

PLAN DE COMUNICACIÓN Y SENSIBILIZACIÓN (EGSI)



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



Tabla de contenido

1. ANTECEDENTES	3
2. OBJETIVO DEL PLAN	3
2.1. OBJETIVOS ESPECÍFICOS	4
3. DESCRIPCIÓN GENERAL DEL PLAN DE COMUNICACIÓN Y SENSIBILIZACIÓN	4
3.1. ALCANCE DEL PLAN	4
3.2. DISEÑO DEL PLAN DE COMUNICACIÓN Y SENSIBILIZACIÓN.....	5
3.2.1. Materiales y canales de difusión del Plan de Comunicación y	
Sensibilización	7
3.2.2. Estrategias para el Plan de Comunicación y Sensibilización	10
3.3. IDENTIFICACIÓN DE NECESIDADES.....	14
3.4. ROLES Y RESPONSABILIDADES	16
3.5. RESULTADOS Y LOGROS ESPERADOS.....	19
3.6. CRONOGRAMA DE ACTIVIDADES DE COMUNICACIÓN O SENSIBILIZACIÓN	20
4. GLOSARIO DE TÉRMINOS	21
5. DOCUMENTOS DE REFERENCIA	23
6. FIRMAS DE RESPONSABILIDAD.....	23
CONTROL DE VERSIONES DEL FORMATO REFERENCIAL	25
HISTORIAL DE CAMBIOS DEL FORMATO REFERENCIAL.....	25



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



1. Antecedentes

El Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), en cumplimiento de la normativa legal y técnica vigente en materia de seguridad de la información, se encuentra en proceso de implementación y fortalecimiento del Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de los activos de información que sustentan sus funciones misionales y de apoyo institucional.

Considerando que la información institucional es un activo crítico para la gestión operativa de emergencias, prevención, administración, formación y coordinación interinstitucional, resulta indispensable promover una cultura organizacional orientada a la seguridad de la información, que involucre activamente a todos los funcionarios, directivos y actores relacionados con el tratamiento de dicha información.

En este contexto, el Plan de Comunicación y Sensibilización del EGSÍ se constituye como un instrumento estratégico que permite informar, sensibilizar y comprometer a los servidores del BCBG respecto a la importancia de cumplir las políticas, normas y controles establecidos en el EGSÍ, reconociendo que uno de los principales factores de riesgo en seguridad de la información está asociado al desconocimiento, omisión o uso inadecuado de la información por parte del factor humano.

El presente plan define las acciones, estrategias, materiales y canales de comunicación necesarios para difundir de manera clara y progresiva los principios, responsabilidades y buenas prácticas de seguridad de la información, así como para reforzar el rol de cada funcionario en la protección de los activos de información, tanto en medios digitales como físicos.

Los resultados esperados se alcanzarán mediante la ejecución de actividades de comunicación, capacitación y sensibilización, tales como campañas informativas, socializaciones, talleres y difusión de material educativo, las cuales permitirán fortalecer el compromiso institucional, reducir incidentes de seguridad de la información y asegurar la sostenibilidad del EGSÍ en el tiempo.

2. Objetivo del Plan

Informar, sensibilizar y comprometer a todos los funcionarios del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG) sobre la importancia de la seguridad de la información, involucrándolos activamente en la implementación y mantenimiento del Esquema Gubernamental de Seguridad de la Información (EGSI), promoviendo su conciencia, responsabilidad y cumplimiento de las políticas y medidas de seguridad, con el fin de garantizar la protección de los activos de información institucionales y asegurar la sostenibilidad del sistema en el tiempo.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



2.1. Objetivos Específicos

1. **Difundir las políticas de seguridad de la información a todos los funcionarios del BCBG**, asegurando que comprendan las normativas y procedimientos establecidos en el EGSÍ.
2. **Fomentar una cultura organizacional centrada en la seguridad de la información**, asegurando que todos los empleados adopten prácticas seguras tanto en el manejo de información digital como impresa.
3. **Aumentar la conciencia sobre los riesgos de seguridad de la información**, incluyendo amenazas comunes como el acceso no autorizado, el phishing, y la fuga de información, entre otros.
4. **Fortalecer la capacidad de respuesta ante incidentes de seguridad**, instruyendo a los empleados sobre los procedimientos a seguir en caso de brechas de seguridad o incidentes relacionados con la información.
5. **Garantizar el compromiso continuo con el EGSÍ**, a través de la implementación de actividades de capacitación y socialización periódicas, para asegurar que todos los funcionarios mantengan actualizados sus conocimientos en materia de seguridad de la información.

