UNIVERSIDAD APEC

Decanato de Escuela de graduados

Maestría en Gerencia y Productividad

Titulo

"Propuesta de las políticas y procedimientos para la seguridad de la información tecnológica (CYBERSECURITY) en la empresa AES Dominicana, año 2014"

NOMBRE	MATRICULA
Yoel Fabian	2004-0544

PROFESORA:

Edda Freites, MBA

Santo Domingo, República Dominicana

2014

Resumen

El objetivo de desarrollo de esta investigación está determinado por la necesidad que existe mundialmente en las empresas de garantizar la integridad de su información. Se presenta una *propuesta de las políticas y procedimientos para la seguridad de la información tecnológica (CYBERSECURITY) en la empresa AES Dominicana, año 2014.* La interrogante de la investigación realizada surge para proponer un modelo de protección continua contra cualquier amenaza tecnológica externa o interna contra la empresa en busca de sustraer, modificar o eliminar datos en los sistemas. La seguridad informática ha logrado obtener una participación mayor dentro de las organizaciones debido a las condiciones cambiantes y nuevas plataforma que día tras días salen a la calle y cuyos individuos muy inteligentes se aprovechan de estas para lograr introducirse sin autorización a la compañía y comprometer la información de la empresa. El propósito es describir las normas de seguridad cibernética recomendadas que deben aplicar y ser adoptadas AES Dominicana, empresa parte de la SBU MCA&C. Estas normas establecen los requisitos mínimos de seguridad cibernética. Podrían elegir implementaciones más rigurosas de estas normas pero no deben estar por debajo. Considerando que las políticas tienen como propósito fundamental definir las reglas para un negocio de alto nivel para la seguridad cibernética, esta propuesta establece los requisitos detallados sobre cómo se deben implementarse las políticas.

Agradecimiento

Quiero agradecer a mis familiares por el apoyo incondicional recibido y sus soportes en los días más difíciles como estudiante. Agradezco a Dios por darme la salud física y mental necesaria.

A la empresa AES Dominicana, por permitir hacer el desarrollo de esta monografía dentro de sus instalaciones, ofreciendo herramientas y las informaciones necesarias en colaboración con este proyecto.

Por último y no menos importante quiero agradecer a mis amigos, y compañeros de trabajo, en especial a las nuevas y otras no tan nuevas pero valiosas amistadas que pude cosechar durante el desarrollo de la maestría como fueron Omar Duran, Geraldine Rodriguez, Rubén Aponte, Miguel Pontier e Indhira Marte en especial con quien estuve desde el primer día de la maestría y fue un ejemplo a seguir de dedicación y perseverancia.

Dedicatoria

Esta tesis de grado está a dedicada en primer lugar a Dios, por ser el principal soporte de vida y de todo lo que la compone. A mi padre fallecido en la gracia del señor Dios, que durante toda mi vida fue un pilar de mi desarrollado, siempre preocupado, atento y dispuesto a ayudarme por encima de sí mismo; hasta el último momento de su vida. Mi madre por ser la persona que desde mi nacimiento se dedicó por entera a luchar y sacrificarse para que este donde estoy. Mi esposa por el amor, apoyo, comprensión sin importar el momento en que fuese y por soportar las largas horas robadas de su tiempo.

Esta tesis de grado está dedicada por entera a estas tres personas que han sido y son mi razón de vida.

Índice de contenido

Índice de imágenes

Introducción

Muchos aspectos de nuestras vidas dependen de Internet y las computadoras, incluidas las, transporte, finanzas, la medicina y educación (aulas virtuales, entrenamientos, elearnings).

Considere qué parte de su información personal o de la empresa se almacena ya sea en su propio ordenador o en algún otro sistema. ¿Cómo es que los datos y los sistemas en los que se transmite o que residen los datos mantienen segura? La seguridad informática consiste en la protección de la información y sistemas de los que dependemos todos los días, ya sea en el hogar o en el trabajo.

Esto, junto con la cada vez más poderosa tecnología y la interdependencia de los sistemas ha aumentado las amenazas y el impacto potencial de los ataques de manera exponencial.

El interés que se presenta es primero que todo concientizar la evolución de la seguridad de la información, la cual ya no es tener los documentos de la empresa en una caja fuerte resguarda. La seguridad de la información evoluciona y cambia dinámicamente con el pasar de las horas y las empresas deben estar constantemente actualizadas y poseer los medios de protección contra los ataques que cada día son más sofisticados. Con esta propuesta de adopción que en primer lugar debe ser la norma mínima de seguridad de la información y en segundo lugar ser obligatoria, AES Dominicana actuara proactivamente frente a la seguridad de la información.

Este documento en su estructura tiene en su **Capítulo I: Sistema Eléctrico Dominicana:** Presenta la historia de manera evolutiva desde el primer sistema de iluminación que utilizaban los tainos hasta la capacidad instalada, su generación y transmisión del sistema interconectado nacional de la Republica Dominicana.

Capítulo II: AES Corp y AES Dominicana. En este capítulo se describe la empresa objeto de estudio AES Dominicana en detalle con una referencia de su casa matriz AES Corp. **Capítulo III: Seguridad de la información.** Muestra desde el concepto de lo que es la seguridad de la información, pasando por los detalles conceptuales que envuelven hasta los mitos de lo que es y no es. **Capítulo IV: Propuesta de gestión de la seguridad de la información es AES Dominicana.** Este es el capítulo central del trabajo donde se realizan las recomendaciones de implementación detalladamente que la empresa AES Dominicana debe implementar en su infraestructura para preservar la integridad de este importante activo que es la información de la empresa. **Capítulo V: Análisis mundial de la seguridad de la información tecnológica.** Se presenta una perspectiva regional de la seguridad de informacion, la incidencias de ataques, reportes y como se esta actuando.

CAPITULO I

Sistema Eléctrico de la Republica Dominicana

1.1. Historia[1]

Para 1492, a la llegada de los españoles a Quisqueya, los aborígenes incuestionablemente conocieron la manifestación más elemental de la energía: El fuego. Las formas como ellos lograban producir fuego era por frotamiento, creando remanentes del fuego celestial, fuego.

