse en posibles incidentes de seguridad de la información, por lo que es importante realizar el respectivo análisis de la situación reportada y/o detectada, sin embargo, no es tarea fácil determinar si se ha producido un incidente o no, por lo que se debe contar con las herramientas necesarias y el personal capacitado para llevar a cabo correctamente esta fase. De esta forma, la Universidad se cuentan con diferentes fuentes para realizar la detección de posibles incidentes de seguridad, algunas de estas son:

- Funcionarios con acceso a activos de información, tanto administrativos como docentes.
- Administradores de las herramientas tecnológicas con las que cuenta la institución, Dirección de Sistemas de Tecnológica – Área de Servicios Tecnológicos – Sistemas de Información.
- Notificaciones externas brindadas por proveedores de servicios.
- El Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información establecido por la Universidad, tiene la facultad de detectar e identificar los eventos y/o incidentes dentro de su campo de actuar.
- Boletines y alertas emitidas desde instancias gubernamentales como CSIRT Gobierno, PoNaL, entre otras.

9.2. Reporte de eventos y/o incidentes de seguridad de la información.

Una vez detectados los eventos y/o incidentes, los funcionarios con algún tipo de vínculo contractual con la Universidad, deberán reportar cualquier evento y/o incidente que pueda afectar la confidencialidad, integridad o disponibilidad de la de información, como lo estipula el Manual de Roles y Responsabilidades en Seguridad y Privacidad de la Información ESG-SSI-M004.

La recepción de eventos e incidentes de seguridad, se deberá realizar mediante las herramientas que se tengan para tal fin, como lo establecerá la **Guía para el reporte de eventos y/o incidentes de seguridad** y adicionalmente se podrán comunicar personalmente con los funcionarios pertenecientes al Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información, los cuales se encargarán de realizar el debido proceso para el tratamiento de estos.

9.3. Evaluación y decisiones

Siguiendo con el ciclo de vida de los eventos y/o incidentes de seguridad de la información y generando el reporte como producto de la detección de estos casos, se deberá establecer la evaluación de los eventos y su probabilidad significativa de convertirse en incidentes que puedan afectar los activos de información, a fin de reducir el impacto que se pueda producir la materialización de un incidente. En esta fase debe contar con un esquema estructurado donde se pueda conocer las actividades específicas para ejecutar y atender estos de manera precisa y concreta.

Es por esto por lo que, dentro de la Universidad de Cundinamarca se tiene establecido el Procedimiento Gestión de incidentes de Seguridad de la Información ESG-SSI-P009, donde se definen los lineamientos por medio de la documentación y divulgación necesaria para atender los eventos e incidentes de seguridad de la información de forma eficiente. Dentro del procedimiento en mención, se establece la actividad precisa para esta fase la cual corresponde a la clasificación de los eventos e incidentes de seguridad de la información a fin de verificar si los eventos que sean reportados, puedan convertirse en incidentes de acuerdo a su clasificación, la cual estará bajo la revisión de los funcionarios del **Equipo de Respuesta Inmediata a Incidentes de Seguridad** de la Información con el que la institución cuenta.

9.4. Clasificación de incidentes

Dentro del proceso de evaluación se deberá clasificar los incidentes de acuerdo a su respectivo análisis, para esto el Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información de la Universidad, establece los tipos de incidentes, los cuales se evidencian a continuación:

CLASIFICACION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		
CLASE DE INCIDENTE	**DESCRIPCION**	**TIPO DE INCIDENTE**
Accesos no autorizados	Intentos reales no autorizados, para acceder o utilizar correctamente un sistema, un servicio o red de información.	-Aprovechamiento de vulnerabilidades para acceder a bases de datos. - Violación a las medidas de seguridad física de la

CLASIFICACION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		
CLASE DE INCIDENTE	**DESCRIPCION**	**TIPO DE INCIDENTE**
		Universidad que dan como resultado acceso a la información. - Mala configuración de sistemas operativos, debido a cambios no controlados. - Intentos por recuperar archivos de contraseñas. - Ataques por desbordamiento de búfer para obtener acceso privilegiado a un objetivo.
Ingeniería Social	Ataques dirigidos a adquirir información fundamental, en algunas ocasiones a través de ingeniería social o de identificación de vulnerabilidades entre otros.	- Robo de información digital (carpetas, bases de datos) - Identificación de vulnerabilidades(scaning) - Sniffing - Phishing
Código malicioso (Malware)	Los códigos maliciosos identifican un programa informático o parte de éste insertado en otro programa, con la intención de modificar su comportamiento original.	- Virus, Gusanos, troyanos, spyware, rootkit, ransomware(secuestro de datos), códigos móviles y combinaciones de estos.
Abuso y/o uso inadecuado de los servicios de información	Incidente que ocurre cuando un usuario viola las políticas de la seguridad de la información. Ataques intencionados para dañar a la imagen de la institución o a utilizar medios electrónicos para usos ilegales.	- Descargar e instalar herramientas no autorizadas por la Dirección de Sistemas y Tecnología. - Usar el correo institucional para generar Spam o para la promoción de negocios personales. - Usar recursos institucionales para crear un sitio web no autorizado. - Generar actividades entre funcionarios para adquirir o distribuir archivos piratas (música, video, software).