3. Descripción general del Plan de Comunicación y Sensibilización

El Plan de Comunicación y Sensibilización del Esquema Gubernamental de Seguridad de la Información (EGSI) tiene como objetivo garantizar que todos los funcionarios del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG) comprendan la importancia de la seguridad de la información y se comprometan activamente con la implementación, mantenimiento y mejora del EGSÍ.

Este plan es esencial porque, además de cumplir con las normativas legales y técnicas sobre seguridad de la información, busca crear una cultura organizacional sólida que fomente la protección de los activos de información mediante el compromiso y la participación de cada miembro de la institución. A través de la sensibilización y la capacitación continua, se pretende reducir los riesgos de seguridad derivados del desconocimiento, negligencia o malas prácticas relacionadas con el manejo de la información, tanto en formato digital como impreso.

3.1. Alcance del Plan

El Plan de Comunicación y Sensibilización está dirigido a:

- Todos los servidores del BCBG, incluyendo personal administrativo, operativo y directivo, así como a aquellos involucrados en la gestión,



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



procesamiento, almacenamiento y transferencia de la información institucional.

- Proveedores externos, instituciones públicas, usuarios y contratistas que tienen acceso o gestionan información crítica de la institución.
- Áreas específicas como la Dirección General de Operaciones de Emergencias y Seguridad Física, Dirección General de Prevención de Incendios, Dirección General de Talento Humano, Dirección General Financiera, Dirección General de Asesoría Legal; y, Dirección General de Tecnologías de la Información y Comunicaciones (TIC).

El alcance geográfico abarcará todas las instalaciones del BCBG, la Primera Jefatura y demás dependencias administrativas incluyendo también las estaciones de bomberos, donde se maneje o resguarde información crítica.

3.2. Diseño del Plan de Comunicación y Sensibilización

Situación Actual

En la actualidad, la seguridad de la información en el Benemérito Cuerpo de Bomberos de Guayaquil (BCBG) enfrenta varios desafíos. A pesar de la importancia crítica de la información para el funcionamiento operativo y administrativo de la institución, existe un bajo nivel de conciencia y conocimiento general sobre la seguridad de la información entre muchos de los funcionarios. Este desconocimiento genera riesgos, especialmente en cuanto a la correcta gestión, protección y uso de los datos.

Un gran porcentaje de los empleados no está familiarizado con los conceptos de seguridad de la información, lo que genera confusión entre lo que es seguridad informática y seguridad de la información. La seguridad de la información no solo involucra lo digital, sino también la protección de la información impresa, lo cual a menudo se pasa por alto.

Además, las vulnerabilidades de seguridad frecuentemente provienen desde el interior de la organización, ya sea por desconocimiento, accesos no autorizados, motivación insuficiente o incluso falta de entrenamiento adecuado en las políticas de seguridad establecidas. Esto aumenta significativamente el riesgo de incidentes relacionados con la protección de datos.

Alternativas para la ejecución del Plan

Para abordar estos problemas, el plan de comunicación y sensibilización incluirá diversas alternativas y estrategias de ejecución, que se alinearán con las



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



necesidades específicas de la institución y los perfiles de los funcionarios. Las alternativas incluyen:

1. Materiales impresos y visuales:

- Folletos informativos que expliquen de manera sencilla los conceptos clave de seguridad de la información, el EGSÍ y las políticas internas de seguridad.
- Carteles y letreros en lugares visibles (como salas comunes, oficinas y centros operativos) que refuercen las mejores prácticas de seguridad de la información.
- Fondos de pantalla en los equipos institucionales con mensajes clave relacionados con la protección de la información.

2. Uso de correo institucional:

- Envío de boletines periódicos con consejos prácticos, actualizaciones sobre el EGSÍ y recordatorios de las políticas de seguridad.
- Alertas urgentes a través de correo electrónico para informar sobre posibles amenazas o incidentes de seguridad.

3. Capacitaciones y talleres:

- Capacitación presencial y virtual sobre los aspectos fundamentales de la seguridad de la información, incluyendo la correcta gestión de contraseñas, manejo de información sensible, protocolos de acceso y seguridad física.
- Talleres interactivos y simulacros de incidentes de seguridad (como ciberataques o robo de información), para que los empleados se familiaricen con los protocolos de respuesta.

4. Socialización y reuniones:

- Reuniones periódicas con cada equipo de trabajo para discutir temas relevantes de seguridad de la información y compartir experiencias o dudas.
- Sesiones informativas sobre el EGSÍ, donde se explique a fondo el alcance del esquema y los roles de cada persona dentro del proceso de protección de la información.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



5. Duración del Plan y ejecución

El Plan de Comunicación y Sensibilización será un proceso continuo y progresivo a lo largo del tiempo, con actividades anuales, pero con evaluaciones periódicas de su efectividad. Se organizarán actividades como las capacitaciones, talleres y campañas de sensibilización de manera que se adapten a los cambios y necesidades de la institución. La duración inicial del plan será de 12 meses, con revisiones trimestrales para medir el impacto y hacer ajustes.