El único sistema de iluminación de los aborígenes en taínos, caribes, macorixes, etc.; fue la tea hecha con trozos de madera resinosa como la de pino, popularmente llamada “cuaba”. La fogata fue el exclusivo sistema de calefacción de nuestras comunidades aborígenes.

En el año 1845, se instaló el Primer alumbrado público en Baní, ya que el tipo de alumbrado que existía era mediante el uso de faroles de vela de cera. El encendido de las calles cuya iluminación, como es dable suponer, era rústica, se iniciaba a la 6:00 PM., cuatro horas más tarde, es decir, a las 10:00 p. m. El mismo “Martín el farolero” procedía a apagarlos.

A partir del 1920, este sistema de alumbrado vial fue eliminado, dando paso a otro más moderno. En los albores Post-Independiente, en 1859, comenzó el alumbrado público de la capital aproximadamente 15 años después de la independencia, ya que para esta fecha Santo Domingo disponía con todas las deficiencias previsibles en aquel tiempo, de un sistema de alumbrado vial.

Para el año 1877, se implementa el sistema de alumbrado de iluminación por gas. En 1896, el alumbrado eléctrico en Santo Domingo entraba en un proceso de progreso con la implementación de un sistema de alumbrado eléctrico para las calles y hogares de la ciudad de Sto. Dgo.

[1] http://www.edenorte.com.do/nuestra-empresa/resena-del-sector-electrico-dominicano/

En 1912, específicamente para el 15 de agosto se inaugura un sistema de alumbrado eléctrico, considerado como muy moderno.

En 1913, mediante la resolución número 5223, se aprueba el contrato celebrado con el señor J.J. Moore, para establecer en la ciudad de La Vega una planta eléctrica. Con la resolución 5230 se aprobó el contrato con el referido Sr. Moore y el Sr. Arthur Lithgow, quienes prometían establecer el alumbrado en Moca, Santiago de los Caballeros y Puerto Plata.

El 2 de Mayo se enciende por primera vez la caldera de la planta eléctrica de Puerto Plata bautizada con el nombre “Ina”. El día 4 del mismo año llega el servicio energético a las instituciones públicas y privadas, y la empresa del Sr. Lithgow, la “Compañía Anónima Dominicana de Luz y Fuerza Motriz” es la responsable del acontecimiento.

En 1914, Se construye en la ciudad de Santiago de los 30 Caballeros otra compañía casi de nombre similar, con el fin de adquirir los sistemas de distribución eléctrica en las ciudades de Santiago y Puerto Plata, instalada por el Sr. J.J. Moore. En este mismo año se instalan en la Romana, un sin número de faroles.

Para 1915, el día 3 de febrero, el regidor Arturo Logroño propuso que se dediquen los días lunes y viernes para resolver todos los problemas relacionado a la luz. El 16 de Diciembre del mismo año, queda marcado el hito de la presencia de la energía eléctrica en la Hidalga ciudad de Santiago.

En 1916, Se instaló en puerto Plata “La primera planta eléctrica con una red transmisora de alta tensión para llevar energía a Santiago.

En 1919, el Ayuntamiento de Santo Domingo, resuelve celebrar un contrato con la persona o corporación, que ofrezca mejor condiciones para instalar por cuenta del Municipio y en la capital una Moderna Planta Eléctrica; asimismo se proyecta la instalación de una hidroeléctrica en el Salto de Jimenoa, en Jarabacoa Provincia de La Vega.

En 1920, el 23 de Abril, el señor Sabino Valdés llega al país con el objetivo de instalar una planta eléctrica en Santo Domingo que proporcione energía a la ciudad y a los barrios y ensanches adyacentes. [2]

Este contrato establecía que se debía pagar por Una bombilla de 10 vatios 0.75 centavos mensuales. 2 bombillas de 10 vatios 1.25 mensuales. Tres bombillas de 10 vatios 2.00 mensuales.

En 1921, se ilumina Salcedo desde la 6:00 a.m. de la tarde hasta la 11:00 p.m. Ricardo Durán, vende a Juan López la Cía por $5,000.00, luego la empresa Russo hermanos adquiere la Cía. e instala el alumbrado en la ciudad de La Vega. Luego la empresa pasa a mano de la Cía. Anónima de Agua, Luz y Fuerza Motriz, por un valor de 400,000 pesos donde 100,000 serían pagados por Puerto Plata.

En 1933, Se regulan las instalaciones eléctricas, y los exámenes que se deben recibir los electricistas, para poder ejercer su profesión. Se aprueba mediante la resolución 434 el contrato entre el ayuntamiento y la Común de Santa Bárbara de Samaná. Se instala en Azua de Compostela un generador de 15 Kw.

En 1950, se inaugura la Iluminación de la Avenida George Washington. En 1952, se inauguró la central Hidroeléctrica de Constanza, que daría luz a esa población, con una capacidad de 250 kilovatios.

En 1954, el Sistema Eléctrico Nacional para finales de este año se encontraba formado por tres principales fuentes generadoras de energía eléctrica:

- Plantas Térmicas.
- Plantas Hidroeléctricas.
- Plantas Diesel.

[2] Ibid.

Este Sistema tripolar estaba administrado por la Compañía Eléctrica de Santo Domingo (CESD). La principal fuente generadora de energía eléctrica de la CESD eran, subestación termoeléctrica en la calle La Marina, de la ciudad capital, la hidroeléctrica de Jimenoa, San Pedro de Macorís, Santiago y Puerto Plata, con un potencial instalado de 44,742 kilovatios y una demanda pico en el mes de octubre. [3]

Periodo comprendido entre los años 1955 – 1966

En 1955, el día 16 de enero el Estado Dominicano adquirió la Compañía Eléctrica de Santo Domingo, por un valor de 13,200.000.00. Mediante decreto N0.555, queda constituida la Corporación Dominicana de Electricidad, está empresa, ahora netamente nacional, asume la responsabilidad de mantener, ampliar, mejorar y generar todo el servicio energético en la República Dominicana.