CLASIFICACION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		
CLASE DE INCIDENTE	**DESCRIPCION**	**TIPO DE INCIDENTE**
		- Acceso no autorizado de información.
Borrado de información (Compromiso)	Incidentes relacionados con el acceso y fuga(Confidencialidad), modificación o borrado(Integridad) de información no pública.	- Modificación y borrado no autorizado de información. - Publicación no autorizada de información.
Denegación de Servicio (Dos/DDoS) (Disponibilidad)	Incidentes provocados en un sistema, servicio o red de información, que dejan de operar en su capacidad prevista consumiendo sus recursos (Memoria RAM, CPU, capacidad almacenamiento y recursos de red) que inhabilitan el acceso a usuarios.	- Violaciones a las medidas de seguridad físicas que resultan en robo o daño intencionado y destrucción de equipos. - Sobrecarga y/o mal funcionamiento de los sistemas de información, software y hardware. - Degradación de los servicios por falla externa de proveedores. - Cambio en las condiciones ambientales por ejemplo altas temperaturas que puedan afectar a equipos encargados de proveer servicios a la institución. - Daño accidental al hardware por incendio o daño por agua(inundación.)
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diferentes tecnologías con el fin de ingresar en forma fraudulenta en sistemas de información y sitios web de la institución.	- Defacement (desfiguración) - Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF) - Falsificación de petición entre sitios cruzados - Inyección SQL - Spear Phishing - Pharming - Ataque de fuerza bruta

CLASIFICACION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		
CLASE DE INCIDENTE	**DESCRIPCION**	**TIPO DE INCIDENTE**
		- Inyección de Ficheros Remota - Explotación de vulnerabilidad software. - Explotación de vulnerabilidad hardware.
Multicomponente	Situaciones en las que se involucran más de una clase de incidentes.	- Incidentes mencionados anteriormente en esta tabla de clasificación.
Otros	Situaciones en las que no se puede categorizar los incidentes dentro de las categorías mencionadas anteriormente.	- Eventos y/o situaciones de seguridad de la información donde se crea que se está infringiendo las políticas de seguridad de la Información.

Tabla 1. Categorizaciones de incidentes de seguridad de la información.

En el proceso de clasificación de los incidentes que se puedan presentar en la institución, los cuales se mencionaron con anterioridad, es indispensable la correcta categorización, ya que se debe priorizar la atención y la forma en la que estos puedan impactar la continuidad de las operaciones de la Universidad generando consecuencias negativas ya sean de imagen, legales entre otros.

9.5. Priorización de incidentes de seguridad según su impacto

La Universidad de Cundinamarca entendiendo los efectos adversos que pueden generar los incidentes de seguridad en los activos de información y la importancia que estos tienen para la institución, como también los niveles de impacto provenientes del análisis de riesgos de estos activos, establece la priorización en atención a incidentes de acuerdo con 5 niveles de criticidad e impacto , así como se observa en la Tabla 2 y 3, a fin de atenderlos de acuerdo con la necesidad requerida y brindar la contención y erradicación de estos, es importante resaltar que será el equipo de respuesta inmediata a incidentes de seguridad de la información los encargados de priorizar estos incidentes.

NIVEL DE CRITICIDAD	VALOR	DESCRIPCIÓN
Muy Bajo	1	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.

NIVEL DE CRITICIDAD	VALOR	DESCRIPCIÓN
Bajo	2	Sistemas que apoyan a una sola dependencia o proceso de la institución.
Medio	3	Sistemas que apoyan más de una dependencias o procesos de la institución.
Alto	4	Sistemas pertenecientes a la Dirección de Sistemas de Tecnología – Sistemas de Información - Área de Servicios Tecnológicos y estaciones de trabajo de usuarios con funciones críticas.
Muy Alto	5	Sistemas Críticos (de acuerdo al análisis de los activos de información)

Tabla 2. Niveles de criticidad de los activos de información

NIVEL DE CRITICIDAD	VALOR	DESCRIPCIÓN
Muy Bajo	1	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	2	Sistemas que apoyan a una sola dependencia o proceso de la institución.
Medio	3	Sistemas que apoyan más de una dependencias o procesos de la institución.
Alto	4	Sistemas pertenecientes a la Dirección de Sistemas de Tecnología – Sistemas de Información - Área de Servicios Tecnológicos y estaciones de trabajo de usuarios con funciones críticas.
Muy alto	5	Sistemas Críticos (de acuerdo al análisis de los activos de información)

Tabla 3. Niveles de criticidad de Impacto

9.6. Respuesta, contención, erradicación y recuperación.

En esta etapa el Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información establecido por la institución, serán los funcionarios encargados de brindar la oportuna respuesta del manejo de los incidentes que se presenten en la institución y según la clasificación, la criticidad y el impacto que estos puedan generar, brindarán la oportuna comunicación a las áreas involucradas y les darán el cierre oportuno una vez se erradique el incidente.