- **Fase inicial (0-3 meses):** Lanzamiento del plan con distribución de materiales informativos, primeras sesiones de capacitación, y definición de responsabilidades.
- **Fase de ejecución continua (4-9 meses):** Implementación de capacitaciones regulares, simulacros y campañas visuales. Revisión de las actividades y ajustes según la retroalimentación.
- **Evaluación y ajustes (10-12 meses):** Evaluación del impacto, medición de participación y efectividad, y ajustes para asegurar la sostenibilidad del EGSi a largo plazo.

6. Aspectos relacionados a la implementación del EGSi

Para asegurar el éxito del plan, se debe alinear la comunicación y sensibilización con los procedimientos establecidos por el EGSi, integrando los siguientes puntos:

- Revisión periódica de las políticas y medidas de seguridad, a fin de mantener a los empleados actualizados con las últimas normativas y mejores prácticas.
- Promoción de la responsabilidad compartida: Resaltar que la seguridad de la información no depende solo de los equipos de TI, sino que es responsabilidad de cada miembro de la institución.

3.2.1. *Materiales y canales de difusión del Plan de Comunicación y Sensibilización*

Materiales de apoyo para la ejecución del plan

1. Infraestructura

- **Ambientes de capacitación:** Las actividades de sensibilización y capacitación se llevarán a cabo en salas de capacitación adecuadas proporcionadas por la institución, tales como salas de reuniones y aulas virtuales. Estas instalaciones deben contar con



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



una buena ventilación, tecnología audiovisual y suficiente espacio para las actividades grupales.

- **Plataformas virtuales:** Se utilizarán plataformas de videoconferencia como Zoom, Microsoft Teams o Google Meet para las capacitaciones y talleres virtuales. Estas plataformas permitirán a los empleados acceder a las sesiones de capacitación desde cualquier ubicación.

2. Mobiliario, equipo y otros

- **Mobiliario:** Las actividades presenciales de capacitación y socialización contarán con mesas de trabajo, sillas ergonómicas y tableros de notas o pizarras interactivas.
- **Equipos multimedia:** Para las presentaciones, se utilizarán proyectores, pantallas de TV, altavoces y computadoras portátiles que permitirán compartir videos, diapositivas y otros materiales visuales que faciliten la comprensión de los conceptos.
- **Material de oficina:** Las actividades presenciales contarán con materiales como carpetas con los recursos informativos, marcadores para las pizarras, y papel para las actividades grupales o ejercicios de sensibilización.

3. Documentos

- **Material de estudio:** Los participantes recibirán folletos, manuales y guías detalladas que incluyen las políticas de seguridad del EGSÍ, las normas aplicables, las mejores prácticas de seguridad y los procedimientos para responder a incidentes de seguridad.
 - **Encuestas de evaluación:** Para medir la efectividad de las actividades de capacitación y sensibilización, se distribuirán encuestas de evaluación al final de cada sesión. Estas encuestas permitirán obtener retroalimentación sobre la claridad de los contenidos, la utilidad de los materiales y la satisfacción general de los empleados.
 - **Piezas gráficas:** Se elaborarán piezas gráficas que serán enviadas por correo institucional, resumiendo los temas cubiertos en las capacitaciones, actualizaciones del EGSÍ, y recordatorios sobre las políticas y procedimientos clave.
-



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



4. Canales o medios eficientes para la divulgación de los mensajes

1. Correo institucional

- Se utilizarán los correos electrónicos institucionales como el principal canal para enviar materiales educativos, recordatorios de las políticas de seguridad, alertas urgentes sobre incidentes de seguridad y encuestas de evaluación para cada actividad.
- Además, se enviarán boletines periódicos con consejos prácticos y actualizaciones sobre el EGSÍ, reforzando los mensajes de sensibilización.

2. Intranet y plataformas internas

- En la intranet institucional, se publicarán documentos, videos y materiales interactivos sobre seguridad de la información, accesibles a todos los empleados.
- Se utilizarán plataformas de capacitación en línea (como Moodle o el sistema de gestión de aprendizaje que utilice la institución) para albergar los módulos educativos sobre el EGSÍ y permitir la autoformación.

3. Reuniones y talleres presenciales y virtuales

- Reuniones interactivas: Se organizarán sesiones interactivas presenciales o virtuales donde se pueda socializar sobre el EGSÍ y responder dudas en tiempo real.
- Talleres y simulacros: Durante las capacitaciones presenciales y virtuales, los funcionarios participarán en simulacros prácticos de incidentes de seguridad, como ciberataques, robos de información y otras situaciones de riesgo.