En 1960, se le designa un capital de $12,000,000.00 a la Corporación Dominicana de Electricidad mediante el decreto 6231 se nombra administrador al Sr. José Cimadevilla Valdés.

En 1962, se instaura la autonomía de la Corporación Dominicana de Electricidad, se les paga retiros, pensiones, y pago en caso de muerte a los empleados de la C.D.E.

En 1963, se crea el Sindicato de trabajadores, el 28 de Febrero, -SITRACODE- en la C.D.E., siendo el secretario general el Sr. Juan Bautista Durán.

En 1965, se establece el primer pacto colectivo, de condiciones de trabajo, entre la C.D.E. y sus empleados, entre las cláusulas que se firman en este pacto, está el seguro de empleado, plan de retiro, pensiones y plan de vivienda.

[3] Ibid.

En 1966, se inaugura la unidad turbogenerador bautizado con el nombre de Puerto Plata I, con capacidad 27.6 Mw fue puesta en servicio el 17 de julio. [4]

Periodo comprendido entre los años 1967 – 1978

Para este período se incorporaron al Sistema Eléctrico Haina I con una capacidad de 54 megavatios, fue puesta en servicio el día 1 de diciembre del año 1968 por el Presidente Dr. Joaquín Balaguer y la Haina II también con una capacidad de 54 MW.

Se interconectaron Haina 3 y 4 en el año 1976, lo que significó una adición al sistema de 278 MW, es decir un 50% de la capacidad mínima requerida.

Periodo comprendido entre los años 1979 – 1993

Se incorporan al Sistema:

- Una Central termoeléctrica a carbón (Itabo I) de 125 MW para el año 1982, entrando en servicio en el 1984.
- López-Angostura, Central Hidroeléctrica de 18 MW para 1985, entró en servicio en el 1987.
- Los Toros, hidroeléctrica de 12 MW para 1985.
- Río Blanco, hidroeléctrico de 25 MW.
- Dos extensión de Itabo (Itabo II y III), térmica en carbón de 2×125 MW.
- Se inaugura el 27 de abril en Puerto Plata, la planta Wartsilla, con una capacidad para generar 20 mil kilovatios.

[4] Ibid.

En 1992, el 28 de Septiembre, se inician los trabajos de construcción de 34.8 kilómetros de líneas de alta tensión, esto forma el anillo, Los Prados – Embajador, Embajador – Matadero, Itabo – Los Prados, Haina – Matadero, Matadero – La UASD. [5]

En 1993, mediante el decreto Núm. 148 – 93, se crea el Consejo Nacional para la Energía. Se inician los contratos de trabajo con la empresa Smith and Enron. Transformador de Canabacoa entra en funcionamiento en fecha 13 de Septiembre, con una capacidad de 200 mil MVA.

Periodo comprendido entre los años 1994-2000

Durante éste periodo se realizaron los siguientes aportes al Sistema Eléctrico Nacional: Se incorporó al Sistema la Unidad de Puerto Plata II, con 36 megavatios de potencia firme. Esta unidad estaba fuera de servicio desde el año 1992, siendo necesario el reemplazo del turbogenerador de vapor. Se rehabilitó con recursos propio el Parque de Haina, donde la mayoría de sus unidades se encontraban fuera de servicio.

Se firmaron los contratos con la firma Alemania SIEMENS AG para el suministro de una turbina VO84-2 con una potencia garantizada de 99.7 Mw. El monto contrato de instalación ascendió a US$34.0 millones, siendo éste financiamiento garantizado por un pool de bancos nacionales. Se adquirieron 5 unidades de turbogás de 34 megavatios cada una, que aportaron al sistema un total de 170.0 Mw, el monto de este contrato ascendió a US$ 71.0 millones y fue firmado con la empresa ALSTEOM G.A.

[5] Ibid.

Se realizó un acuerdo con el gobierno español para el financiamiento de dos plantas térmicas a Vapor; El año 1999 marca un cambio trascendental en el Sector Eléctrico Nacional, con la materialización de la ejecución de las disposiciones del Decreto No. 428-98, emitido por el poder ejecutivo en fecha 25 de noviembre de 1998, que modifica el Reglamento No. 1034, de fecha 26 de julio de 1955, mediante el cual se divide la Corporación Dominicana de Electricidad en 7 unidades de Negocios y una Unidad Corporativa que operarían como empresas independientes, facilitando así el proceso de capitalización de la CDE.

En el área de Comercialización y Distribución de la CDE, resultaron ganadores la Distribuidora del Este, AES Corporation y la Distribuidora del Norte y Sur, la Empresa UNIÓN FENOSA. [6]

La licitación del área de Generación se realizó el 13 de mayo, con la participación de tres empresas, resultando ganador de la Generadora Itabo y Haina, el consorcio New Caribbean Investment.

Durante la etapa de transición, la CDE actuó como organismo de soporte del Sistema Eléctrico Nacional y continúa administrando el Sistema de Transmisión de Electricidad y la Generación Hidroeléctrica, desde la Unidad Corporativa.

Periodo a partir del 2001[7]

Desagregación y privatización del sector

El gobierno, con el objetivo de resolver los continuos problemas de falta de capacidad instalada y de apagones constantes, promulgó la Ley General de Reforma de la Empresa Pública, la cual proporcionó el marco para la privatización y reestructuración del sector energético.

[6] Ibid.

[7] http://es.wikipedia.org/wiki/Sector_el%C3%A9ctrico_en_la_Rep%C3%BAblica_Dominicana

En el período 1998-1999, bajo el primer gobierno de Leonel Fernández, el sector se desagregó y el monopolio público verticalmente integrado de la *Corporación Dominicana de Electricidad* (CDE) fue disuelto en una serie de compañías de generación. Empresa Generadora de Electricidad Haina (EGE Haina) y EGE Itabo, que operaban las plantas térmicas, fueron privatizadas; también se crearon y privatizaron tres compañías de distribución: EdeNorte (Empresa Distribuidora de Electricidad), EdeSur y EdeEste.