9.7. Contención, erradicación y recuperación

Dentro de la etapa de contención de incidentes, la institución permite dar la correcta protección a los sistemas, servicios o redes de información esenciales dentro de los procesos que se llevan al interior, de tal forma que se pueda limitar el daño que estos incidentes puedan generar en los activos de información, como también evitar la propagación y que de acuerdo a esto se puedan erradicar y recuperar de los activos afectados. En el proceso de recuperar los estados actuales de los sistemas, servicios o redes de información afectados por materialización de incidentes, se busca propiciar el restablecimiento total de sus funcionalidades y además prevenir incidentes con patrones similares a futuro, en la siguiente tabla se muestra las estrategias referentes a la contención, erradicación y recuperación de incidentes de seguridad de la información de acuerdo a su criticidad y su nivel de impacto.

Clase de incidente	Ejemplos de incidentes	Nivel de criticidad	Nivel de impacto	Estrategias de contención	Estrategias de erradicación y recuperación
Código malicioso (Malware)	Virus, Gusanos, troyanos, spyware, rootkit, rasonware (secuestro de datos), códigos móviles y combinaciones de estos.	ALTO	MUY ALTO	Desconexión de la red, del o las estaciones de trabajo afectadas.	Corrección de efectos producidos, restauración de backups, reinstalación de sistemas operativos y recuperación de datos.
Ingeniería Social	Robo de información digital (carpetas, bases de datos), Identificación de vulnerabilidades(scaning)Sniffing, Phishing	ALTO	MUY ALTO	Desconexión del recurso compartido.	Recuperación de información a partir de copias de seguridad.

Clase de incidente	Ejemplos de incidentes	Nivel de criticidad	Nivel de impacto	Estrategias de contención	Estrategias de erradicación y recuperación
Abuso y/o uso inadecuado de los servicios de información	Descargar e instalar herramientas para la piratería informática. Usar el correo institucional para generar Spam o para la promoción de negocios personales. Usar recursos institucionales para crear un sitio web no autorizado. Usar actividades entre funcionarios para adquirir o distribuir archivos piratas (música, video, software). Acceso no autorizado	ALTO	ALTO	Uso de políticas de Seguridad y Privacidad de la Información .(Privilegios de roles de acceso a sistemas, servicios y/o redes)	Aplicación de políticas y/o reglas en dispositivos de seguridad perimetral (Firewall, routers entre otros.)

Clase de incidente	Ejemplos de incidentes	Nivel de criticidad	Nivel de impacto	Estrategias de contención	Estrategias de erradicación y recuperación
	de información.				
Borrado de información	Modificación y borrado no autorizado de información, publicación no autorizada de información.	MUY ALTO	ALTO	Desconexión del recurso compartido, suspender o eliminar la publicación no autorizada	Recuperación de datos.
Accesos no autorizados	Intentos por recuperar archivos de contraseñas. Aprovechamiento de vulnerabilidades para acceder a bases de datos. Violación a las medidas de seguridad física de la Universidad que dan como resultado	ALTO	ALTO	Evaluación de apagado de sistemas.	Cambios de contraseñas, aplicaciones de nuevas políticas y y/o reglas en dispositivos de seguridad perimetral (Firewall, video vigilancia, entre otros.) Habilitación de factores de autentificación.

Clase de incidente	Ejemplos de incidentes	Nivel de criticidad	Nivel de impacto	Estrategias de contención	Estrategias de erradicación y recuperación
	acceso a la información. Mala configuración de sistemas operativos, debido a cambios no controlados. Ataques por desbordamiento de búfer para obtener acceso privilegiado a un objetivo.				
Denegación de Servicio (Dos/DDoS) (Disponibilidad)	Daño accidental al hardware por incendio o daño por agua(inundación.) Sobrecarga y/o mal funcionamiento de los sistemas de información,	MUY ALTO	MUY ALTO	Restricción de accesos físicos y lógicos.	Restitución del servicio caído.

Clase de incidente	Ejemplos de incidentes	Nivel de criticidad	Nivel de impacto	Estrategias de contención	Estrategias de erradicación y recuperación
	software y hardware. Cambio en las condiciones ambientales por ejemplo altas temperaturas que puedan afectar a equipos encargados de proveer servicios a la institución.				
Intrusiones	Compromiso de cuenta de usuario. Defacement (desfiguración), Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados	ALTO	ALTO	Incorporación de reglas de filtrado en firewall y evaluación de desconexión de los sistemas y/o recursos afectados.	Reinstalación de parches de seguridad, Reparación de sitios web.