4. Redes sociales internas y herramientas de mensajería

- En caso de que la institución cuente con plataformas internas de mensajería como Slack, Microsoft Teams o grupos de WhatsApp, se utilizarán para enviar alertas rápidas, recordatorios y enlaces a recursos educativos.
- Estos canales serán útiles para mantener un contacto directo y rápido con los empleados y fomentar una comunicación más fluida.

5. Pantallas digitales y carteles en áreas comunes



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- Se instalarán pantallas digitales en lugares clave (como el hall de entrada o áreas de descanso) que mostrarán mensajes clave sobre seguridad de la información, recordatorios sobre el manejo adecuado de contraseñas, cómo identificar correos fraudulentos, etc.
- Además, se utilizarán carteles y letreros en áreas visibles como salas de reuniones, oficinas y áreas comunes, recordando las mejores prácticas de seguridad y las políticas de acceso y protección de la información.

6. Eventos especiales y ferias informativas

- Se organizarán eventos de sensibilización como ferias informativas o jornadas temáticas sobre seguridad de la información, donde los funcionarios podrán participar en actividades lúdicas, obtener materiales educativos y recibir charlas especializadas.

Aprobación de materiales y canales

Todos los materiales educativos (folletos, videos, carteles) y los canales de comunicación (correo institucional, intranet, redes sociales internas) deberán ser aprobados por el Comité de Seguridad de la Información (CSI) antes de su distribución o implementación. Este proceso de aprobación garantiza que los mensajes sean claros, consistentes y alineados con las políticas del EGSÍ.

3.2.2. Estrategias para el Plan de Comunicación y Sensibilización

Objetivos específicos de los instrumentos de sensibilización

1. **Aumentar la conciencia sobre la seguridad de la información:** Informar a todos los empleados sobre los riesgos de seguridad cibernética y la importancia de proteger los activos de información de la institución.
2. **Promover la adopción de buenas prácticas:** Incentivar el uso adecuado de contraseñas, la protección de dispositivos, la gestión de datos personales y el correcto manejo de información confidencial tanto digital como impresa.
3. **Fomentar el compromiso con el EGSÍ:** Lograr que todos los funcionarios se sientan responsables de la protección de la información, adoptando un comportamiento activo en la implementación de las políticas y procedimientos del EGSÍ.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



4. **Reducir incidentes de seguridad:** Minimizar los riesgos e incidentes de seguridad mediante la formación y sensibilización continua sobre las amenazas cibernéticas y las medidas de protección.

Diseño de la campaña

Para que la campaña de sensibilización sea efectiva, debe ser impactante, memorables y relevante. Por eso, proponemos una estrategia visual y de comunicación que se construya alrededor de un nombre y una imagen atractiva que capte la atención de todos los funcionarios.

Nombre de la campaña:

- “Seguridad en Cada Acción”
 - Este nombre transmite el concepto de que la seguridad de la información no es solo responsabilidad de un área específica, sino una acción diaria de todos dentro de la institución.

Slogan de la campaña:

- “Tu información bajo control”
 - Un mensaje claro y directo que motiva a los empleados a tomar conciencia de la importancia de proteger la información que manejan.

Imagen de la campaña:

- **Logotipo:** Un símbolo que combine elementos relacionados con la seguridad (candados, redes, protección) con íconos institucionales (como el logo del BCBG o un elemento representativo del trabajo de bomberos) para hacerlo más cercano y significativo.
- **Colores:** Utilizar colores como azul (confianza y seguridad), verde (protección) y amarillo (alerta y precaución), que son visualmente atractivos y transmiten los valores de seguridad.

Elementos visuales:

- Gráficos dinámicos como infografías y carteles que ilustran ejemplos de cómo proteger los datos.
- Videos cortos de 30 segundos a 1 minuto para explicar en términos sencillos el proceso de proteger información en un entorno de trabajo diario.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- Material de apoyo visual: Fondos de pantalla, carteles de advertencia y letreros con mensajes sencillos y directos para mantener la campaña visible en todo momento.

Estrategias de comunicación

1. Comunicación continua y consistente:

- La campaña debe ser constante, con mensajes periódicos sobre la seguridad de la información a través de todos los canales disponibles (correo institucional, intranet, reuniones, pantallas digitales).
- Además, se hará un seguimiento regular para mantener el tema activo durante todo el año, sin que la campaña pierda fuerza.

