Unidad para las Víctimas

Guía para la Gestión ante el Incumplimiento de las Políticas de Seguridad de la Información

Procedimiento Seguridad de la Información

2024

Oficina de Tecnologías de la Información

1. OBJETIVO

Establecer una guía para gestionar el incumplimiento de los controles de seguridad de la información para prevenir y corregir conductas que sean objeto de sanciones por incumplimiento de las obligaciones o funciones de los funcionarios, contratistas y proveedores de la Unidad para la Atención y Reparación Integral para las Victimas (UARIV), en el marco de la Política de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información (MSPI).

2. ALCANCE

Está dirigido a todos los funcionarios, contratistas y proveedores de todas las direcciones territoriales y aplica para todos los procesos de la UARIV y grupos de interés que accedan a los activos de información de la entidad; ya que el propósito es prevenir y corregir las posibles afectaciones a los activos de información.

3. DEFINICIONES

- **Activo de información:** Es todo aquel recurso tangible o intangible que tenga valor o importancia para la entidad, de acuerdo con la tipificación definida.

- **Confidencialidad:** Consiste en garantizar que el activo de información no esté disponible o sea divulgado por personas, entidades o procesos NO autorizados.

- **Integridad:** Consiste en asegurar o salvaguardar que el activo de información cuente con las propiedades de: exactitud, precisión, consistencia, confiabilidad y autenticidad.

- **Disponibilidad:** Consiste en garantizar que el activo de información esté accesible y utilizable en el momento oportuno que se requiera bajo la demanda de personas, entidades o procesos.

- **Acuerdo de Confidencialidad:** Documento anexo suscrito entre los funcionarios, contratistas y proveedores de la Unidad para la Atención y Reparación Integral a las Victimas, con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

- **Copia de seguridad (BACKUP):** En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.

ACTIVIDADES:

La finalidad y los principios de esta guía tienen como objetivo prevenir y corregir conductas previas ante el incumplimiento de las políticas de seguridad de la información de la UARIV y orientar la ejecución y cumplimiento de la Política de Seguridad y Privacidad de la Información y demás políticas relacionadas con esta, a través de los siguientes lineamientos:

- Propender la Seguridad de la información de la UARIV a través del equipo de Seguridad de la Información de la Oficina de Tecnologías de la Información (OTI) la cual será

encargada de establecer, implementar y mantener una mejora continua que permita las medidas preventivas y de reacción del individuo, la entidad y las tecnologías, para proteger la información y salvaguardar principios como la confidencialidad, autenticidad, integridad y disponibilidad.

- Velar por el cumplimiento de los acuerdos de confidencialidad, integridad y disponibilidad de la información de la UARIV por parte de los funcionarios, contratistas y proveedores pertenecientes a la Entidad, teniendo en cuenta el principio de equivalencia funcional con fundamento en la Ley 527 de 1999.

- Velar por las copias de seguridad del evento o incidente suscitado como parte integral del proceso en tema de registro y evidencias.

- Realizar las indagaciones o investigaciones necesarias según el caso, para sancionar las conductas que trasgrede, el Reglamento Interno de Trabajo de la UARIV y la ley penal colombiana, relacionadas con la infracción de las políticas y procedimientos definidos en la Política de Seguridad y Privacidad de la entidad, dentro del marco del debido proceso consagrado en el artículo 29 de la Constitución Política de Colombia en aras de adelantar un procedimiento transparente y objetivo que tenga como finalidad proteger los activos de la información de la entidad y el respeto de los derechos fundamentales de las personas vinculadas en las diligencias.

- Iniciar las acciones legales internas o externas, por medio de la Oficina de Control Interno Disciplinario, pertinentes por el acceso no autorizado a los activos de información y los eventos o incidentes de seguridad al incumplimiento de esta política, como el incumplimiento de los principios acá mencionados.

NORMA DE CLASIFICACIÓN PROVISIONAL DE CARGOS

Cuando se inicie un análisis de evento o incidente suscitado, la persona vinculada al proceso deberá ser notificada por escrito de las presuntas infracciones cometidas, que son objeto de verificación, para que pueda ejercer el derecho de defensa con fundamento en el artículo 29 de la constitución política de Colombia.

