PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN

SERVICIUDAD E.S.P
DOSQUEBRADAS

Elaboró	Revisó	Aprobó
Harrison González Santa Técnico grado 3 sistemas	**Wilson Arias Castaño** Profesional especializado	**Mauricio Andrés Rodas T.** Subgerente Planeación (e)
Fecha: 26/11/2021	Fecha: 29/11/2021	Fecha: 29/11/2021

INTRODUCCIÓN

En la actualidad las tecnologías de información y comunicaciones se han convertido en una importante herramienta para optimizar procesos y brindar opciones de eficiencia y eficacia en la prestación de sus servicios. El tratamiento de seguridad y privacidad de la información no se basa únicamente en el blindaje de plataformas y procesos, sino que involucra el factor humano como punto clave del manejo de incidencias y requerimientos en servicios tecnológicos. Por lo anterior, SERVICIUDAD E.S.P presenta este documento como guía para la comunicación, socialización y sensibilización en materia de seguridad y privacidad de la información al interior de la misma.

1. OBJETO

Definir el Plan de capacitación, sensibilización y comunicación de SERVICIUDAD E.S.P con el fin de brindar una herramienta con las directrices en las que se establecen acciones para consolidar la seguridad y privacidad de la información al interior de la Entidad.

2. ALCANCE

Brindar las directrices de comunicación en términos de seguridad y privacidad de la información de manera transversal a todos los macroprocesos alineados a los servicios prestados por la Entidad.

3. DEFINICIONES

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

Entrenamiento: Proceso utilizado para capacitar y fortalecer habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

Comunicación Horizontal: Es el proceso de interacción determinado por el mismo nivel jerárquico que existen en una Entidad.

Comunicación vertical: Es el proceso de interacción determinado por los niveles jerárquicos que existen en una Entidad, de forma descendente o ascendente.

Capacitación: Es un proceso que tiene como objetivo incrementar las aptitudes y habilidades del individuo, mediante la enseñanza, para que éste pueda aumentar su desempeño y competencias al momento de realizar sus labores asignadas dentro de la Entidad.

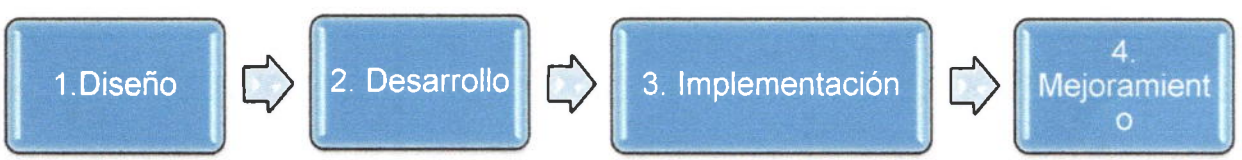
4. RESPONSABLE

El responsable del Plan de sensibilización, Capacitación y Comunicación de Seguridad y Privacidad de la Información, es el Comité de Seguridad de la Información de la Entidad.

5. DESCRIPCIÓN DEL PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN

Este plan pretende sensibilizar, capacitar y comunicar las reglas de comportamiento adecuadas para el uso seguro de los servicios de TI plasmados en el portafolio de servicios, políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean adoptados y adaptados por parte de todos los usuarios del sistema. Teniendo en cuenta lo anterior, este plan de capacitación, sensibilización y comunicación adecuado, debe llevarse a cabo con base a las siguientes fases:

IMAGEN Nª1. FASES PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN SERVICIUDAD E.S.P



Fuente: Elaboración propia

1. **DISEÑO:** En esta fase se Identifican las actividades necesarias para cumplir con el Plan de acuerdo a la matriz de interesados de la Entidad.

TABLA Nª1. MATRIZ DE INTERESADOS DEL PLAN

INTERESADO	EXPECTATIVA/ NECESIDAD
Gerencia/ Comité Directivo	Deben conocer y entender las leyes y directivas que forman la base del Modelo de Seguridad y Privacidad de la Entidad. A su vez, deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás Dependencias.
Comité de Seguridad de la Información	Deben velar por la actualización y cumplimiento de las políticas y gestionar de manera oportuna las incidencias y requerimientos presentados en materia de Seguridad y Privacidad de la Información al interior de la Entidad.
Director Oficina de TI	Debe velar por la gestión de los controles de seguridad en los sistemas de información, con el fin de brindar continuidad y disponibilidad en la prestación de los servicios de TI.
Proveedores de Servicios de TI	Deben proporcionar Acuerdos de Nivel de Servicio que contengan mecanismos de continuidad y disponibilidad en la prestación de los servicios de TI
Usuarios Finales	Colaboradores, contratistas, pasantes universitarios y SENA, personal temporal y otras personas relacionadas a terceras partes, que deben conocer los aspectos relacionados con el Modelo de Seguridad y Privacidad de la Información.

Fuente: Elaboración propia

2. DESARROLLO:

La información resultante y documentada del Plan de Sensibilización, capacitación y comunicación debe conservarse en un repositorio de fácil acceso para su consulta y guía, para tal efecto SERVICIUDAD E.S.P dispone de la siguiente ruta: _ Sistema de gestión de Calidad y Documentación (serviciudad.gov.co) como fuente de almacenamiento y consulta.

