	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 1 de 9
		Fecha de aprobación 02/06/2022

PORTADA


A) HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN DE LA MODIFICACIÓN
1	20/12/2019	Lanzamiento del plan
2	25/06/2021	Actualización para integrar temática de continuidad de negocio en el título y contenido del documento
3	02/06/2022	<ul style="list-style-type: none"> • Actualizar las temáticas para sensibilización y capacitación • Se redefinen introducción, objetivo, alcance, términos y definiciones • Se redefine tanto en el contenido como en el título el numeral 6.2 Identificación de necesidades • Se elimina el numeral 6.4 Temáticas de comunicación, sensibilización y capacitación, porque el contexto ya se integra en el numeral 6.2 • Se redefinen los numerales 6.3 Recursos disponibles, 6.4 Evidencias de las sesiones y 6.5 Medición del aprovechamiento • En relación a la Unidad de Riesgo Operativo se incluyen apartes respecto a los posibles escenarios de pérdida de continuidad.

B) REVISIONES Y APROBACIONES DEL DOCUMENTO


ELABORÓ	REVISÓ	APROBÓ
Nombre: Jesús Goyes Alvarado	Nombre: Germán Correa Amado	Nombre: Francisco Álvaro Ramírez Rivera
Cargo: Contratista Asesor Tecnología, Seguridad y Ciberseguridad	Cargo: Jefe Oficina Asesora de Planeación y Sistemas	Cargo: Director General
Fecha: 24/05/2022	Fecha: 01/05/2022	Fecha: 02/06/2022

REVISÓ	REVISÓ
Nombre: Oscar Herrera Isaza	Nombre: Andrea del Pilar León
Cargo: Contratista Asesor Sistemas de Gestión	Cargo: Coordinador unidad de riesgo operativo URO
Fecha: 31/05/2022	Fecha: 31/05/2022

	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 2 de 9
		Fecha de aprobación 02/06/2022

C) LISTA DE DISTRIBUCIÓN

N°	NOMBRE Y CARGO
1	Director General.
2	Jefe Oficina Asesora de Planeación y Sistemas.
3	Jefe Oficina Asesora Jurídica.
4	Subdirectora de Prestaciones Económicas.
5	Subdirector Administrativo y Financiero
6	Coordinador Grupo Interno de Trabajo de Bienes y Servicios
7	Coordinador Grupo Interno de Trabajo de Contabilidad.
8	Coordinador Grupo Interno de Trabajo de Tesorería.
9	Coordinador Grupo Interno de Trabajo Gestión Talento Humano.
10	Asesor Control Interno.
11	Coordinadora Grupo de Afiliación, Aportes e Historia Laboral.
12	Coordinadora Grupo de Gestión de Cartera
13	Profesional Especializado Unidad de Riesgo Operativo
14	Asesor Tecnologías de la Información
15	Asesor Sistemas de Gestión

	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 3 de 9
		Fecha de aprobación 02/06/2022

**PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN
DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE
NEGOCIO**

Versión 3

ORIGINAL FIRMADO



	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 4 de 9
		Fecha de aprobación 02/06/2022

TABLA DE CONTENIDO

1. INTRODUCCION	5
2. OBJETIVO	5
3. ALCANCE	5
4. TÉRMINOS Y DEFINICIONES.....	6
5. MARCO DE REFERENCIA.....	7
6. Plan para comunicación, sensibilización y capacitación de seguridad de la información y continuidad de negocio.....	7
6.1 MODELO DEL PLAN	7
6.2 IDENTIFICACIÓN DE TEMÁTICAS PARA CAPACITACIÓN Y SENSIBILIZACIÓN.....	8
6.3 RECURSOS DISPONIBLES	8
6.4 EVIDENCIAS DE LAS SESIONES.....	9
6.5 MEDICIÓN DEL APROVECHAMIENTO.....	9
6.6 periodicidad.....	9

ORIGINAL FIRMADO

	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 5 de 9
		Fecha de aprobación 02/06/2022

1. INTRODUCCION

Dentro de la estrategia de Fonprecon para fortalecer la seguridad de la información, existe un conjunto de planes, políticas y procedimientos que enmarcan aspectos relacionados con la seguridad de la información, la ciberseguridad y la continuidad de negocio, basado en referentes como el modelo de seguridad y privacidad de la información del MINTIC.