De acuerdo con las leyes aplicables a servidores públicos se definen las sanciones por incumplimientos a las políticas de seguridad de la información del UARIV**,** La sanción puede ser aplicada por "Acción y/u omisión"; de acuerdo con el artículo 27 del código disciplinario ley 1952 del 2019; la falta disciplinaria puede ser realizada por acción u omisión en el cumplimiento de los deberes propios del cargo o función, o con ocasión de ellos, o por extralimitación de sus funciones.

De acuerdo con el artículo 46 de la ley 1952 del 2019 por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario, esta notificación se hará por escrito a través del documento de clasificación provisional de cargos, el cual deberá contener:

- Análisis de los argumentos de los sujetos procesales.
- Análisis de pruebas para cada cargo.
- Cargo desempeñado.

- Confianza depositada en el investigado o de la naturaleza del cargo.
- Criterios de gravedad o levedad de la falta.
- Descripción y determinación de la conducta investigada (Modo, Tiempo y Lugar).
- Forma de culpabilidad.
- Grado de culpabilidad toda vez que constituye el elemento subjetivo de la conducta y por tanto hace parte de su descripción.
- Grado de participación.
- Identificación del Autor o Autores.
- Modalidades y circunstancias en que se cometió la falta.
- Normas presuntamente violadas.
- Trascendencia social de la falta o perjuicio causado.
- Las modalidades y circunstancias en que se cometió la falta se apreciarán teniendo en cuenta el cuidado empleado en su preparación, el nivel de aprovechamiento de la confianza depositada en el investigado o de la que se derive de la naturaleza del cargo o función, el grado de participación en la comisión de la falta, si fue inducido por un superior a cometerla, o si la cometió en estado de ofuscación originado en circunstancias o condiciones de difícil prevención y gravedad extrema, debidamente comprobadas.
- La Secretaria General y la Oficina Asesora Jurídica, efectuará según corresponda la indagación e investigación necesaria, cumpliendo con los lineamientos, procedimientos y trámites contenidos en el Reglamento Interno de Trabajo, para investigar el incumplimiento de actividades y obligaciones relacionadas con la Política de Seguridad de la Información y demás políticas afines teniendo en cuenta las conductas punibles tipificadas en la Ley de Delitos Informáticos No. 1273 de 2009, mediante la cual se adicionó el Título VII Bis denominado "De la Protección de la Información y de los datos", las cuales se traen a colación, con la respectiva política afectada, sanción penal y procedimiento adoptado por la entidad, como se observa en el cuadro que se encuentra a continuación:

Ley	Falta y/o conducta	Descripción	Política afectada	Sanción penal / Procedimiento aplicado por la entidad
Art. 269A. **Ley 1273 del 2009**	Acceso abusivo a un sistema informático.	"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo (…)"	• Política Seguridad y privacidad de la Información. • Política de control de acceso.	"Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes."

Ley	Falta y/o conducta	Descripción	Política afectada	Sanción penal / Procedimiento aplicado por la entidad
Art. 269B. Ley 1273 del 2009	Obstaculización ilegítima de sistema informático o red de telecomunicación.	"El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones de la Entidad (…)"	• Política Seguridad y privacidad de la Información.	Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Art. 269C. Ley 1273 del 2009	Interceptación de datos informáticos.	"El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte (…)"	• Política Seguridad y Privacidad de la Información.	Incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Art. 269D. Ley 1273 del 2009	Daño Informático.	"El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos (…)"	• Política Seguridad y privacidad de la Información.	Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Art. 269F. Ley 1273 del 2009	Violación de datos personales.	"El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte,	• Política Seguridad y privacidad de la Información. • Política de Protección de Datos Personales	Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Ley	Falta y/o conducta	Descripción	Política afectada	Sanción penal / Procedimiento aplicado por la entidad
		divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes (…)"		
Art. 269G. Ley 1273 del 2009	Suplantación de sitios web para capturar datos personales.	"El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes (…)"	• Política Seguridad y privacidad de la Información. • Política de Protección de Datos Personales	Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Art. 269I. Ley 1273 del 2009	Hurto por medios informáticos y semejantes	"El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos (…)"	• Política Seguridad y privacidad de la Información. • Política gestión de Activos.	Incurrirá en las penas señaladas en el artículo 240 de este Código y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
		"El que, con ánimo de lucro y valiéndose de alguna manipulación informática o	• Política General de Seguridad de la Información.	Incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses.