Ley de Electricidad de 2001[8]

No se promulgó un marco regulador integral hasta julio de 2001, cuando se aprobó la Ley de Electricidad (ley nº 125-01) bajo el gobierno de Hipólito Mejía. Bajo esta ley, la presencia operativa del gobierno en el sector se haría a través de tres entidades:

- La corporación de servicios públicos antiguamente integrada CDE, que mantuvo los contratos con los productores de energía independientes (IPP).
- Una empresa de transmisión, Empresa de Transmisión Eléctrica Dominicana (ETED)
- Una empresa de generación hidroeléctrica, *Empresa de Generación Hidroeléctrica Dominicana* (EGEHID).

Se estableció un nuevo conglomerado de empresas, la *Corporación Dominicana de Empresas Eléctricas* (CDEE), para que asumiera la propiedad de ETED y EGEHID, y para que finalmente sustituyera a la CDE. Inicialmente, el gobierno pensó en transferir sus activos para administrar las empresas como una inversión bajo un fondo en fideicomiso independiente de las entidades reguladoras del sector, en lugar de usar su titularidad como instrumento potencial para las políticas del sector. Sin embargo, este cambio no se realizó.

[8] Ibid.

La Ley de 2001 y sus normas complementarias de 2002 incluyeron la creación de una agencia reguladora autónoma, la Superintendencia de Electricidad (SIE). También se creó la Comisión Nacional de Energía (CNE) y un mercado mayorista bajo la responsabilidad de un Organismo Coordinador.

La crisis y renacionalización de las compañías de distribución[9]

La reforma favoreció la instalación de nuevas plantas generadoras, construidas y financiadas por el sector privado, y la inversión en distribución a cargo de las empresas privatizadas. Gracias a las nuevas inversiones, entre fines de 2000 y mediados de 2003, la capacidad efectiva experimentó un aumento del 43%; también se registraron mejoras en la red de distribución.

Esto condujo a la reducción provisional de los apagones y las pérdidas en distribución, y a un incremento en la eficacia operativa; una combinación que se tradujo en mejoras en la calidad del servicio. El suministro de energía no atendido disminuyó al 11% de la demanda potencial en 2002, por debajo del 40% de 1991. En el mismo período, se estima que el déficit de capacidad para afrontar abiertamente la demanda cayó del 30% al 16%. Sin embargo, el aumento en el precio del petróleo, la aparición de subsidios generalizados y las interferencias políticas afectaron negativamente a la salud financiera del sector.

En 2003, estas condiciones desfavorables y una fuerte presión política llevaron al gobierno a volver a adquirir las acciones de Unión Fenosa en las empresas de distribución privatizadas EdeNorte y EdeSur. Desde su renacionalización, estas empresas han experimentado un deterioro en su eficacia operativa.

El sector eléctrico ha permanecido en una crisis sostenida desde 2002, caracterizada por pérdidas muy elevadas (tanto técnicas como comerciales) y apagones frecuentes de larga duración.

[9] Ibid.

Esta situación derivó en costos económicos y sociales muy elevados: costos fiscales elevados para el gobierno, altos costos de producción e incertidumbre para los consumidores industriales como resultado de las interrupciones en el servicio, altos costos para los consumidores industriales y residenciales por la generación pública y privada de energía, y creciente inestabilidad social, incluyendo el incremento en la tasa de delitos como consecuencia de los frecuentes apagones y los cortes en los servicios públicos básicos (por ejemplo, hospitales, clínicas y escuelas). Además, se desalentó la inversión doméstica e internacional, especialmente en sectores que dependen de un suministro confiable para sus actividades, aunque muchas instalaciones (como los complejos turísticos) cuentan con fuentes de energía propias.

1.2 Generación[10]

El 86% de la capacidad de generación se encuentra en manos privadas (excluyendo la autogeneración) y el 14% es de propiedad pública.

[10] Ibid

La capacidad de generación está compartida por diferentes empresas de la siguiente manera:

Empresa	Capacidad de generación (MW)	Participación (%)	Áreas geográficas (Norte, Sur, Este)
Haina (privada)	663,3	19,5%	N, S, E
Itabo (privada)	630,5	18,6%	N, S, E
Hidroelectricidad (pública)	469,3	13,8%	N, S
Productores de energía independientes (IPP) (privada)	515	15,2%	N, S, E
Unión FenosaUnión Fenosa (privada)	194,5	5,7%	N
CEPP (privada)	76,8	2,3%	N
Trans Capital Corporation (privada)	116,3	3,4%	S
Monte Río (privada)	100	2,9%	S
AES (privada)	555	16,4%	E
Metaldom (privada)	42	1,2%	S
Laesa (privada)	31,4	0,9%	N
TOTAL	**3.394,1**		

Fuente: Estadísticas de la Superintendencia de Electricidad. El 86% de la capacidad de generación se encuentra en manos privadas. Cuadro 1.1

1.3 Transmisión[11]

El sistema de transmisión, que se encuentra bajo total responsabilidad de la compañía pública ETED (Empresa de Transmisión Eléctrica Dominicana), consta de 940 km de líneas de circuito simple de 138 kV que parten radialmente desde Santo Domingo hacia el norte, el este y el oeste.

1.4 Distribución[12]

En la República Dominicana hay tres empresas de distribución. El gobierno es propietario de las tres, EdeNorte, EdeEste y EdeSur, a través de la CDEEE (50%) y del *Fondo Patrimonial de las Empresas* (FONPER).

1.5 Evolución de la Generación año 2012 – 2013

A continuación se muestra el cuadro comparativo de la evolución de la generación bruta obtenida desde el reporte final año 2013 del SENI mes a mes.

