MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN “MIPG”

POLITICA DE SEGURIDAD DIGITAL

EMPRESA SOCIAL DEL ESTADO
ESE BELLOSALUD
BELLO, ANTIOQUIA

DICIEMBRE 2020

DIEGO ALFONSO MONTOYA GRAJALES
GERENTE

FABIO LEÓN LONDOÑO PARRA
SUBGERENTE DE TALENTO HUMANO

ALEJANDRO ALZATE
SUBGERENTE ADMINISTRATIVO Y FINANCIERO

PAULA ANDREA GONZALEZ LEON
SUBGERENTE DE SERVICIOS DE SALUD

LINA MARÍA VÁSQUEZ CASTAÑEDA
PROFESIONAL UNIVERSITARIO MIPG

JAVIER ANTONIO LÓPEZ RESTREPO
JEFE DE OFICINA DE CONTROL INTERNO

INTRODUCCION

La dependencia de las tecnologías de la información y las comunicaciones interconectadas globalmente ha puesto en el centro de la discusión la necesidad de trabajar en políticas y/o estrategias nacionales de seguridad digital. Esta necesidad es alimentada por el aumento de incidentes y ataques digitales con potenciales consecuencias catastróficas para la protección de la seguridad de la información, por tanto, de las personas.

Siendo la seguridad digital una discusión cada vez más crítica, hay que reconocer que la sociedad civil y los grupos de interés público no son suficientemente considerados, algo que desequilibra el debate y lo ubica en un tema enfocado en los sistemas o vagos conceptos de seguridad nacional, en lugar de las personas.

Sin embargo, la seguridad digital está intrínsecamente relacionada con las personas, pues la forma en cómo se definen e implementan las políticas de regulación del comportamiento en línea y la seguridad de la información tienen profundas implicaciones para los derechos humanos, en especial la privacidad, la libertad de expresión o la libre asociación.

Es así que la Política de seguridad digital está enfocada a contrarrestar las amenazas cibernéticas, siendo la gestión del riesgo la parte fundamental de esta política, la seguridad digital por ser la información el activo más importante de la organización, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad de la información. Por lo tanto, las entidades, organismos y órganos de control deberán analizar las particularidades de funcionamiento de cada entidad y adoptar las políticas de protección y mitigación que resulten pertinentes a sus necesidades, adoptando el enfoque de gestión de riesgos al que hace referencia el CONPES 3854 de Seguridad Digital o aquella norma que lo modifique o sustituya.

El presente documento se encuentra la formulación de la Política de Seguridad Digital para la ESE Bellosalud, la cual se diseña bajo los lineamientos del Modelo Integrado de Planeación y Gestión -MIPG, en el marco de su implementación.

1. JUSTIFICACION

En el Decreto 1499 de 2017 y el Manual de MIPG se encuentra la Dimensión Gestión con Valores para Resultados donde la entidad debe tener en cuenta acciones relevantes dentro de su organización asociadas a aspectos considerados de la "Ventanilla hacia adentro" haciendo necesario la implementación y adopción de una política de Seguridad digital, la cual debe desarrollarse con lineamientos contenidos en el CONPES 3854 de 2016 Política Nacional de Seguridad digital.

Que el numeral 8 del artículo 2 de la Ley 1341 de 2009 establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea, con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada Ley determinó que es función del Estado intervenir en el sector de las TIC, con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector; así como reglamentar las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada.

2. OBJETIVO

Diseñar estrategias para mejorar las capacidades de los funcionarios de la ESE Bellosalud para identificar, tratar y mitigar los riesgos de seguridad digital, en todas sus actividades en el entorno digital, en un marco de cooperación, colaboración y asistencia.

3. ALCANCE

La Política de Seguridad Digital en la ESE Bellosalud busca garantizar que la entidad identifique el peligro de los riesgos de su entorno digital con el fin de desarrollar nuevas capacidades frente a sistemas de seguridad digital que permiten que la entidad tenga un manejo confiable y seguro de la información.

4. MARCO LEGAL

Numero	Año	Descripción
Constitución Política de Colombia	1991	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 23	1982	Derechos de autor

Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594	2000	Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100de 2004. Por medio del cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Ley 603	2000	Esta Ley se refiere a la protección de los derechos de autor en Colombia. El software en un archivo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
Ley 962	2005	Simplificación y Racionalización de Tramite. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150	2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266	2008	Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273	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.
Ley 1341	2009	Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones – TIC -, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Ley 1712	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.
Decreto 2693	2012	Estrategia de Gobierno en Línea. Ministerio de tecnologías de la Información y las comunicaciones.
Decreto 1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto 103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de tecnologías de la Información y las Comunicaciones.

5. DEFINICIONES

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligue o genere, obtenga, adquiera, transforme o controle en su calidad de tal.
Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Lineamientos: Directriz o disposición establecida por el Ministerio TIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.

Estándar: Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización y es de obligatorio cumplimiento.

Arquitectura: Este habilitador busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades Institucionales y de gestión TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

Seguridad de la Información: Este habilitador busca que las entidades públicas incorporen la Seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales; este habilitador tiene un soporte en el MSPI.