2. Sensibilización a través de la interacción:

- **Simulacros de seguridad:** Realizar simulacros donde los funcionarios enfrenten situaciones como ciberataques o pérdidas de datos. Esto no solo genera aprendizaje, sino que crea un ambiente de preparación.
- **Concursos y desafíos de seguridad:** Organizar competencias amistosas dentro de la institución donde los empleados deban identificar vulnerabilidades o responder preguntas relacionadas con seguridad de la información.
- **Testimonios y ejemplos reales:** Compartir casos reales (sin comprometer la confidencialidad) donde se hayan producido incidentes de seguridad debido a malas prácticas. Esto ayuda a sensibilizar de manera más efectiva.

3. Capacitación interactiva:

- **Módulos de aprendizaje en línea:** Cursos interactivos en línea sobre las principales políticas de seguridad de la información, amenazas comunes y protocolos de respuesta a incidentes.
- **Sesiones prácticas:** Talleres donde los empleados puedan practicar cómo crear contraseñas seguras, reconocer correos electrónicos fraudulentos o manejar información confidencial de forma adecuada.

4. Liderazgo visible:



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- Involucrar a los directores y subdirectores en la campaña, pidiéndoles que participen activamente en las sesiones de sensibilización, fomenten la cultura de seguridad dentro de sus equipos y sirvan de ejemplo para los demás.
- Los directivos deben transmitir el mensaje de que la seguridad de la información es una prioridad institucional.

Tiempos de cumplimiento

1. Fase inicial (0-3 meses):

- Lanzamiento de la campaña con la distribución de materiales visuales (carteles, folletos, fondos de pantalla).
- Capacitación general para todos los funcionarios sobre el EGSi y la importancia de la seguridad de la información.
- Simulacro inicial de seguridad (por ejemplo, pruebas de respuesta ante un ciberataque).

2. Fase de ejecución continua (4-9 meses):

- Realización de talleres prácticos y capacitación continua.
- Campañas cuatrimestrales enfocadas en temas específicos como el manejo de contraseñas, protección de dispositivos móviles, y respuestas ante incidentes.
- Evaluación intermedia de la efectividad de la campaña con encuestas y análisis de participación.

3. Fase de evaluación y ajustes (10-12 meses):

- Evaluación global del impacto de la campaña a través de encuestas de satisfacción y pruebas de conocimiento.
- Ajuste de la estrategia según los resultados obtenidos para mejorar la sensibilización en áreas que requieran más atención.
- Informe final de evaluación con los logros alcanzados y las áreas de mejora.

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN

3.3. Identificación de necesidades

Análisis de la situación actual

Para entender la situación actual respecto a la seguridad de la información en el Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), es fundamental identificar las fortalezas y áreas de mejora dentro de los procesos y prácticas relacionadas con la protección de la información. Este análisis nos permitirá priorizar las acciones de sensibilización y capacitación en los puntos críticos y garantizar que la campaña de sensibilización sea dirigida a las necesidades reales de la institución.

Metodología: Encuesta y evaluación de procesos actuales

El análisis previo se realizará principalmente a través de encuestas y entrevistas con los empleados de diferentes niveles y áreas de la institución. Esto permitirá recoger información sobre su conocimiento y prácticas actuales relacionadas con la seguridad de la información. La encuesta cubrirá, entre otros, los siguientes temas:

1. Conocimiento sobre el EGSi:

- ¿Conoces las políticas de seguridad de la información implementadas en la institución?
- ¿Sabes cuáles son los principales riesgos asociados a la seguridad de la información?

2. Prácticas de seguridad actuales:

- ¿Con qué frecuencia actualizas tus contraseñas?
- ¿Sigues procedimientos establecidos para manejar información confidencial?
- ¿Cómo gestionas el acceso a la información en tu área de trabajo?

3. Amenazas y vulnerabilidades percibidas:

- ¿Qué tipo de amenazas consideras que son las más peligrosas en tu entorno de trabajo (phishing, robo de datos, acceso no autorizado, etc.)?
- ¿Sientes que la institución tiene medidas adecuadas para prevenir incidentes de seguridad?

4. Capacitación previa y necesidad de formación:



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- ¿Has recibido capacitación en seguridad de la información? Si es así, ¿con qué frecuencia?
- ¿Qué temas te gustaría que se cubrieran más a fondo en futuras capacitaciones?
- ¿Cómo evaluarías tu nivel de conocimiento sobre seguridad informática versus seguridad de la información?

5. Identificación de los temas clave de sensibilización y capacitación

A partir de las respuestas a las encuestas y el análisis de los procesos actuales, se podrán identificar los temas que requieren mayor atención. Algunos de los temas clave que probablemente se destaquen incluyen:

1. Gestión de contraseñas y autenticación:

- La necesidad de contraseñas seguras y el uso de autenticación de dos factores puede ser una de las áreas con mayor desconocimiento.