3. IMPLEMENTACIÓN:

El material dispuesto como consulta y guía del Plan de Sensibilización, Capacitación y Comunicación de Seguridad de la Información, puede visualizarse en documentación ofimática y audiovisual para su mejor entendimiento y comprensión.

4. MEJORAMIENTO:

La información inherente del plan debe ser validada y actualizada por el Comité de Seguridad de la Información con periodicidad de revisión cuatrimestral y de acuerdo a los requerimientos exigidos por MinTIC. Cabe resaltar que, este Comité tiene dentro de sus funciones realizar monitoreos constantes de la efectividad del plan y de esta forma realizar acciones de mejora con base a los hallazgos identificados.

5. ROLES RESPONSABLES DE LOS TEMAS A COMUNICAR EN EL PLAN

TABLA Nª2. TEMAS A COMUNIAR POR RESPONSABLE

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
Control interno	Seguimiento y Control Sobre los Planes de Auditoria de Seguridad de la Información	Profesional Especializada de Control Interno
	Revisión independiente de la seguridad de la información	
	Velar por el cumplimiento de las políticas y normas de seguridad de la información	
	Auditorías Internas e identificación de hallazgos sobre la seguridad de la Información	
	Documentación de Planes de mejoramiento sobre los hallazgos encontrados en Seguridad de la información	
	Aplicación de las sanciones correspondientes de acuerdo a las faltas en materia de seguridad de la Información	
Gestión Humana	Selección e investigación de antecedentes del Colaborador	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	Términos y condiciones del empleo	Profesional Especializado en Talento Humano
Responsable de compras y adquisiciones	Relación con los Proveedores	Subgerente Financiera y Administrativa /Secretario General
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	
Responsable de la continuidad	Gestión sobre los aspectos de seguridad de la información para la continuidad del negocio	Director Oficina de TI
	Continuidad de la seguridad de la información	
	Planificación de la continuidad de la seguridad de la información	
	Implementación de la continuidad de la seguridad de la información	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Disponibilidad de sistemas de Información para la continuidad de la Información	
Responsable de la seguridad física	Seguridad Física y del Entorno Áreas seguras	Comité de Seguridad de la Información
	Perímetro de seguridad física	
	Controles de Acceso al cuarto de Servidores	
	Seguridad Física y del Entorno	
Responsable de Seguridad de la Información	Políticas de Seguridad de la Información	Comité de Seguridad de la Información
	Organización de la Seguridad de la Información	
	Seguridad del Talento Humano	
	Gestión de los activos de Información	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	Modelo de Seguridad y Privacidad de la Información	
	Política de Acceso a las Tecnologías de la información	
	Cumplimiento de requisitos legales y contractuales	
	Criptografía	
	Proyectos de Seguridad de la Información	
	Metodologías de Seguridad de la información	
	Procedimientos de operación documentados y responsables	
	Protección Contra códigos maliciosos	
	Copias de respaldo	
	Gestión de Vulnerabilidades	
	Registros de eventos	
	Adquisición, desarrollo y mantenimiento de los sistemas de Información	
	Transferencia de Información	
	Controles sobre auditorías de sistemas de información	
	Requisitos de seguridad de los sistemas de información	
	Identificación y valoración de riesgos	
	Tratamiento de riesgos de seguridad de la información	
	Sensibilización y socialización sobre los temas de la seguridad de la información	
	Planificación y control operacional	
	Implementación del plan de tratamiento de riesgos	
	Indicadores de gestión del MSPI	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	Plan de seguimiento, evaluación y análisis del MSPI	
	Evaluación del plan de tratamiento de riesgos	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la Entidad	
	Inventario de Activos de Información.	
	Gestión de riesgos que incluya riesgos de ciberseguridad	
	Respuesta a incidentes de ciberseguridad, planes de recuperación y restauración	
Responsable de TICs	Teletrabajo	Director Oficina de TI
	Manejo de medios	
	Derechos de propiedad intelectual.	
	Control de Acceso	
	Seguridad de la Operaciones	
	Procedimientos Operacionales y de respaldo	
	Copias de Seguridad	
	Políticas de TI	
	Adquisición, desarrollo y mantenimiento de los sistemas de Información	
	Gestión de la Seguridad de las Redes	
	Gestión de Incidentes de Seguridad de la Información	
	Plan y Estrategia de transición de IPv4 a IPv6	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	Implementación del plan de estrategia de transición de IPv4 a IPv6	
	Indicadores de TI	
Calidad	Procedimientos de control documental del MSPI	Profesional Especializada de Calidad

Fuente: Elaboración propia

6. AUDIENCIA OBJETIVO

La audiencia objetivo que debe ser sensibilizada, capacitada y entrenada son los usuarios de lectura, consulta y ejecución de tareas en los servicios de TI.

7. FRECUENCIA DE CAPACITACIÓN Y ENTRENAMIENTO DEL PLAN

La frecuencia de las inducciones, reinducciones y capacitaciones se da de acuerdo a los requerimientos de las subgerencias en materia de ingresos de personal nuevo, traslados y acciones de mejora al interior de la Entidad, validada por la Oficina de Control Interno.

8. DOCUMENTACIÓN RELACIONADA

- Política de Seguridad de la Información
- Política de Gobierno Digital
- Plan de Seguridad y Privacidad de la Información