UNP

GUIA

CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS ESPECIALES

GTE-GU-06-V1

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
08-10-2024

Tabla Contenido

1. OBJETIVO 3

2. ALCANCE 3

3. DEFINICIONES 3

4. RESPONSABILIDADES 5

5. MARCO LEGAL 5

6. CONDICIONES GENERALES 6

7. CONTACTO CON AUTORIDADES 7

8. GRUPOS DE INTERÉS ESPECIAL 8

9. VIGENCIA 9

10. DOCUMENTOS RELACIONADOS 10

11. CONTROL DE CAMBIOS 10

12. BIBLIOGRAFÍA 10

1. OBJETIVO

Brindar una guía apropiada para los servidores públicos, contratistas, colaboradores y todas las partes interesadas de la Unidad Nacional de Protección de acuerdo con los lineamientos de las autoridades y grupos especiales de seguridad de la información apropiados para la gestión de reportar un incidente de seguridad que requiere escalamiento según su clasificación.

2. ALCANCE

La presente guía inicia con la definición, clasificación de los entes vigentes y sus contactos y continua con su apropiación en el reporte de incidentes de seguridad en cumplimiento Anexo A control A 6.1.3 de la norma de la ISO/IEC 27001 y demás partes que estén interesadas con la actualización de normativas, directrices que las autoridades pertinentes divulguen para el conocimiento de la comunidad.

3. DEFINICIONES

NOMBRE	DEFINICIÓN
Activos de información	Los activos de información son datos o información propietaria en medios electrónicos, impresos u otros medios, entre los cuales se encuentran los públicos, y los considerados sensitivos o críticos para los objetivos de la Entidad. (Norma ISO 27000)
Amenaza	Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)
Ciberespacio:	Ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009.
Ciberseguridad:	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
Clasificación de la Información:	Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)
Confidencialidad:	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Norma ISO 27000).
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Norma ISO 27000).

NOMBRE	DEFINICIÓN
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Norma ISO 27000)
Los Grupos de Interés Internos:	Son aquellos grupos imprescindibles para la operación de la Entidad, es decir, todos aquellos que tienen una relación laboral o contractual con la UNPo, como lo son los servidores públicos, contratistas.
Los Grupos de Interés Externos:	Son aquellos grupos que no participan directamente en las actividades de operación de la Entidad, pero que son destinatarios de los servicios que en la UNP ofrece en el marco del desarrollo de su cadena de valor, también hacen parte de este grupo aquellos que no participan directamente en el intercambio de información con de la UNP
Incidente	**de seguridad de la información:** Un incidente de seguridad de la Información está indicado por un único evento o una serie de eventos de Seguridad de la Información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar la seguridad de la información". (Norma ISO 27000)
Información	Conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Ley 1712 de 2014)
Información Pública Clasificada (Ley 1712 de 2014, art 6).	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
Información Pública Reservada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
Integridad	Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. (Norma exactitud y completitud. (Norma ISO 27000).
Probabilidad	Hace referencia a la oportunidad de que algo suceda, esté o no definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito utilizando términos o matemáticos. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAF)
Riesgo de seguridad de la información	Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)
Seguridad de la información	**P**reservación de la confidencialidad, integridad, y disponibilidad de la información. (Norma ISO 27000). y de mejora continua. (Norma ISO 27000).
Sistema de Gestión de Seguridad de la Información SGSI	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión
Vulnerabilidad: Debilidad	de un activo o control que puede ser explotada por una o más amenazas. (Norma ISO 27000).

4. RESPONSABILIDADES

Responsables	Responsabilidades
CIO y/o Coordinador de Gestión de las Tecnologías de la Información.	Realizar la aprobación de solicitud por parte de los servidores públicos y/o contratistas para la autorización y aprobación de la creación de la cuenta de usuario.
Responsable de la Mesa de Servicios -	Por medio de la plataforma de mesa de servicios las solicitudes de creación de cuentas de usuarios con sus respectivos servicios. - Velar por el cumplimiento de los lineamientos y políticas definidas para el uso de las cuentas asignadas - Aplicar las medidas de protección en la utilización de las cuentas disponibles. - Administración de la plataforma donde se reportan los eventos o incidentes de seguridad.
Responsable del MSIP	Es el responsable del análisis de la justificación de las solicitudes tal como se deja en la descripción de las actividades Subdirección de Talento Humano
Analista Funcional	Verifica los datos y la información, la pertinencia y consistencia de consultas, reportes y requerimientos
Responsable SGSI	Identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo y cumplimiento de los controles.
Servidores Públicos, contratistas	Responsables de reportar cualquier evento o incidente que se presente

5. MARCO LEGAL

A continuación, se relaciona la normativa que aplica a la Guía de contacto autoridades y grupos de interés especial.