Clase de incidente	Ejemplos de incidentes	Nivel de criticidad	Nivel de impacto	Estrategias de contención	Estrategias de erradicación y recuperación
	Inyección SQL Spear Phishing, Pharming Ataque de fuerza bruta Inyección de Ficheros Remota Explotación de vulnerabilidad software. Explotación de vulnerabilidad hardware.				
Multicomponente	Incidentes mencionados anteriormente en esta tabla de clasificación.	Varía dependiendo los incidentes que apliquen	Varía dependiendo los incidentes que apliquen	Estas estrategias aplican dependiendo los incidentes que apliquen.	Estas estrategias aplican dependiendo los incidentes que apliquen.
Otros	Eventos y/o situaciones donde se presentan eventos y/o situaciones de seguridad de la informació	Varía dependiendo los incidentes que apliquen	Varía dependiendo los incidentes que apliquen	Estas estrategias aplican dependiendo los incidentes que apliquen.	Estas estrategias aplican dependiendo los incidentes que apliquen.

Clase de incidente	Ejemplos de incidentes	Nivel de criticidad	Nivel de impacto	Estrategias de contención	Estrategias de erradicación y recuperación
	n donde se crea que se está infringiendo las políticas de seguridad de la Información.				

Tabla 3. Estrategias de contención, erradicación y recuperación.

9.8. Lecciones aprendidas

En esta última instancia del ciclo de vida de los incidentes, inicia cuando estos se han solucionado y a través de los mismos se genera el aprendizaje y la recopilación de información que ayuda a generar estrategias de mejora en los procesos que se han visto comprometidos. El Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información, serán los responsables de identificar las lecciones aprendidas y de ser necesario la aplicación de controles y/o medidas de seguridad de la información, en trabajo conjunto con los procesos involucrados de la institución. De igual forma, otras actividades a realizar por el equipo serán las siguientes:

- Generación de consolidado de eventos y/o incidentes de seguridad de la información con el propósito de servir como base del conocimiento.
- Identificación y aplicación de acciones correctivas para prevenir nuevos incidentes.
- Identificación y realización de mejoras al esquema de incidentes de seguridad de la información con el que cuenta la Universidad, dentro de estas mejoras al esquema, se deberán revisar procedimientos, manuales, formatos de reportes y los que apliquen.
- Generar informes en caso de requerirse, los cuales serán brindados a las partes interesadas de la institución.

10. BIBLIOGRAFÍA Y WEBGRAFÍA

DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3854 de 2016 [sitio web]. Bogotá D.C. [Consultado: 25 de octubre de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Incidentes de Seguridad de la Información, Conceptos Básicos. ISO/IEC 27035. Bogotá D.C.: El Instituto, 2014. 2 p.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Seguridad de la información e informática. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 25 de octubre2022] Disponible en: https://www.mineducacion.gov.co/1759/articles322548_Manual__Gestion_de_Incidentes_de_Seguridad_de_la_Informacion_e_Informatica_.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la gestión de incidentes. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 25 de octubre2022] Disponible en: http://www.idep.edu.co/sites/default/files/Guia.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Políticas del Sistema de Gestión de Seguridad de la Información – SGSI [sitio web]. Bogotá D.C. [Consultado: 10 de octubre de 2022]. Disponible en: https://sigi.sic.gov.co/SIGI/files/mod_documentos/documentos/GS02-I06/versiones/POL%CDTICAS%20DEL%20SISTEMA%20DE%20GESTI%D3N%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%D3N%20-%20SGSI_V2.doc

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2022	12	13	Emisión del documento
2	2023	03	31	Se genera actualización referente a cambios en la Política y se realiza cambios de estructuración a nivel de objetivos.

ELABORÓ	
NOMBRES Y APELLIDOS	CARGO
Jhon Alexander Cristancho Córdoba	Técnico

REVISÓ	
NOMBRES Y APELLIDOS	CARGO
María del Pilar Delgado Rodríguez	Coordinadora del SGSI Profesional Universitario I

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del SGSI Profesional Universitario I	2023	03	31

OBJETIVO:	Garantizar la adecuada gestión de eventos y/o incidentes de seguridad de la información en la Universidad de Cundinamarca, adoptando la metodología propuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones, la cual comprende un enfoque por etapas del ciclo de vida de gestión de incidentes, las cuales son: Preparación, Detección, Evaluación y Análisis, Contención, Erradicación y Recuperación y Actividades Post-incidente. Este enfoque permitirá gestionar, mitigar y reducir la probabilidad de que un evento se materialice generando un incidente que puede tener un impacto significativo en la institución, comprometiendo la Confidencialidad, Integridad y Disponibilidad de la Información.
ALCANCE:	Este procedimiento aplica en todos los procesos, servicios, talento humano, infraestructura tecnológica e instalaciones de la Universidad de Cundinamarca, ante el caso de notificación de un evento y/o incidente que amenace la seguridad de la información.
LÍDER DE PROCEDIMIENTO:	Coordinadora del Sistema de Gestión de Seguridad de la Información - SGSI