2. Reconocimiento de amenazas cibernéticas:

- Muchos funcionarios pueden tener dificultades para identificar correos electrónicos fraudulentos, ataques de phishing, o software malicioso. La capacitación debe enfocarse en enseñar a identificar estos ataques.

3. Protección de datos personales y confidenciales:

- Los empleados pueden no estar completamente familiarizados con la importancia de proteger la información sensible, tanto en formato digital como impresa. Se debe reforzar la capacitación en la clasificación de la información y los procedimientos de manejo adecuado.

4. Procedimientos de respuesta ante incidentes de seguridad:

- La mayoría de los empleados puede no saber qué hacer en caso de una brecha de seguridad. Se deben impartir simulacros y procedimientos claros para que todos sepan cómo actuar.

5. Confusión entre seguridad informática y seguridad de la información:

- Es crucial aclarar que la seguridad de la información abarca no solo la protección de sistemas informáticos, sino también la protección



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



de información física (documentos, archivos) y las políticas de acceso a esos datos.

6. Priorización de temas para la capacitación

Basado en los resultados de las encuestas y entrevistas, se priorizarán los temas más críticos y con mayor desconocimiento, de modo que las capacitaciones y socializaciones se enfoquen en estas áreas. Por ejemplo, si la mayoría de los empleados tienen poca comprensión sobre los riesgos de phishing, se organizará una campaña intensiva sobre cómo reconocer correos fraudulentos y qué hacer al respecto.

7. Evaluación continua de las necesidades

Una vez implementado el plan, se realizará una evaluación continua mediante:

- **Encuestas post-capacitación:** Para medir la efectividad de las actividades realizadas y detectar posibles áreas de mejora.
- **Monitoreo de incidentes:** Evaluar si ha habido una reducción en los incidentes de seguridad, lo que indicaría que los empleados están aplicando correctamente los conocimientos adquiridos.

3.4. Roles y responsabilidades

1. Comité de Seguridad de la Información (CSI)

Rol principal: Liderar, coordinar y supervisar el desarrollo e implementación del **Plan de Comunicación y Sensibilización**.

Responsabilidades:

- **Definir la estrategia global** de comunicación y sensibilización en relación con el EGSÍ.
- Aprobar el **contenido y los materiales** de capacitación y sensibilización.
- **Monitorear y evaluar** la efectividad del plan, ajustando las estrategias según sea necesario.
- Coordinar las **actividades de sensibilización** a nivel institucional, asegurándose de que todos los departamentos estén alineados con las políticas de seguridad de la información.
- **Gestionar la participación** de los directores de cada Dirección para asegurar la adopción de las políticas en todas las unidades.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



2. Dirección General De Tecnologías De La Información Y Comunicaciones

Rol principal: Apoyar en la infraestructura tecnológica y en la gestión de plataformas de capacitación.

Responsabilidades:

- Proporcionar la infraestructura técnica para la realización de capacitaciones virtuales (plataformas de e-learning, videoconferencias, etc.).
- Asegurarse de que los canales de difusión digital (correo electrónico, intranet, plataformas de aprendizaje) funcionen correctamente.
- Apoyar en el desarrollo y distribución de materiales digitales (videos, infografías, etc.) para las actividades de sensibilización.
- Soporte en la seguridad: Asegurar que los sistemas utilizados para la capacitación y la distribución de información sean seguros y no vulnerables a amenazas cibernéticas.

3. Dirección General de Recursos Humanos (RR.HH.)

Rol principal: Coordinar la logística y el seguimiento de las actividades de sensibilización dentro de los departamentos.

Responsabilidades:

- Coordinar las capacitaciones con las diferentes direcciones, asegurándose de que todos los funcionarios estén informados y participen.
- Gestionar la logística de las sesiones presenciales y virtuales, incluyendo la programación, inscripción y seguimiento.
- Colaborar en la evaluación del impacto de las capacitaciones mediante encuestas de satisfacción y desempeño.

4. Directores de las distintas dependencias

Rol principal: Difundir y velar por el cumplimiento de las políticas de seguridad de la información dentro de sus equipos.

Responsabilidades:



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- Promover la participación activa de sus equipos en las actividades de sensibilización y capacitación.
- Realizar seguimiento a la aplicación de las políticas de seguridad de la información en el día a día de sus equipos.
- Ser responsables de la transmisión de la información: Asegurar que sus equipos entiendan y apliquen correctamente los procedimientos de seguridad.
- Proveer retroalimentación sobre las necesidades de capacitación o problemas específicos que enfrenten sus equipos en relación con la seguridad de la información.