Dentro de ello, uno de los aspectos más relevantes, tiene que ver con la sensibilización y capacitación en seguridad y continuidad de negocio a *servidores*, contratistas y proveedores, en cuanto a sus roles y responsabilidad frente a la prevención de incidentes. Para ello es indispensable impartir temáticas de sensibilización y capacitación que les amplie sus capacidades de cómo actuar frente a las diversas amenazas del cibercrimen.

2. OBJETIVO

Adoptar temáticas para desarrollarse periódicamente y que permitan a los funcionarios y contratistas fortalecer sus conocimientos y actuar en mejor forma frente a las amenazas del cibercrimen frente a la seguridad, ciberseguridad y continuidad de negocio.


Proponer estrategias de recuperación que contengan medidas para prevenir y detectar amenazas de tal forma que minimice su probabilidad y sus efectos.

Preparar la implementación, capacitación y comunicación a los involucrados para su puesta en marcha.

3. ALCANCE

Este plan establece las temáticas, grupos a quién va dirigido, periodicidad para realizar actividades dentro de sus funcionarios, contratistas y proveedores, mediante la construcción de material multimedia en el que se explica una determinada temática.

Al incorporar en los mapas de riesgo de gestión el riesgo de “perdida de continuidad de negocio “ bajo 5 escenarios se dinamiza la cultura de riesgo involucrando activamente a la entidad en cada uno de sus roles.

	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 6 de 9
		Fecha de aprobación 02/06/2022

4. TÉRMINOS Y DEFINICIONES

Sensibilización: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

EJEMPLO: Uso correcto de contraseñas, consecuencias reales sobre prestar una contraseña y qué hacer si no recuerdo mi contraseña. El éxito de la sensibilización es la practicidad y la simplicidad en que esta información es entregada, para captar la atención del aprendiz.

Fuente: Guía 14 MSPI MINTIC

Entrenamiento: Busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas a su cargo. Un programa de entrenamiento no busca certificar (aunque puede llegar a hacerlo), pero puede tener mucha temática relacionada con un curso de certificación. **EJEMPLO:** Un curso de seguridad de la información, enfocado a administración de riesgos, ciclo de vida del servicio de seguridad y controles operacionales. Un curso sobre administración de plataformas de verificación de registros (Log).


Fuente: Guía 14 MSPI MINTIC

Educación formal: Se define como todos los niveles y habilidades de seguridad envueltos en un único cuerpo de conocimiento. **EJEMPLO:** Programa de estudios de educación superior, postgrados, etc. **Fuente: MINTIC - GUÍA 14:** Plan para comunicación, sensibilización y capacitación de seguridad de la información

Desarrollo profesional: busca asegurar que los usuarios desde el más principiante hasta el más experimentado, tengan los conocimientos suficientes para desempeñar sus roles. Esto se logra a través de certificaciones, que ofrecen proveedores de plataformas específicas, sistemas operativos etc.... o algunas otras relacionadas con conceptos de seguridad informática (gestión, planeación etc....). Esta parte de desarrollo profesional, depende de cada institución si requiere de certificaciones para desempeñar bien sus roles o si son motivo para brindar algún tipo de bonificación adicional al empleado por su preparación. **Fuente: MINTIC - GUÍA 14:** Plan para comunicación, sensibilización y capacitación de seguridad de la información

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona autorizada o entidad competente.

	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 7 de 9
		Fecha de aprobación 02/06/2022

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Plan de Continuidad de Negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000)

5. MARCO DE REFERENCIA

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1008 de 2018: 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.