Evolución mensual de la generación 2012-2013 Evolución De La Generación En GWh

MES	2012	2013	EVOLUCION EN %
ENERO	980.67	1102.00	12.37%
FEBRERO	948.00	1015.93	7.17%
MARZO	1019.83	1138.14	11.60%
ABRIL	1030.54	1142.70	10.88%
MAYO	1181.68	1229.37	4.04%
JUNIO	1170.32	1192.97	1.94%
JULIO	1214.21	1239.68	2.10%
AGOSTO	1179.98	1273.85	7.95%
SEPTIEMBRE	1176.19	1203.55	2.33%
OCTUBRE	1198.04	1255.55	4.80%
NOVIEMBRE	1137.03	1154.56	1.54%
DICIEMBRE	1119.25	1145.07	2.31%
Total GWh	13355.76	14093.36	5.52%

Fuente: Estadísticas de la Superintendencia de Electricidad. Informe de operación real periodo 2013. Cuadro 1.2

[11] Ibid

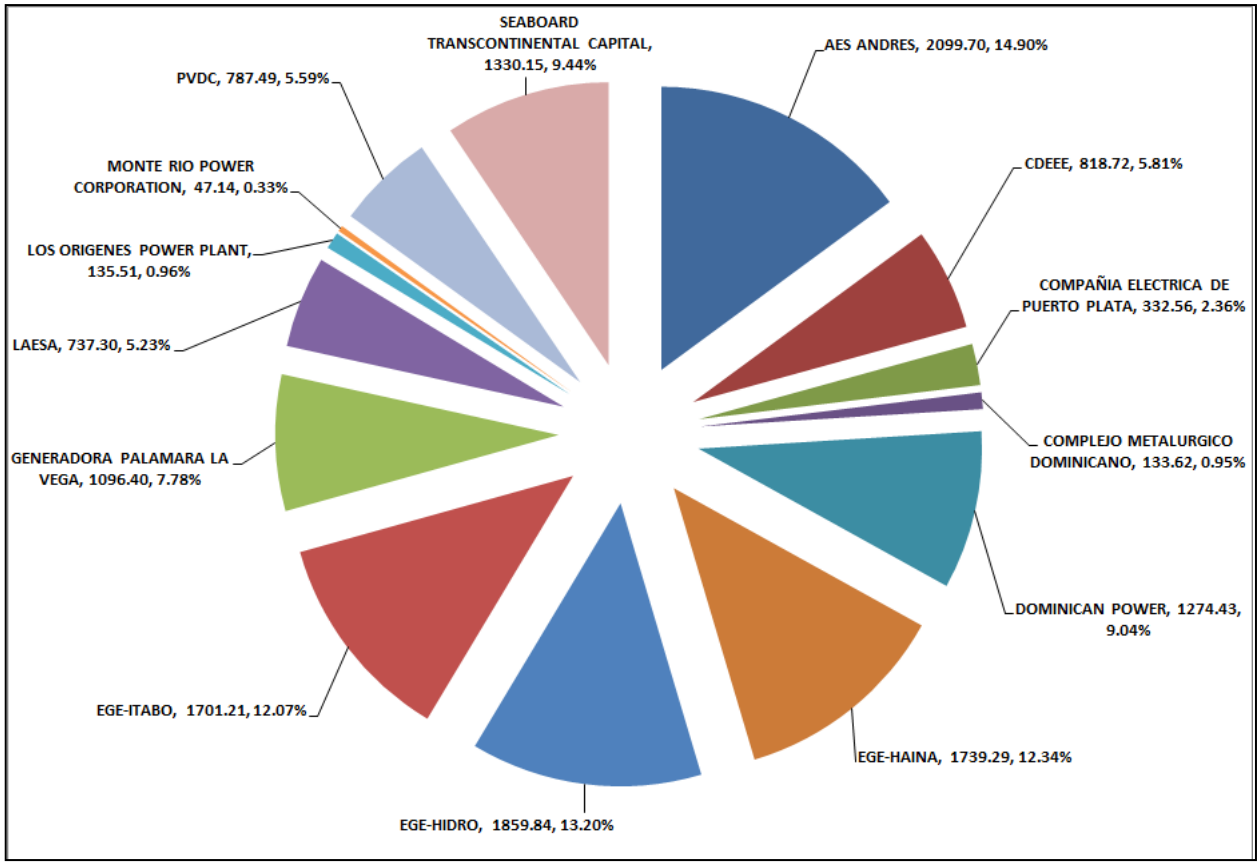
[12] ibid

- La energía total entregada en el año 2013 aumentó en un 5.52% equivalente a 737.6 GWh en relación al año 2012, es importante señalar, que como nueva generación se interconectaron al SENI, las siguientes centrales:

- El 08 de septiembre del 2013 las centrales de Quisqueya 1 y Quisqueya 2, con 215 MW cada una entraron al SENI en calidad de prueba.

- El 21 de septiembre del 2013, la central Los Orígenes de 25 MW, fue declarada comercialmente.