DEFINICIONES

ACTIVIDAD POST - INCIDENTE: Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores. [1]

CICLO DE VIDA DE GESTIÓN DE INCIDENTES: El ciclo de vida de Gestión de Incidentes de seguridad de la información permite tener un enfoque estructurado y bien planificado para el manejo adecuado de eventos y/o incidentes de seguridad de la información.[2]

[1] Ministerio de las Tecnologías de la Información y Comunicaciones. (2016). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [PDF]. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[2] Ministerio de las Tecnologías de la Información y Comunicaciones. (2021). Documento Maestro - Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [PDF]. https://gobiernodigital.mintic.gov.co/692/articles-237908_maestro_mspi.pdf

DEFINICIONES

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [3]

CONTENCIÓN, ERRADIACION Y RECUPERACIÓN: La entidad debe implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.[4]

CONTROL: Medida para modificar el riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones para modificar el riesgo. [ISO 27000:2014]. Control se usa como sinónimo de salvaguardo o contramedida. [5]

CSIRT: Cyber Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad de la Información), el cual se encarga de gestionar de forma eficiente el daño resultante de incidentes, así como también proveer de respuesta y recuperación efectiva, ante estos.[6]

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [7]

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia o cambio de circunstancias identificadas en un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, falla de los controles o una situación desconocida.[8]

[3] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html
[4] GUÍA 21 de Gestión de Incidentes [sitio web] [Consultado: 02 de agosto de 2023] articles-5482_Modelo_de_Seguridad_Privacidad
[5] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html
[6] DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3995 de 2020 [sitio web]. Bogotá D.C. [Consultado: 20 de septiembre de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf
[7] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html
[8] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html

DEFINICIONES

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos o fases para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.[9]

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud. [10]

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [11]

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. [12]

REQUISITOS Y CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

La Universidad de Cundinamarca, consciente de la importancia de proteger sus activos de información, atiende y enfrenta los posibles eventos y/o incidentes de seguridad de la información, a partir de las amenazas y vulnerabilidades que puedan acarrear la perdida de confidencialidad, integridad y/o disponibilidad de la información. Por lo tanto, se hace necesario contar unas actividades documentadas que permitan gestionar los eventos y/o incidentes que puedan ocurrir al interior de la institución, articulados con el ciclo de vida de gestión de incidentes, documentado en la Guía No.21 “Gestión y Clasificación de Incidentes de Seguridad de la Información”, que comprende las etapas de Preparación, Detección, Evaluación y Análisis, Contención, Erradicación y Recuperación, y las Actividades Post-Incidente.

[9] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html

[10] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html
[11] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html
[12] ISO27000.ES. Glosario [sitio web] [Consultado: 18 de marzo de 2024]. Disponible en: https://www.iso27000.es/glosario.html

REQUISITOS Y CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

En este contexto, el Sistema de Gestión de Seguridad de la Información – SGSI, presenta los siguientes lineamientos relacionados a la gestión y tratamiento de eventos y/o incidentes de seguridad de la información:

- Se deben tener en cuenta los roles y responsabilidades documentados en el Manual ESG-SSI-M004 – “ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.”

- El Equipo de Respuesta a Incidentes de Seguridad de la Información – CSIRT, conformado por los ingenieros de la Dirección de Sistemas y Tecnología vinculados al Área de Servicios Tecnológicos y los ingenieros del Sistema de Gestión de Seguridad de la Información - SGSI, deberán hacer la identificación y/o evaluación del incidente, en donde se caracteriza si hace referencia a un incidente de seguridad o privacidad de la información.

- Es responsabilidad de los funcionarios administrativos y docentes en todas las modalidades de contratación, deben reportar al Área de Servicios Tecnológicos adscrita a la Dirección de Sistemas y Tecnología y al Sistema de Gestión de Seguridad de la Información - SGSI, cualquier irregularidad que se considere un evento o un posible incidente en seguridad o privacidad de la información, por los canales dispuestos para tal fin y que atente contra los principios de seguridad de la información.

- Una vez el CSIRT o quien haga sus veces, sea notificado de un evento y/o incidente en seguridad de la información, procederán de acuerdo con las actividades descritas en el presente procedimiento, para atender y dar respuesta ante la posible materialización de un riesgo que comprometa la Confidencialidad, Integridad y/o Disponibilidad de la información.

- Se establece como control ante los eventos y/o incidentes de seguridad de la información, incluir en el ESG-SSI-PL01 - Plan institucional de sensibilización y entrenamiento en seguridad y privacidad de la información, las estrategias de cómo abordar y tratar los incidentes de seguridad de la información por parte de los funcionarios administrativos y docentes en todas sus modalidades de contratación.