Confidencialidad: La información no se pone a disposición, ni se revela a individuos, entidades o procesos autorizados.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Riesgo: Posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Múltiples partes interesadas: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

Bajo el enfoque de la política nacional de seguridad digital:

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Entorno digital abierto: entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Incidente digital: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido

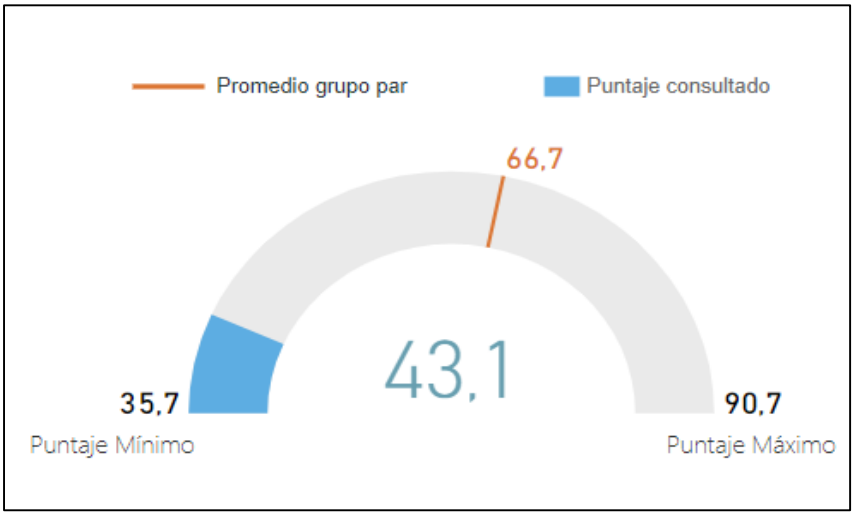
Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

6. DIAGNOSTICO

Teniendo como base el diligenciamiento del cuestionario del Formulario Único de Reporte de Avance a la Gestión, FURAG, aplicado para la vigencia 2019, se puede evidenciar que la Empresa Social del Estado ESE Bellosalud,

presenta el 43,1% de avance en la elaboración, aprobación e implementación de la política de Seguridad Digital, tal como se evidencia en la gráfica.

RESULTADO FURAG 2019. Política de Seguridad Digital



7. PRINCIPIOS POLITICA DE SEGURIDAD DIGITAL

La Política nacional de gobierno digital recomienda que se debe tener en cuenta dos tipos de principios que son: generales y operativos. Los principios generales están dirigidos a las múltiples partes interesadas quienes, directa o indirectamente, desarrollan algunas o todas sus actividades socioeconómicas en el entorno digital. Los principios operativos están dirigidos a los líderes o tomadores de decisiones, quienes por su alto nivel en las organizaciones deben enfocar sus acciones hacia la adopción del marco general de gestión del riesgo de seguridad digital.

Principios Generales:

Conocimiento, capacidades y empoderamiento: Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto.

Responsabilidad: Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.

Derechos humanos y valores fundamentales: Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

Cooperación: Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

Principios operativos:

Evaluación De Riesgos Y Ciclo De Tratamiento: la evaluación de riesgos debe llevarse a cabo de manera sistemática y continua, evaluando las posibles consecuencias de las amenazas y las vulnerabilidades digitales en las actividades económicas y sociales en juego. El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable en relación con los beneficios económicos y sociales.

Medidas De Seguridad: los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo, y deben tener en cuenta su potencial impacto, negativo o positivo, sobre las actividades económicas y sociales que tienen por objeto proteger. La evaluación de riesgos de seguridad digital debe guiar la selección, operación y mejora de las medidas de seguridad para reducir el riesgo a niveles aceptables.

Innovación: los líderes y tomadores de decisiones deben asegurarse de que la innovación sea considerada como parte integral de la reducción del riesgo de seguridad digital. Esta debe fomentarse tanto en el diseño y funcionamiento de la economía, y de las actividades sociales basadas en el entorno digital, como en el diseño y el desarrollo de las medidas de seguridad.

Preparación Y Continuidad: con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales, deben adoptarse preparaciones y planes de continuidad. El plan debe identificar las medidas para prevenir, detectar, responder y recuperarse de los incidentes y proporcionar mecanismos claros de escalamiento.

Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. En caso de limitación a estos derechos, debe ser bajo medidas excepcionales y estar conforme con la Constitución Política y los estándares internacionales aplicables. Estas medidas, deben ser proporcionales, necesarias y estar enmarcadas en la legalidad.

Adoptar un enfoque incluyente y colaborativo que involucre activamente a las múltiples partes interesadas, y que permita establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del país y sus habitantes, y aumentar la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital.

Asegurar una responsabilidad compartida entre las múltiples partes interesadas, promoviendo la máxima colaboración y cooperación. Lo anterior, teniendo en cuenta el rol y el grado de responsabilidad de cada parte para gestionar los riesgos de seguridad digital y para proteger el entorno digital.

La ESE Bellosalud estable las siguientes acciones para mantener el estado de implementación de esta Política:

- ✓ Revisión de la Política de Seguridad Digital y mecanismos que permitan verificar su cumplimiento.
- ✓ Revisión y aprobación de los activos y Riesgos de Seguridad Digital.
- ✓ Realizar campañas de concientización en temas de Seguridad Digital teniendo en cuenta los diferentes roles definidos dentro de la “Matriz roles y responsabilidades” del Sistema de Gestión de la Seguridad de la Información SGSI.
- ✓ Revisión de indicadores asociados a los objetivos del Sistema de Gestión de la Seguridad de la Información SGSI, con el fin de verificar su cumplimiento y alineación.

DIEGO ALFONSO MONTOYA GRAJALES
Gerente ESE Bellosalud

Elaboró	**Revisó**	**Aprobó**
Profesional Universitarios MIPG	Asesor de Planeación	Comité de Gestión y desempeño
Fecha: Diciembre de 2020	Fecha: Diciembre de 2020	Fecha: Diciembre de 2020