Ley	Falta y/o conducta	Descripción	Política afectada	Sanción penal / Procedimiento aplicado por la entidad
Art.269J. Ley 1273 del 2009	Transferencia no consentida de activos	artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave (…)"	• Política gestión de Activos.	Multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

4. RECOMENDACIONES

El alcance de cada sanción se establecerá teniendo en cuenta el grado de intencionalidad, descuido o negligencia que se revele en la conducta, el daño al interés público, la reiteración o reincidencia, así como el grado de participación. Los responsables para evaluar la gravedad o levedad de la falta disciplinaria y con ello determinar las sanciones, serán los definidos al interior de la entidad en cabeza de la Secretaría General, la Oficina Asesora Jurídica, y el Grupo de Control Interno Disciplinario, con el apoyo del Oficial de Seguridad de la Información, o quien haga sus veces. Las faltas cometidas podrán imponerse las siguientes sanciones a los servidores públicos:

SANCIONES ADMINISTRATIVAS Y DISCIPLINARIAS
1. Destitución e inhabilidad general de diez (10) a veinte (20) años para las faltas gravísimas dolosas.
2. Destitución e inhabilidad general de cinco (5) a diez (10) años para las faltas gravísimas realizadas con culpa gravísima.
3. Suspensión en el ejercicio del cargo de tres (3) a cuarenta y ocho (48) meses e inhabilidad especial por el mismo término para las faltas gravísimas realizadas con culpa grave.
4. Suspensión en el ejercicio del cargo de tres (3) a veinticuatro (24) meses e inhabilidad especial por el mismo término para las faltas graves dolosas.
5. Suspensión en el ejercicio del cargo de uno (1) a dieciocho (18) meses para las faltas graves culposas.
6. Multa de veinte (20) a noventa (90) días de salario básico devengado para la época de los hechos para las faltas leves dolosas.
7. Multa de cinco (5) a veinte (20) días de salario básico devengado para la época de los hechos para las faltas leves culposas
8. Despido disciplinario del personal laboral, que sólo podrá sancionar la comisión de faltas muy graves y comportará la inhabilitación para ser titular de un nuevo contrato de trabajo con funciones similares a las que desempeñaban.
9. Suspensión firme de funciones, o de empleo y sueldo en el caso del personal laboral, con una duración máxima de 6 años.

10. Traslado forzoso, con o sin cambio de localidad de residencia, por el período que en cada caso se establezca.
11. Demérito, que consistirá en la penalización a efectos de carrera, promoción o movilidad voluntaria.
12. Apercibimiento.
13. Cualquier otra que se establezca por Ley.
14. Multa de 10 a 100 salarios mínimos mensuales legales vigentes al momento de la comisión del hecho y, concurrentemente, inhabilidad para ejercer empleo público, función pública, prestar servicios a cargo del Estado, o contratar con este de uno a veinte años. Cuando la conducta disciplinable implique detrimento del patrimonio público, la sanción patrimonial será igual al doble del detrimento patrimonial sufrido por el Estado.
15. Cuando la prestación del servicio sea permanente y la vinculación provenga de nombramiento oficial, será de destitución e inhabilidad de 1a 20 años.

4.1 DOCUMENTO DE REFERENCIA Y/O LEYES APLICABLES

- Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común.
- Código Penal 599 del 2000.
- Ley 1273 de 2009 Delitos informáticos.
- Guía Técnica Colombiana GTC-ISO/IEC 27002:2018 Código de práctica para controles de seguridad de la información.
- Ley 1952 del 2019, Código General Disciplinario.
- Norma Técnica Colombiana ISO/IEC 27001:2022 Sistemas de Gestión de Seguridad de la Información.
- Manual operativo Modelo Integrado de planeación y gestión MIPG
- Política Seguridad y privacidad de la Información.

5. ANEXOS

- Procedimiento Gestion de Incidentes de Seguridad
- Formato de Eventos o Incidentes de Seguridad
- Formato de Entrega de Evidencia Física

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	25/10/2024	Creación del documento