- Para fortalecer y atender los eventos y/o incidentes de seguridad de la información, se estableció y fue aprobado por la alta dirección el rol de vigía de seguridad de la información, el cual deberá reportar los incidentes de

REQUISITOS Y CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

seguridad o privacidad de la información, que evidencien al interior de la institución, al Equipo de Respuesta a Incidentes de Seguridad de la Información – CSIRT, en las herramientas que se dispongan para tal fin.

- De presentarse un incidente que sobre pase las capacidades técnicas y tecnológicas de la institución, el CSIRT o quien haga sus veces, podrá contactar a los grupos de apoyo como autoridades, grupos de interés externos que manejen asuntos relacionados a incidentes de seguridad de información para dar solución al mismo.

- Este procedimiento tiene como referencia el control A.16 “Gestión de incidentes de seguridad de la Información” de la Norma ISO 27001:2013 y la Guía No.21 “Gestión y Clasificación de Incidentes de Seguridad de la Información” del MINTIC.

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
1. Recepcionar las notificaciones de eventos de seguridad y/o privacidad de la información que vulneren la confidencialidad, integridad y disponibilidad de la información, de acuerdo con la etapa No.1 del ciclo de vida de gestión de incidentes.	Equipo de respuesta a incidentes de Seguridad de la Información CSIRT	Se establece un plazo de tres (3) días hábiles para que el CSIRT (Equipo de Respuesta a Incidentes de Seguridad de la Información) brinde respuesta al reporte por medio de los canales de comunicación institucionales. Sin embargo, se aclara que, de acuerdo con la naturaleza y gravedad del caso, se pueden ampliar los tiempos de respuesta.	Guía 21 – Gestión de Incidentes. MinTIC	Reportes por medios de comunicación institucional: (Correo electrónico, línea telefónica, comunicación verbal.)
Si el evento notificado está relacionado con un incidente de seguridad en el tratamiento de datos personales, se solicita dirigirse al procedimiento ESG-SSI-P10 - GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES. De lo contrario, se da continuidad al procedimiento de gestión de incidentes de seguridad de la información con la actividad No.2.				
2. Realizar el Análisis y la Evaluación del evento y/o incidente de seguridad de la información allegado, de acuerdo con la etapa No.2 del ciclo de vida de gestión de incidentes.	Equipo de respuesta a incidentes de Seguridad de la Información. CSIRT	Evaluación del nivel de impacto, priorización de atención y tiempos estimados de respuesta del evento y/o incidente de seguridad de la información allegado al equipo CSIRT con el fin de brindar una atención oportuna.	Guía 21 – Gestión de Incidentes. MinTIC **ESG-SSI-F036** **ESG-SSI-F035**	Correo electrónico y medios de comunicación institucionales **ESG-SSI-r036** **ESG-SSI-r035**