Porcentaje de Energía Generada por Empresa en GWh año 2013

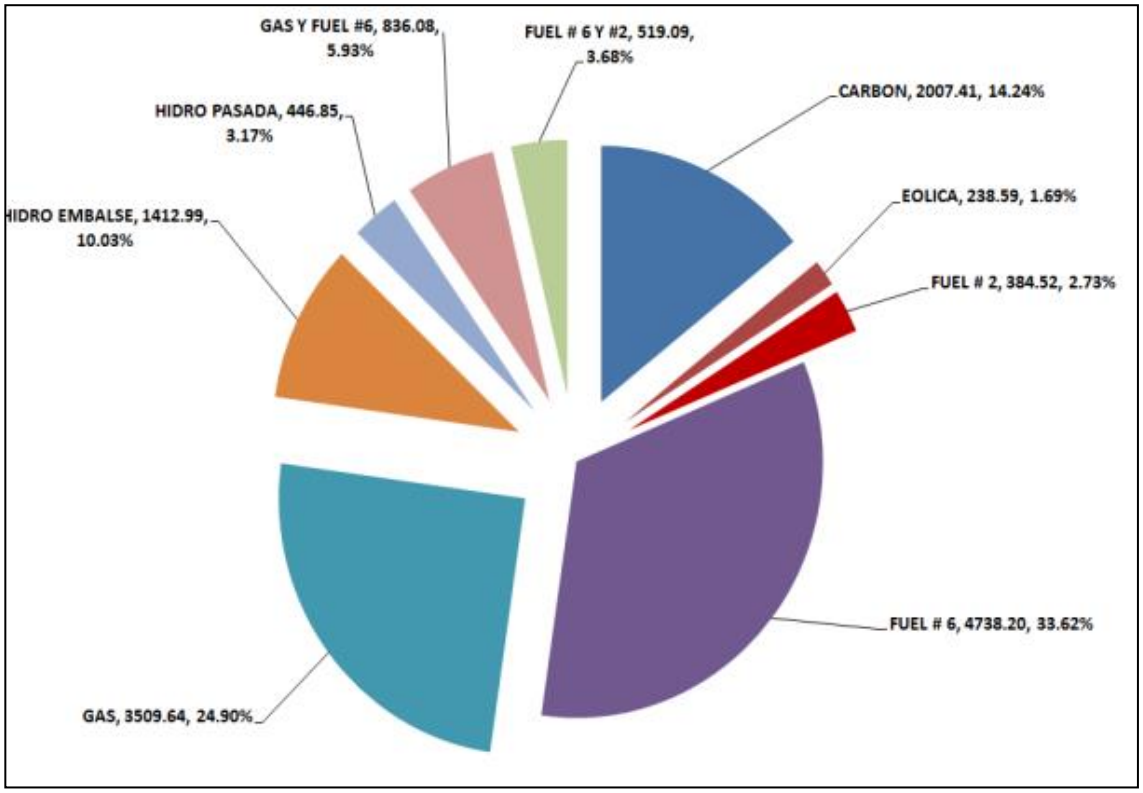


Fuente: Estadísticas de la Superintendencia de Electricidad. Informe de operación real periodo 2013.

Grafica 1.1

Para el año 2013, la empresa con mayor aportación al SENI fue AES-Andrés con un 14.90%, equivalente a 2099.70 GWh, seguido luego por EGE-HIDROELECTRICA con un 13.20%, equivalente a 1739.29 GWh y EGE-HAINA con un 12.34% correspondientes a 1739.29 GWh.

Porcentaje de Energía Generada por tipo de combustible año 2013 en GWh



Fuente: Estadísticas de la Superintendencia de Electricidad. Informe de operación real periodo 2013.

Grafica 1.2

Los combustibles más usados en el año 2013 para la generación fue el fuel oíl #6, en un 33.62%, seguido por el gas natural con un 24.90%.

CAPITULO II

2.1 AES Corp[13]

AES Corp es una compañía de energía internacional con las empresas de generación y distribución en los cinco continentes. Desde su fundación en 1981, AES ha impulsado el crecimiento del sector de la energía, pionero en los avances en muchos mercados y hoy se erige como un líder global de la industria de la energía en la innovación y la excelencia operativa.

En 1985, bajo la dirección de Roger Sant como director general, la primera planta de energía AES fue construido en Texas. Rápidamente se convirtió en una de las plantas de energía competitivas principales en los Estados Unidos. En 1988, AES se convirtió en el mayor productor independiente de energía (IPP) en los EE.UU., con tres plantas en operación (Placerita, Beaver Valley y de aguas profundas). Esta expansión interna impulsó una búsqueda mundial de un nuevo financiamiento, la construcción y las oportunidades operacionales.

Dado que los mercados internacionales se abrieron, AES comenzó a generar electricidad en el Reino Unido y, a continuación, se expandió a Argentina, Pakistán, China, Hungría y Brasil. En 1998, con Dennis Bakke como CEO, AES se convirtió en un innovador temprana mediante la adquisición de una participación minoritaria en una planta de energía en la privatización de la primera generación sólo en la India. En África occidental y América Central, AES trajo electricidad a lugares que nunca habían tenido previamente una potencia fiable, mientras que al mismo tiempo, servir a los centros urbanos como São Paulo y Indianápolis, IN.

[13] http://www.aes.com/Aboutus/History

Bajo el liderazgo de Paul Hanrahan como CEO, AES ayudó a desarrollar nuevas tecnologías de control de la contaminación y conversiones - en biomasa Qatar, Omán, Sri Lanka, Camerún y Bulgaria, donde construimos proyectos de nueva creación más grande hasta la fecha.

También hemos traído las fuentes renovables de energía al mercado a través de la adquisición y desarrollo de AES Generación Eólica en los EE.UU. y Europa, a través de AES Solar Energy , LLC, empresa conjunta con Riverstone Holdings.

Hoy, con Andrés Gluski a la cabeza, y con un nuevo equipo de liderazgo ejecutivo y la estructura organizativa refinada en su lugar, AES está comprometida a mejorar la vida a través de los servicios esenciales que prestamos. En algunas regiones, el poder puede conducir supercomputadoras y las tecnologías industriales de vanguardia, en otros podemos estar entregando la primera electricidad confiable a hospitales, hogares, escuelas y empresas. Independientemente de la configuración regional, creemos que la electricidad es esencial para el progreso humano y la promoción del crecimiento económico, la salud pública y la seguridad.

2.2 AES Dominicana[14]

AES inicia operaciones en República Dominicana en 1997 con la firme convicción de aportar valor al mercado energético nacional y contribuir con el desarrollo de las comunidades a las cuales sirve. Hoy, AES Dominicana se posiciona como el principal grupo inversor con modernas facilidades de energía, con tecnología de última generación y con la canasta de combustibles más competitivos en precios de los que se utilizan para la generación de electricidad en el mercado nacional.

[14] http://aesdominicana.com.do/app/do_2011/corp_rd.aspx

AES Dominicana es el único grupo con presencia local que cuenta con dos infraestructuras portuarias de gran calado. La terminal de Gas Natural Líquido, ubicada en el parque energético de AES Andrés, es la entrada exclusiva de gas natural al país; mientras que el Puerto Internacional Itabo, es el único puerto de recepción de carbón y otros tipos de granos. [15]

Las inversiones de AES Dominicana superan los 800 millones de dólares e impactan directamente en la vida de más de 300 trabajadores. Este Grupo constituye uno de los principales soportes para el Sistema Eléctrico Nacional Interconectado (SENI) al aportar alrededor del 40% de la energía que se demanda en el país.

