PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

La Plata (H), Enero 2018

CONTEXTO Y JUSTIFICACIÓN

Los grandes volúmenes de información institucionales se originan desde diversas fuentes y con estándares tecnológicos heterogéneos -en hardware, software, comunicaciones- que requieren de una infraestructura de red adecuada, funcional y confiable para su transmisión y almacenamiento.

En el caso de la E.S.E. San Sebastián de la Plata Huila, las soluciones de conectividad y servicios informáticos fueron diseñados fundamentalmente para soportar aplicaciones de procesamiento de datos que funcionan en un servicio de transporte operativo pero que no han sido rigurosas en parámetros de QoS (calidad del servicio) y CyberSec (ciberseguridad). El crecimiento exponencial de nuevos servicios y aplicaciones -para los cuales no se hizo una planeación adecuada; ha desencadenado en un conjunto de dificultades en la operación de la red y en la gestión de la seguridad de la información, elementos que han estado en una baja y arriesgada prioridad en el dimensionamiento tecnológico institucional. En el marco de las TI se hace necesaria la implementación de estrategias de seguridad para preservar los servicios disponibles y garantizar la confidencialidad e integridad de los datos en las aplicaciones. Existen algunos estándares de seguridad informática que sugieren -como primera medida- realizar análisis de vulnerabilidades para responder corrigiendo posibles fallos y apuntando a modelos preventivos. Estos esfuerzos son inocuos, si en este mismo sentido, la alta dirección no está involucrada y comprometida con la implementación de un Sistema Integral de la Seguridad de la Información.

El presente documento pretende exponer una serie de lineamientos para implementar las mejores prácticas de Seguridad Informática en la E.S.E., con el fin de optimizar la disponibilidad, la integridad, la confidencialidad/privacidad, entre otros principios relevantes, teniendo en cuenta la infraestructura y limitaciones actuales.

OBJETIVOS

OBJETIVO GENERAL Elaborar un documento de lineamientos básicos de buenas prácticas en Seguridad y Privacidad para la Empresa.

OBJETIVOS ESPECÍFICOS

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Orientar a las entidades destinatarias en las mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- Optimizar la labor de acceso a la información pública al interior de las entidad.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

SEGURIDAD PERIMETRAL

En la Empresa Social del Estado San Sebastián, se encuentra implementada una solución en alta disponibilidad de Firewall UTM (Unified Threat Management) que contribuye a la seguridad perimetral de los datos, aplicaciones, servicios, servidores y usuarios finales. La solución Fortigate fue configurada para controlar el tráfico bidireccional entre la red de la E.S.E., e internet, evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet y examinar todos los paquetes de datos que entren o salgan de la red local, bloqueando aquellos que no cumplen los criterios de seguridad especificados. Los dispositivos encargados de estas tareas son dos Fortigate, con características completas de UTM (Gestión Unificada de Amenazas) incluyendo firewall, IPS (Sistemas de Prevención de Intrusos), Antivirus, AntiSpam, VPN, Filtrado Web y control de Aplicaciones. Adicionalmente se cuenta con un Fortianalyzer para el análisis de tráfico y la generación de reportes. El análisis de estos reportes lleva a la detección de fallas de seguridad e intrusiones frustradas, además los servicios de subscripción Fortiguard proveen conexión y actualización a las bases de datos propietarias para Antivirus, Prevención de Intrusiones, Filtrado Web, AntiSpam y control de aplicaciones.

En capa lógica, se cuenta con segmentación de dominios de broadcast a través de VLANs conectadas a los diferentes puertos del Firewall, procurando controlar el tráfico de cada subred de acuerdo al rol de grupos de usuarios/máquinas: Equipos activos, administrativos, Innovación, oficina de sistemas, almacenamiento, telefonía y Wireless, además se cuenta con un configuración de dominio empresarial desde la cual solo los usuarios y equipos registrados en el Active Directory del Windows Server pueden acceder a los diferentes sistemas de información de la institución.

Para la conectividad WAN la E.S.E tiene un canal dedicado, dividido en 500 Mbps operativo y 500 Mbps para uso administrativo, contratados con Azteca y vinculados a un enrutador Cisco y este a su vez a un enrutador TPLINK que realiza la conmutación de forma transparente de acuerdo al destino del paquete enviado, si se trata de una petición hacía uno de los sitios de la red operativa, la navegación se realiza a través del canal de 500 Mbps y si se trata de una solicitud hacía una página comercial, se utiliza el otro canal de 500 Mbps. Debido a las necesidades actuales de la institución, se hace necesario aplicar traffic shapers a las políticas de navegación de las redes, así como filtros web y controles de aplicaciones para cada VLAN, con el fin de optimizar la seguridad y el uso del canal.