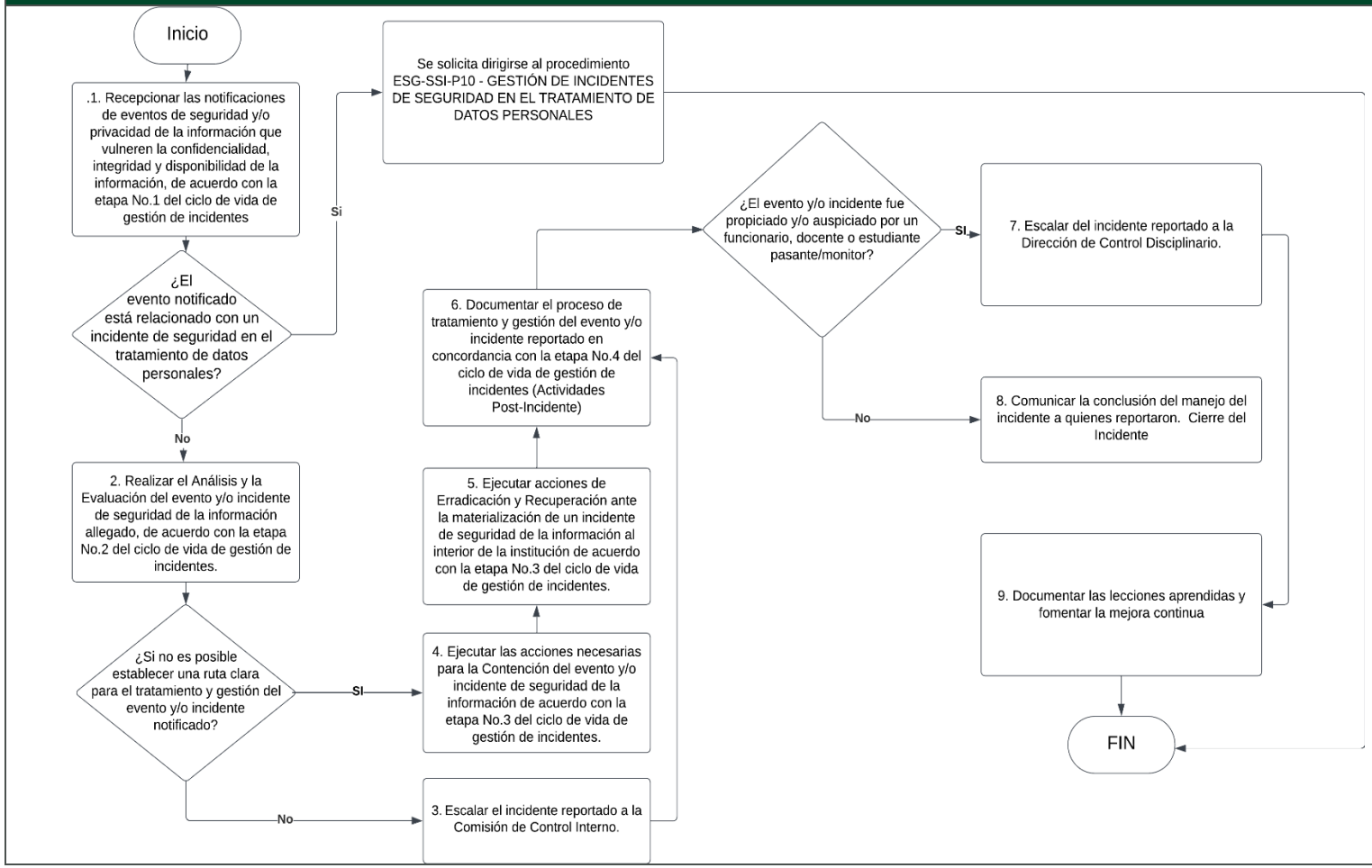
ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
Si el evento y/o incidente notificado no ha materializado un riesgo de seguridad de la información, pero no es posible establecer una ruta clara para el tratamiento y gestión de este, el Sistema de Gestión de Seguridad de la Información – SGSI, procederá con el escalado del caso a la Comisión de Control Interno de la Universidad de Cundinamarca, mediante la actividad No.3 de este documento para la continuidad del tratamiento del incidente y llevar a cabo las acciones pertinentes para la respuesta y cierre del mismo. De lo contrario, se da continuidad al procedimiento de gestión de incidentes con la actividad No.4.				
3. Escalar el incidente reportado a la Dirección de Control Interno.	Equipo de respuesta a incidentes de Seguridad de la Información CSIRT	La Dirección de Control Interno en trabajo articulado con el Sistema de Gestión de Seguridad de la Información, establecerá una ruta procedimental para el tratamiento del evento y/o incidente reportado cuando no se tiene claridad de las acciones necesarias y no se ha materializado el riesgo.	**ESG-SSI-F036** **ESG-SSI-F035** **ADOF006** **ADOF010** Correo electrónico y medios de comunicación institucionales	**ESG-SSI-r036** **ESG-SSI-r035** **ADOr006** **ADOr010** Correo electrónico y medios de comunicación institucionales
4. Ejecutar las acciones necesarias para la Contención del evento y/o incidente de seguridad de la información de acuerdo con la etapa No.3 del ciclo de vida de gestión de incidentes.	Equipo de respuesta a incidentes de Seguridad de la Información. CSIRT	Realizar todas las acciones pertinentes durante la gestión del caso para el debido y oportuno tratamiento del evento y/o incidente reportado al interior de la institución, minimizando su impacto en caso de materializarse. Esto puede incluir la restauración del Sistema(s), Servicio(s) y/o Redes de Información u otras acciones aplicables según el caso reportado.	Guía 21 – Gestión de Incidentes. MinTIC	Correo electrónico y medios de comunicación institucionales Solicitudes de requerimientos de seguridad de la infraestructura TI al área de servicios tecnológicos

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
				Visitas de vigías de seguridad y/o el equipo CSIRT
5. Ejecutar acciones de Erradicación y Recuperación ante la materialización de un incidente de seguridad de la información al interior de la institución de acuerdo con la etapa No.3 del ciclo de vida de gestión de incidentes.	Equipo de respuesta a incidentes de Seguridad de la Información CSIRT	Identificar si se requieren actividades complementarias para el tratamiento de los incidentes de seguridad de la información, con el fin de restablecer la normalidad y continuidad de las actividades internas de la institución.	Guía 21 – Gestión de Incidentes. MinTIC **ESG-SSI-F035**	Correo electrónico y medios de comunicación institucionales Solicitudes de requerimientos de seguridad de la infraestructura TI al área de servicios tecnológicos Visitas de vigías de seguridad y/o el equipo CSIRT **ESG-SSI-r035**
6. Documentar el proceso de tratamiento y gestión del evento y/o incidente reportado en	Equipo de respuesta a incidentes de	Registro y consolidado de reportes de los eventos y/o incidentes de seguridad de la información que se han	**ESG-SSI-F036 ESG-SSI-F037 ESG-SSI-F035 ADOF006**	**ESG-SSI-r036 ESG-SSI-r037 ESG-SSI-r035 ADOr006**