ITEM	NÚMERO	DESCRIPCIÓN - EPÍGRAFE
1	Constitución Política 1993	Artículos 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.
2	Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
3	Ley 1474 de 2011	Por la cual se dictan Políticas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

ITEM	NÚMERO	DESCRIPCIÓN - EPÍGRAFE
4	Decreto Ley 4065 de 2011	Por el cual se crea la Unidad Nacional de Protección (UNP), se establecen su objetivo y estructura.
5	Ley 1755 de 2015	Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
6	Ley 1581 de 2012	por la cual se dictan disposiciones generales para la protección de datos personales.
7	Ley 1712 de 2014	"Ley de transparencia y del derecho de acceso a la información pública nacional"
8	CONPES 3649 DE 2010	Establece la Política Nacional de Servicio al Ciudadano. Contribuir a la generación de confianza y al mejoramiento de los niveles de satisfacción de la ciudadanía respecto de los servicios prestados por la Administración Pública del orden nacional.
9	CONPES 3785 DE 2013	Mejorar la efectividad, la colaboración y la eficiencia de las entidades de la Rama Ejecutiva del orden nacional y sus capacidades para atender oportunamente y con calidad los requerimientos de los ciudadanos. Para ello, se adoptará el modelo de Gestión Pública Eficiente al Servicio del Ciudadano que integre los procesos internos con sus capacidades para atender a los ciudadanos
10	Decreto 1078 de 2015 (DUR-TIC),	Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
11	Norma NTC-ISO/IEC 27001	Seguridad de la Información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información —

Fuente: Elaboración propia

6. CONDICIONES GENERALES

Esta guía ofrece lineamiento que pueda poner en peligro en la presencia de un incidente de seguridad de la información que pueda poner en peligro la confidencialidad, integridad y disponibilidad de la información y debe ser reportado de manera inmediata ante las autoridades vigentes y brindar los escalamientos y subsanación de los eventos que se presenten en la Unidad Nacional de protección y de esta manera evaluar las acciones pertinentes a tomar por parte del personal encargado.

7. CONTACTO CON AUTORIDADES

Las siguientes autoridades listadas corresponden a las entidades competentes en caso de que se presentara un incidente de cualquier índole que pusiera en riesgo la confidencialidad, integridad y disponibilidad de la información, en caso de requerirse el llamado a las autoridades mencionadas, sólo podrán hacerlo el personal encargado.

CONTACTO	DESCRIPCIÓN	CORREO ELECTRONICO	NÚMERO DE TELÉFONO
Colcert	Grupo de Respuestas a Emergencias Cibernéticas de Colombia.	**www. Colcert.gov.co**	**+57 601 344 34 60 - Línea Gratuita: 01-800-0910742 opción 2**
Csirt – Gobierno	Equipo de Respuesta a Incidentes Informáticos – CSIRT. organismos de regulación	csirtgob@mintic.gov.co	**Nacional:** 01 8000 952525 **- Bogotá: +57 601 390 7950 ... Horario de Atención Canales Virtuales: lunes a viernes de 8:30 am - 4:30 pm ...**
Csirt-ccit Policía nacional	Centro de Coordinación Seguridad Informática Colombia. - Atención a incidentes de seguridad informática colombiano	https://cc-csirt.policia.gov.co	**Atención Administrativa lunes a viernes de 7:00 am - 6:00 pm.** Teléfonos **(571) 5159090/ 5159586.**
Policía Nacional	Centro Cibernético Policial – CAI Virtual CCC. - Violación de Datos personales - Uso de Software malicioso - Suplantación de Sitios Web - Transferencia no consentida de activos - Hurto por medios informáticos - Phishing - Ingeniería Socia	https**://www.ccp.gov.co**	**60 (1) 5702000 (#7) en Bogotá, 018000919748 o línea celular 122 para el resto del país. Atención las 24 horas del día, los 7 días de la semana, los 365 días del año.**
Fiscalía	- Encargada de hacer cumplir la ley Acceso abusivo a sistemas informáticos. - Violación de Datos personales - Uso de Software malicioso - Suplantación de Sitios Web - Transferencia no consentida de activos - Hurto por medios informáticos - Phishing - Ingeniería Socia		
Superintendencia de Industria de Comercia (SIC)	- autoridades de supervisión	www.sic.gov.co	**Líneas de atención Teléfono Conmutador: +60 (1) 587 00 00 - Bogotá -**