5. Comunicación Institucional

Rol principal: Apoyar la visibilidad y difusión de la campaña de sensibilización a través de canales de comunicación internos.

Responsabilidades:

- Diseñar, crear y distribuir los materiales visuales de la campaña, incluyendo carteles, folletos, videos y otros recursos gráficos.
- Gestionar la difusión de los mensajes de sensibilización a través de la intranet, correo electrónico y pantallas digitales.
- Organizar eventos internos de sensibilización, como seminarios, jornadas de concienciación, etc.
- Monitorear el impacto de las campañas de sensibilización, recopilando datos sobre la participación y efectividad.

6. Gestión de Recursos Económicos

Rol principal: Gestionar los recursos financieros necesarios para implementar las actividades del plan.

Responsabilidades:

- Asignar y gestionar el presupuesto necesario para llevar a cabo las actividades de sensibilización, incluyendo la compra de materiales, contratación de facilitadores o expertos y costos asociados a la logística de las capacitaciones.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- Evaluar el retorno de inversión (ROI) de las actividades de sensibilización, asegurando que los recursos sean utilizados de manera eficiente.

7. Oficial de Seguridad de la Información

Rol principal: Medir la efectividad del plan y realizar ajustes para mejorar las futuras actividades de sensibilización.

Responsabilidades:

- Desarrollar y aplicar métodos de evaluación para medir el impacto de las capacitaciones y actividades de sensibilización (encuestas, pruebas de conocimientos, análisis de incidentes de seguridad, etc.).
- Recopilar y analizar retroalimentación de los participantes para identificar áreas de mejora en el contenido y formato de las actividades.
- Ajustar las estrategias de comunicación y sensibilización basadas en los resultados de las evaluaciones y los cambios en el entorno de seguridad de la información.

3.5. Resultados y logros esperados

Logros esperados

- **Compromiso con el EGSi:** Los funcionarios adoptarán las políticas de seguridad de la información y estarán comprometidos con su implementación.
- **Reducción de incidentes de seguridad:** Se disminuirán los incidentes relacionados con el acceso no autorizado y la pérdida de información.
- **Mayor conocimiento:** Los empleados estarán mejor preparados para identificar amenazas y aplicar buenas prácticas de seguridad.
- **Cambio cultural:** Se promoverá una cultura organizacional de responsabilidad sobre la seguridad de la información.
- **Alta participación:** Se espera una participación mínima del 80% de participación en actividades de sensibilización.

Evaluación de eficacia



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- **Encuestas de satisfacción:** Medición de la efectividad de las capacitaciones.
- **Evaluaciones de conocimiento:** Comparación del nivel de conocimiento antes y después de las actividades.
- **Monitoreo de incidentes:** Análisis de la reducción de incidentes de seguridad.
- **Participación:** Seguimiento de la asistencia y el involucramiento en las actividades

3.6. Cronograma de actividades de comunicación o sensibilización

Fase 1: Lanzamiento y Preparación (Mes 1)

- **Semana 1:**
 - Lanzamiento oficial del Plan de Comunicación y Sensibilización (presentación del objetivo, importancia, y expectativas).
 - Distribución de materiales iniciales (folletos, carteles, fondos de pantalla, etc.).
 - Reunión introductoria con los Directores y líderes de cada área para alinear las actividades.
- **Semana 2-3:**
 - Capacitación inicial sobre el EGSÍ para todos los empleados (presencial o virtual).
 - Campaña de sensibilización: Anuncio sobre el plan a través de correo institucional e intranet.

Fase 2: Ejecución de actividades de sensibilización (Meses 2-9)

- **Mes 2-3:**
 - Realización de talleres interactivos sobre seguridad de la información (reconocimiento de amenazas, manejo de contraseñas, etc.).
 - Simulacro de incidentes de seguridad: Actividad práctica para evaluar la respuesta ante un ciberataque.
- **Mes 4-6:**



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- Campaña de concientización continua: Recordatorios mensuales a través de pantallas digitales, correo electrónico y carteles.
- Capacitación adicional sobre protección de datos personales y seguridad en dispositivos móviles.

- **Mes 7-9:**

- Sesiones de actualización para nuevos empleados y para aquellos que necesiten repaso de los contenidos clave.
- Encuesta de evaluación para medir el impacto de las actividades hasta el momento (retroalimentación sobre lo aprendido y áreas de mejora).

Fase 3: Evaluación y Ajustes (Meses 10-12)

- **Mes 10:**

- Revisión y análisis de los resultados obtenidos: ¿Qué se ha logrado? ¿Dónde hay oportunidades de mejora?
- Informe de impacto sobre la reducción de incidentes de seguridad y aumento en la participación.