Como grupo empresarial, combina una perspectiva global con conocimientos locales profundos y un incansable compromiso con la excelencia operativa para ayudar a que las comunidades crezcan a través de un suministro de energía eléctrica seguro y confiable.

Una muestra de ello es que año tras año los negocios de AES vienen superando sus propios records históricos de disponibilidad, generación y eficiencia. Además de dar muestras fehacientes de transparencia al emplear las mejores prácticas de gobierno corporativo dentro de la industria eléctrica dominicana.

AES Dominicana sustenta el crecimiento de la empresa en pilares como la Responsabilidad Social Corporativa, el cuido del Medio Ambiente y en su Gente, lo que considera el principal activo. Asimismo, trabajan apegados a los principios globales de ser una empresa socialmente responsable a través de la Fundación AES Dominicana donde se abordan las áreas en más precarias condiciones como son la educación y la salud infantil.

[15] http://aesdominicana.com.do/app/do_2011/corp_rd.aspx

2.3 Portafolio de Negocios[16]

AES Dominicana cuenta con varias unidades de negocio de generación eléctrica ubicadas en diferentes puntos de la República Dominicana:

AES Andrés, ubicada en Andrés Boca Chica, cuenta con la única terminal de gasificación de gas natural en el Caribe. Actualmente es la entrada de todo el gas naturas que se importa al país y que sirve de soporte a varios sectores nacionales. **AES DPP**, ubicada en la avenida Venezuela, cuenta con dos turbinas de ciclo abierto de 118MW cada una.

AES ITABO, ubicada en la localidad de Bajos de Haina, cuenta con dos unidades cuyo combustible es el carbón mineral.

2.4 Filosofía Corporativa AES[17]

Misión

Atender las necesidades de energía en forma limpia, segura, confiable y socialmente responsable.

Valores

- La Gente AES:

- Pone la seguridad primero.

- Actúa con integridad.

- Cumple sus compromisos.

- Se esfuerza por la excelencia.

- Disfruta su trabajo.

[16] http://aesdominicana.com.do/app/do_2011/neg_andres.aspx

[17] http://aesdominicana.com.do/app/do_2011/corp_filosofia.aspx

¿Qué Significan?[18]

Poner la seguridad primero

La seguridad siempre está primero, para su gente, los contratistas y las comunidades. Así podrán asegurar que las todo el personal llegará sano y salvo a sus hogares.

Actuar con integridad

Son honestos, dignos de confianza y responsables. La Integridad es la esencia en todo lo que hacemos, cómo nos conducimos y cómo nos relacionamos los unos con los otros.

Cumplir compromisos

Honran sus compromisos con los clientes, compañeros, comunidades, accionistas, proveedores y socios, y queremos que el negocio, en general, suponga una contribución positiva a la sociedad.

Esforzarse por la excelencia

Se esfuerzan para ser los mejores en todo lo que hacemos y para operar con niveles de clase mundial.

Disfrutar el trabajo[19]

El trabajo puede ser divertido, gratificante y emocionante. Disfrutamos del trabajo y apreciamos la satisfacción de ser parte de un equipo que está marcando una diferencia. Y cuando deje de ser de esa manera, cambiaremos lo que hacemos o cómo hacemos las cosas.

---

[18] Ibid.

[19] Ibid.

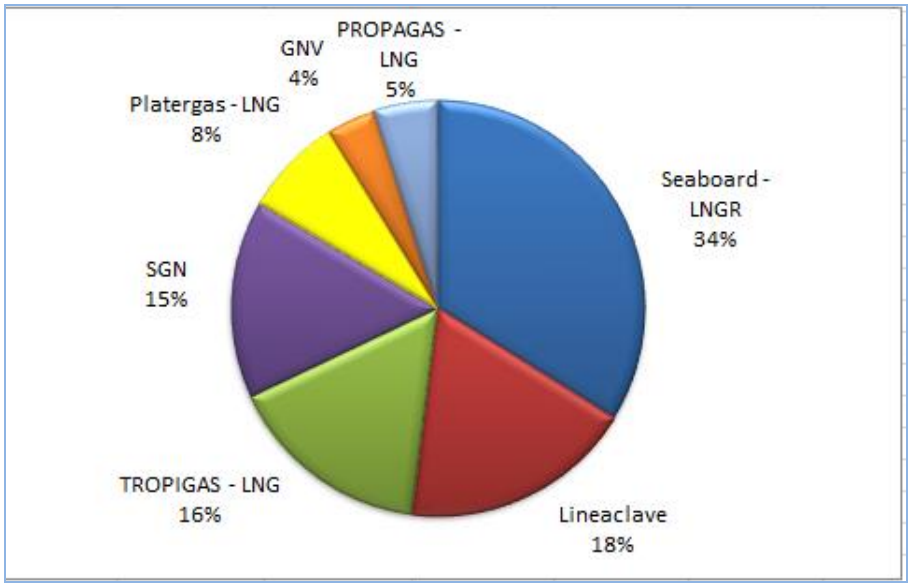
2.5 AES como sistema organizacional híbrido[20]

La terminal de Gas Natural de AES Dominicana obtiene su insumo en el mercado internacional amparado por un contrato a largo plazo con la empresa British Petroleum (BP) en el cual se establece la recepción de 11 buques de Gas Natural por año en estado sólido. Este gas natural es descomprimido y transformado a estado líquido para su consumo en los diferentes ámbitos del negocio de generación y sectores nacionales (empresarial e industrial). Esta terminal vende gas natural a otra unidad de negocios de AES llamada Dominican Power Partner aprovechando la ventaja competitiva de precios a los cuales lo compra AES Andrés. El transporte de este gas hacia DPP se hace a través de un gasoducto de 34KM de largo que desemboca directamente en las instalaciones de la avenida Venezuela. Dicha terminal igualmente suple de este combustible a varios sectores del país aportando más de un 25% de su importación. El transporte del gas natural a los clientes externos se hace a través de camiones especiales que son llenados en una terminal adjunta a las instalaciones de AES Andrés. De acuerdo a la política de Comercialización de Gas Natural se establece que para firmar contrato de suministro directamente con Aes Dominicana la cantidad mínima a contratar son 500,000 MMBtu (0.5 TBtu), y solo grandes generadoras tendrían por si solas una demanda tan alta. Los consumidores directos consolidan las demandas de todos sus clientes para poder llegar a esa nominación mínima. Actualmente los clientes directos de la terminal son: *PROPAGAS –LNG; Seaboard – LNGR; Línea Clave; TROPIGAS – LNG; SGN; PLATERGAS – LNG; GNV*[21]

[20] Infome estadistico AES Dominicana 2013. p.16

[21] Ibid.