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

ISO/IEC 27001:2013: Estándar internacional que define dentro de un marco de referencia, cómo organizar la seguridad de la información.


GTC-ISO 22313: 2016: Sistemas de Gestión de Continuidad de Negocio

GTC-ISO 27032: Técnicas de seguridad. Directrices para ciberseguridad

6. PLAN PARA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO

6.1 MODELO DEL PLAN

Acorde con el tamaño de la Entidad y que su operación se concentra en una sola sede, se adopta el modelo centralizado, por lo que las políticas, la estrategia y la implementación, son fijadas en esta única sede y distribuidas y aplicadas en sus procesos.

	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 8 de 9
		Fecha de aprobación 02/06/2022

6.2 IDENTIFICACIÓN DE TEMÁTICAS PARA CAPACITACIÓN Y SENSIBILIZACIÓN

AUDIENCIA	TEMÁTICA DE INTERÉS
DIRECTIVOS	<ul style="list-style-type: none"> • Contexto de la Seguridad y ciberseguridad en Fonprecon • Uso de contraseñas, vigencia y complejidad • La importancia de las actualizaciones de software, clases de actualizaciones • Antivirus • Malware, Virus, Troyanos, Spywares, Ransomware, Adwares, Botnets • Qué hacer y a quien informar frente a un incidente de seguridad o ciberseguridad en cualquier ámbito (oficina, hogar, otros) • Análisis de contenido malicioso en documentos adjuntos • Qué es y para qué sirve una conexión VPN • Tratamiento de correos sospechosos • Ingeniería social • Phishing • Qué es la continuidad de negocio • Seguridad en el puesto de trabajo - bloquear el computador, información impresa – papel reciclado • ciberamenazas: ciberdelito, ciberdelincuente, ciberterrorismo, hacktivismo, ciberextorción • Uso del correo • Copias de seguridad • Recuperación de desastres tecnológicos • Controles automatizados de ciberseguridad • Legislación, directrices y estándares en seguridad
PERSONAL DE TI	
FUNCIONARIOS CONTRATISTAS	

La sensibilización basada en los escenarios de pérdida de continuidad busca a todos los niveles de la entidad:

ENTENDER LA ENTIDAD

Activo: ¿Qué trata de proteger?

Amenaza ¿Qué se teme que suceda?

¿Cuál es el impacto para la entidad?


ANÁLISIS DE RIESGO

Vulnerabilidad ¿Cómo puede ocurrir la amenaza?

Mitigación ¿Cómo se reduce actualmente el riesgo?

¿Que tan probable es que la amenaza frente a los controles?

RIESGO ES LA MATERIALIZACIÓN DE UNA AMENAZA APROVECHANDO LA VULNERABILIDAD DE UN ACTIVO

	PLAN	CODIGO: PLN-GTC-006
	PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO	VERSIÓN 3
		Página 9 de 9
		Fecha de aprobación 02/06/2022

La Oficina Asesora de Planeación y Sistemas, en función de su equipo de trabajo y los recursos tecnológicos disponibles, creará material audiovisual con duración de pocos minutos abordando una sola temática. Adicionalmente se integrará un formulario en línea para control de asistencia y medición de aprovechamiento.

6.4 EVIDENCIAS DE LAS SESIONES

En la socialización de cada temática se integra:

- Formulario en línea para control de asistencia
- Enlace de acceso al material multimedia de la temática
- Formulario en línea para medición del aprovechamiento mediante preguntas relacionadas a la temática

6.5 MEDICIÓN DEL APROVECHAMIENTO

En la socialización de cada temática se integra:

- Formulario en línea para medición del aprovechamiento mediante preguntas relacionadas a la temática

6.6 PERIODICIDAD

Las sesiones de comunicación, sensibilización y capacitación deben desarrollarse al menos una vez al año.