CONTACTO	DESCRIPCIÓN	CORREO ELECTRONICO	NÚMERO DE TELÉFONO
			Línea Gratuita Nacional: 01 8000 910165
Unidad Nacional de Protección	- Emergencias, enfoque claro en la protección humana,	www.unp.gov.co	**103**
Bomberos	- Emergencia por incendios	www.bomberosbogota.gov.co	**119**
Policía Nacional	- Robo	www.policia.gov.co	**112**
Gaula	- Antisecuestro y Antiextorsión	www.ejercito.mil.co/grupogaula	**165**
Defensa civil	- Siniestros ambientales	www.defensacivil.gov.co	**144**
Cruz roja	- Incidentes laborales	www.cruzrojacolombiana.org	**132**
Centro toxicológico	- Incidentes laborales	www.minsalud.gov.co	**Número gratuito: 018000-916012 - Número fijo: +57(1) 2886012 - Atención 24 horas**
Dijin	- Robo	www.revisionautomotores.policia.gov.co correo electrónico mebuc.sijin@policia.gov.co	**Teléfono 3143644139**
Empresa de servicios públicos	- Codensa	www.enel.com.co	**Call center: 60 1 6 364 379**
	- Acueducto	www.acueducto.com.co	**Teléfono 601+3447000**
	- ETB	www.etb.com	**Teléfono 3777777**
- **ARL Positiva**	- Accidente laboral	www.positivaenlinea.gov.co	**Líneas de Atención. Nacional:** 01-8000-111-170**. Bogotá: +57 (601) 330-7000 ;**

8. GRUPOS DE INTERÉS ESPECIAL

El coordinador del grupo de las tecnologías y/o el responsable de proceso o quien haga sus veces, será el encargado de coordinar los conocimientos disponibles en la entidad, a fin de brindar ayuda en la toma de decisiones en materia de seguridad, éste podrá obtener asesoramiento de otros Organismos.

Se debe mantener contacto permanente con los grupos de investigación, entidades del gobierno, proveedores de tecnología que trabajan en pro de mantener actualizado a las personas que se desarrollan dentro del ámbito de la tecnología, para de esta manera mantenerse al tanto en amenazas, incidentes y posibles soluciones.

NOMBRE	PAGINA	TELEFONO
Presidencia de la República de Colombia	https://www.presidencia.gov.co	Horario de Atención: Lunes a viernes, 8:00 a.m. a 5:00 p.m. Línea Gratuita: (+57) 01 8000 913 666
Ministerio del Interior (MinInterior)	https://www.mininterior.gov.co/	**Horario** de Atención: lunes a viernes de 8:00 a.m. a 4:00 p.m. **Contacto**. **Teléfono**: +57 601 242 74 00. Extensiones: 4130 .
Ministerio de Relaciones Exteriores (MRE),	https://www.cancilleria.gov.co/ Correo institucional: contactenos@cancilleria.gov.co	Conmutador: (+57-601) 3814000 - Fax. (+57-601) 3814747 Información de trámites y servicios: (+57-601) 3826999
Ministerio de Hacienda y Crédito Público (Minhacienda)	https://www.minhacienda.gov.co/webcenter/portal/Minhacienda	Línea Nacional: 01 8000 910071 Teléfono en Bogotá: Conmutador: (57) 601 381 1700
Ministerio de Defensa Nacional (Mindefensa)	https://www.mindefensa.gov.co/	PBX (57-601) 315 0111 Horario de atención de 8:00 a 17:00 horas de lunes a viernes
Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)	https://www.mintic.gov.co/portal/inicio/ Correo Institucional: minticresponde@mintic.gov.co	Teléfono Conmutador: +57 601 344 34 60 - Línea Gratuita: 01-800-0914014 Línea Anticorrupción: 01-800-0912667
DELL	https://www.dell.com/es-co/lp	De lunes a viernes 8:00 AM-6:00 PM 01-800-915-4755
Palo alto	https://www.paloaltonetworks.lat/	Contacte con nosotros Colombia: 01 800 011 0015.
Microsoft	https://www.microsoft.com/es-co	Teléfono: (054) 312 9020.
Fortine	https://www.fortnite.com/	

9. VIGENCIA

Las guías descritas en este documento regirán a partir de la fecha de aprobación y publicación de estas.

10. DOCUMENTOS RELACIONADOS

- GTE-PL-02 Plan Estratégico de seguridad y privacidad de la información
- GTE-MA-02 Manual de políticas especificas de seguridad y privacidad de la información
- GTE-FT-46 – Formato de declaración de aplicabilidad - SOA

11. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del documento para brindar una guía apropiada para los servidores públicos, contratistas, colaboradores y todas las partes interesadas de la Unidad Nacional de Protección de acuerdo con los lineamientos de las autoridades y grupos especiales de seguridad de la información apropiados para la gestión de reportar un incidente de seguridad que requiere escalamiento según su clasificación.	08/10/2024	01

12. BIBLIOGRAFÍA

- ICONTEC. Norma Técnica Colombiana NTC-ISO 27001. Colombia. 2013. Segunda edición.
- ICONTEC, NTC-ISO-IEC 27001, 2022 Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC.
- ISO. Términos y Definiciones. En: Gestión de la seguridad de la información (Fundamentos y vocabulario). 2006. (POLÍTICA ISO/IEC 27000).