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
concordancia con la etapa No.4 del ciclo de vida de gestión de incidentes (Actividades Post-Incidente)	Seguridad de la Información CSIRT	gestionado a través del CSRIT, como base de conocimiento para registrar el desarrollo de cada evento y/o incidente presentado.	**ADOF010**	**ADOr010**
Si el incidente que conlleva a la materialización de un riesgo de seguridad de la información propiciado o auspiciado por un funcionario administrativo, docente o por estudiantes en modalidad de pasantes y monitores, el "Equipo de Respuesta a Incidentes de Seguridad de la Información", procederá con el escalado del caso a la Comisión de Control Interno y la Dirección de Control Disciplinario de la Universidad de Cundinamarca mediante la actividad No.7 de este documento, para la continuidad del tratamiento del incidente y llevar a cabo las acciones pertinentes para la respuesta y cierre del mismo. De lo contrario, se da continuidad al procedimiento de gestión de incidentes con la actividad No.8.				
7. Escalar del incidente reportado a la Dirección de Control Disciplinario.	Equipo de respuesta a incidentes de Seguridad de la Información CSIRT	En conformidad a la ruta procedimental emitida por la Dirección de Control Disciplinario en articulación con el Sistema de Gestión de Seguridad de la Información, se establece el canal de comunicación directa para el tratamiento, gestión y cierre de los incidentes de seguridad de la información en los cuales se requiera la intervención de esta Dirección.	Acuerdo 003 de 2020 "Por el cual se adopta el estatuto disciplinario del personal académico y administrativo de la Universidad de Cundinamarca". **ESG-SSI-F036** **ESG-SSI-F035**	**ESG-SSI-r036** **ESG-SSI-r035** Correo electrónico y medios de comunicación institucionales
8. Comunicar la conclusión del manejo del incidente a quienes reportaron. Cierre del Incidente	Equipo de respuesta a incidentes de	Notificar la solución del incidente involucrando el impacto y las buenas prácticas para su prevención, de ser necesario, se	**ESG-SSI-F036** **ESG-SSI-F037** **ESG-SSI-F035** **ADOF006**	**ESG-SSI-r036** **ESG-SSI-r037** **ESG-SSI-r035** **ADOr006**

ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
	Seguridad de la Información CSIRT	debe comunicar las lecciones aprendidas.	**ADOF010** Correo electrónico y medios de comunicación institucionales	**ADOr010** Correo electrónico y medios de comunicación institucionales
9. Documentar las lecciones aprendidas y fomentar la mejora continua	Equipo de respuesta a incidentes de Seguridad de la Información CSIRT	El incidente de seguridad de la información debe haberse tratado satisfactoriamente y deben proponerse mecanismos para reducir, mitigar y/o prevenir la ocurrencia de estos.	Guía 21 – Gestión de Incidentes. MinTIC **ESG-SSI-F036** **ESG-SSI-F037**	**ESG-SSI-r036** **ESG-SSI-r037**

DIAGRAMA DE FLUJO



SISTEMAS DE INFORMACIÓN			
SISTEMA DE INFORMACIÓN	**DESCRIPCIÓN**	**FRECUENCIA**	**UBICACIÓN**
No aplica	No aplica	No aplica	No aplica

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2021	02	23	Emisión del Documento. Transición del ASIP29.
2	2022	02	16	Actualización de documentos de referencia por interacción con documentación obsoleta.
3	2022	12	13	Se incluye requisitos y condiciones general para el desarrollo del procedimiento. Se actualizó los roles y responsabilidades durante el proceso de gestión de incidentes. Se estableció nuevas actividades para atender los eventos y/o incidentes de seguridad de la información acorde con la fase de gestión.
4	2023	04	28	Se hace corrección de estilo a las actividades y se agrega como documento de referencia en la actividad No.1 la Guía Para El Diligenciamiento Del Reporte De Eventos Y O Incidentes De Seguridad De La Información - ESG-SSI-G006
5	2023	11	20	Se ajustó la redacción y el contenido del objetivo general y el alcance de este procedimiento, se suprimió y modificaron algunos de los requisitos y condiciones, se agregaron definiciones, y se modificó el contenido de las actividades de gestión de incidentes y su respectivo diagrama de flujo.
6	2024	04	04	Se revisó el objetivo general, alcance y actividades del procedimiento, se agregaron y suprimieron definiciones de acuerdo con el contexto del procedimiento, se reestructuro el apartado de requisitos y condiciones y se modificó el contenido de las actividades de la gestión de incidentes de seguridad de la información y su respectivo diagrama de flujo.

ELABORÓ	
NOMBRES Y APELLIDOS	CARGO
Fabián Libardo Parra Gutiérrez	Técnico
Brayan Esteban Ortegón Palomino	Técnico

REVISÓ	
NOMBRES Y APELLIDOS	CARGO
María del Pilar Delgado Rodríguez	Coordinadora del SGSI Profesional Universitario I

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del SGSI Profesional Universitario I	2024	04	04