- **Mes 11-12:**

- Ajustes a la campaña basados en la retroalimentación recibida.
- Segunda ronda de simulacros y capacitación para resolver cualquier área que necesite más atención.

- **Actividades Continuas (Anual)**

- Actualización de contenidos: Revisión anual de materiales de sensibilización y capacitación.
- Reevaluación del conocimiento a través de encuestas y evaluaciones periódicas para seguir mejorando la seguridad de la información.

4. Glosario de términos

Término	Definición
EGSI	Esquema Gubernamental de Seguridad de la Información. Conjunto de políticas y medidas que

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN

	buscan proteger la información dentro del sector público, asegurando su confidencialidad, integridad y disponibilidad.
Seguridad de la Información	Prácticas y procesos destinados a proteger la información contra acceso no autorizado, alteración, destrucción o pérdida. Incluye tanto la seguridad digital como la física.
Phishing	Técnica de fraude cibernético utilizada para engañar a las personas y obtener información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos o sitios web falsos.
Ciberseguridad	Conjunto de medidas y prácticas enfocadas en proteger los sistemas informáticos y redes contra ataques, daños o accesos no autorizados.
Contraseña segura	Conjunto de caracteres que sirven para autenticar la identidad del usuario en un sistema, que debe ser compleja, única y cambiarse regularmente para evitar accesos no autorizados.
Protección de datos personales	Medidas para garantizar la seguridad y privacidad de los datos personales de los individuos, en conformidad con las leyes y normativas aplicables.
Incidente de seguridad	Evento o serie de eventos que comprometen la confidencialidad, integridad o disponibilidad de la información o los sistemas.
Simulacro de seguridad	Ejercicio práctico realizado para entrenar a los empleados en cómo reaccionar ante incidentes de



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



	seguridad, como ciberataques o pérdida de información.
--	--

5. Documentos de referencia

- **Acuerdo Ministerial No. 2024-003 del Ministerio de Telecomunicaciones y de la Sociedad de la Información:** Establece las directrices para la implementación de medidas de seguridad de la información en el sector público.
- **Esquema Gubernamental de Seguridad de la Información (EGSI v3.0):** Documento que establece las políticas, procedimientos y directrices para la protección de la información dentro de las instituciones del Estado.
- **Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27005:** Normas internacionales que definen los requisitos y las mejores prácticas para gestionar la seguridad de la información.
- **Agenda y Reglamento Interno del Comité de Seguridad de la Información:** Documento interno que regula las funciones y responsabilidades del Comité de Seguridad de la Información dentro de la institución.
- **Política de Seguridad de la Información:** Conjunto de directrices y normas que rigen el manejo seguro de la información dentro de la organización.

6. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	Ing. Juan Carlos Mena Molina Oficial de Seguridad de la Información	 Firmado electrónicamente por: JUAN CARLOS MENA MOLINA
Revisado por:	Ing. María Cielito Mejía Muñoz Directora General de Talento Humano (E)	 Firmado electrónicamente por: MARIA CIELITO
Revisado por:	Ing. Felipe Peralta Velasquez Director General Administrativo (E)	 Firmado electrónicamente por: FELIPE ANTONIO PERALTA VELASQUEZ



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



Revisado por:	Ing. Johnny Aguayo Aguirre Director General de Tecnologías de la Información y Comunicaciones	 Firmado electrónicamente por: JOHNNY ALBERTO AGUAYO AGUIRRE
Revisado por:	Abg. Eleana Lecaro Monroy Delegada de Protección de Datos Personales	 Firmado electrónicamente por: ELEANA GABRIELA LECARO MONROY
Aprobado por:	Abg. Camila Veloz Jaramillo Directora General de Asesoría Legal (E)	 Firmado electrónicamente por: CAMILA VICTORIA VELOZ JARAMILLO
Aprobado por:	Ing. Diana Tinoco Ajila Directora General de Comunicación Social	 Firmado electrónicamente por: DIANA CAROLINA TINOCO AJILA
Aprobado por:	Ing. Edwin Angulo Cardona Director General de Planificación Institucional (E)	 Firmado electrónicamente por: EDWIN JOHNNY ANGULO CARDONA



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



Control de versiones del formato referencial

Versión:	1.1
Fecha de la versión:	17-07-2026
Creado por:	Oficial de Seguridad de la Información del Benemérito Cuerpo de Bomberos de Guayaquil
Aprobado por:	Comité de Seguridad de la Información del Benemérito Cuerpo de Bomberos de Guayaquil
Nivel de confidencialidad:	Bajo

Historial de cambios del formato referencial

Versión	Fecha	Detalle del cambio
F1.0	17/07/2026	Emisión inicial del documento