RED

La red LAN de la E.S.E. cuenta con un switch de Núcleo Hewleth Packard, donde convergen las conexiones de los servidores, los switch de distribución de las diferentes sedes y los equipos de seguridad perimetral, formando una topología en estrella extendida con centro en el switch de núcleo, adicionalmente operan varias VLANs que segmentan la red a nivel lógico.

De la mano de cualquier adquisición o mejora a nivel técnico, es importante implementar políticas en el manejo de los recursos tecnológicos, para brindar apoyo y orientación a los funcionarios, docentes y estudiantes respecto a la seguridad de la información, acorde a las necesidades y requisitos de la institución.

SERVIDORES

Bajo la administración de la oficina de sistemas existen 2 Servidores HP ProLiant, 1 como servidor de Dominio en el cual se encuentran las políticas de seguridad Firewall, DNS, IIS, ActiveDirectory, Plantillas de recurso administrativo y otro como Servidor de Base de Datos el cual contiene la información del sistema de información hospitalario y a su vez tiene configurada una carpeta por área en la cual se encuentra la información más importante de las actividades y procesos de cada uno de las áreas de la institución, 1 servidor de almacenamiento storage el cual se programó para que se realice copias de seguridad automática de todo el sistema de información diariamente.

APLICACIONES Y BASES DE DATOS

El análisis de aplicaciones conectadas es primordial para poder establecer posibles fallos de implementación que conducen a vulnerabilidades en cualquier de las capas de las arquitecturas desplegadas.

Los puntos de control más relevantes que se verificarán estarán concentrados en: validar desbordamientos de pilas, verificación de cadenas y secuencias inválidas, datos inconsistentes de control, inspección de Metadatos que conducen a fugas de información, errores de validación, errores de procesamiento, entre otros.

Las bases de datos actuales están instaladas en dos nodos redundantes, en este momento se están ejecutando actividades como: Actualización mensual de las instancias de pruebas, creación de usuarios y esquemas, asignación y revocatoria de permisos en los usuarios, mantenimiento de Tablespaces, detección y eliminación de bloqueos, copias de seguridad diarias, instalaciones periódicas de nuevas actualizaciones de software.

Existen un número importante de aplicaciones desarrolladas y contratadas que tienen vínculo con otros gestores de bases de datos relacionales y servidores de despliegue donde es inminente generar un estudio de seguridad multicapa para identificar riesgos potenciales.

También se deben contemplar otras actividades como: documentación de estadísticas de rendimiento, incluyendo los posibles cambios de configuración y sincronización que esto conlleva y realizar afinamientos periódicos con su correspondiente documentación, para un rendimiento óptimo de la base de datos.

GLOSARIO

- Acceso a la Información Pública:

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- Activo

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Activo de Información:
- En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Archivo:

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un

Sistema o a la organización. (ISO/IEC 2700)

- Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- Autorización:

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- Bases de Datos Personales:

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- 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).

- Ciberespacio

Es el 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).

- 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.

- Datos Abiertos:

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- Datos Personales:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- Datos Personales Públicos:

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- Datos Personales Privados:

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- Datos Personales Mixtos:

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- Datos Personales Sensibles:

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- Declaración de aplicabilidad

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- Derecho a la Intimidad:

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- Encargado del Tratamiento de Datos:

  Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- Gestión de incidentes de seguridad de la información Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- Información Pública Clasificada: 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. (Ley 1712 de 2014, art 6).

- 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)

- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

- Ley de Transparencia y Acceso a la Información Pública:

Se refiere a la Ley Estatutaria 1712 de 2014.

- Mecanismos de protección de datos personales:

Lo constituyen las distintas alternativas con que cuentan las entidades

destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- Plan de continuidad del 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).

- Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- Privacidad:

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- Registro Nacional de Bases de Datos:

Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- Responsabilidad Demostrada:

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y

Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 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 y de mejora continua. (ISO/IEC 27000).

- Titulares de la información:

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- Tratamiento de Datos Personales:

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- Partes interesadas (Stakeholder)

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

CONTROL DE DOCUMENTO Y DISTRIBUCIÓN

Control del Documento

	Nombre	Cargo	Dependencia	Fecha
Autor	John Jader Trujillo	Contratista	GTI	2018.
Revisión	Francisco J. Currea	Subgerente	Subgerencia	
Aprobación	Luis A. Granados A.	Gerente	Gerencia	

Estado:	Preparación:	X	Revisión:	**x**	Aprobación	X

Control de los Cambios

Versión No.	Fecha de Aprobación	Descripción de los Cambios	Solicitó
1	16/01/2018. Resol.020	Primera versión Plan PETI.	Gerencia
2			
3			

Lista de distribución

VERSIÓN	FECHA	ÁREA	FIRMA
1	16/01/2018	Proceso Gestión de la información	
2			