El porcentaje de distribución se muestra en el siguiente gráfico:



Fuente: Reporte anual. Aes Dominicana 2013

Grafica 2.1

Estos a su vez tienen clientes que demandan de este producto y constituyen los clientes indirectos de AES Dominicana entre los cuales destacan: BRUGAL, Fritolay Dominicana, MERCASID, Hoteles Catalonia Bávaro, Leche RICA, La Famosa, Hoteles Barceló, AMBEV, Nestlé, METALDOM, CEPM, Puerto Plata de Electricidad, PLASTIFAR, entre otras empresas.

2.6 Ámbito de Negocio[22]

AES Dominicana tiene como contorno operativo al sector eléctrico dominicano aportando el 40% de la energía que se demanda en el país, se establece como el mayor suplidor en este sector con una gran ventaja competitiva respecto a sus más inmediatos rivales, esto debido mayormente a que generan electricidad con combustibles económicos y amigables al medioambiente como lo son el **gas natural**, utilizado por las unidades generadoras AES Andrés y AES DPP y el **Carbón Mineral**, utilizado por la generadora de electricidad AES ITABO.

[22] Ibid.

A su vez AES Dominicana es la pionera en el mercado de venta de gas natural en el país, aportando un 25% anual del total de importación de este combustible que es destinado al sector empresarial e industrial, así como también al sector transporte.

Esto último fue decretado por el gobierno dominicano como prioridad nacional para establecer en el mercado combustibles más limpios y mucho más económicos y bajar gradualmente la dependencia del crudo de petróleo que se importa desde varias regiones del mundo.

2.7 Mercado de Contratos[23]

Las partes involucradas acuerdan la compra-venta de energía y capacidad por cantidades, precios y términos específicos. Los contratos entre generadoras y distribuidoras tienen la forma de un acuerdo de compra-venta de energía, donde las generadoras venden cantidades de capacidad y energía en el punto de consumo de la distribuidora, independientemente de donde sea generada; sin embargo los acuerdos de venta de energía no involucran al comprador en el despacho económico del vendedor.

Mercado Spot[24]

Funciona en base a las transacciones de energía a medida que ocurren como la diferencia entre la energía total despachada por los generadores en el despacho económico y la energía realmente demandada de acuerdo a los contratos. Igualmente el mercado spot también está compuesto por las transacciones de potencia firme determinada por el Organismo Coordinador.

El- precio spot es calculado cada hora en base al Costo Marginal de Corto Plazo, el cual es definido por el costo variable de producción de la última unidad de generación que fue despachada para atender 1 kWh adicional.

---

[23] Ibid. p. 17

[24] Ibid. p. 18

Si el sistema está en racionamiento, el costo marginal es fijado por la Superintendencia como el costo de la energía no servida.

A continuación se enumeran los agentes que conforman el Mercado Eléctrico Mayorista:

Empresas de Generación[25]

- AES Andrés B.V.
- Dominican Power Partners, Ldc
- Energycorp Caribbean, S.A. - IPP
- Falconbridge Dominicana
- Empresa Generadora de Electricidad de Haina, S.A.
- Empresa de Generación Hidroeléctrica Dominicana
- Empresa Generadora de Electricidad Itabo, S.A.
- Consorcio Laesa, Ltd. –IPP
- Compañía Eléctrica de Puerto Plata, S.A.
- Maxon Engineering Services, S.A. - IPP
- Complejo Metalúrgico Dominicano, C. por A.- IPP
- Monte Rio Power Corporation C. por A.
- Compañía Eléctrica de San Pedro de Macorís - IPP
- Transcontinental Capital Corporation, Ltd
- Smith Enron Cogeneration Limited Partnership - IPP

[25] Ibid. p.19.

Nota: IPP´s (productores privados independientes) realizan las transacciones a través de la Corporación Dominicana de Empresas Eléctricas Estatales (CDEEE).

Empresas de Transmisión y distribución[26]

- Empresa de Transmisión Eléctrica Dominicana
- Empresa Distribuidora de Electricidad del Norte, S.A.
- Empresa Distribuidora de Electricidad del Sur, S.A.
- Empresa Distribuidora de Electricidad del Este, S.A.

Mercado Venta Gas Natural[27]

En el caso de comercialización de Gas Natural se realizan contratos de venta de combustibles a clientes directos llamados distribuidores, estos son los que suplen todos los renglones: gas vehicular (utilizando el gas natural licuado (GNL) y el comprimido (GNC), hoteles, empresas generadoras relativamente pequeñas y empresas de zona franca. Esto es debido a su política de Comercialización de Gas Natural que establece que para firmar contrato de suministro directamente con AES Dominicana la cantidad mínima a contratar son 500,000 MMBtu (0.5 TBtu), y solo grandes generadoras tendrían por si solas una demanda tan alta. Las distribuidoras consolidan las demandas de todos sus clientes para poder llegar a esa nominación mínima.

2.8 Estructura Organizativa

AES Dominicana está compuesta por una estructura organizativa vertical, integrada por una cúpula de liderazgo encabezada por el presidente, 5 vicepresidentes. Debajo de este renglón encontramos a 9 superintendentes, gerentes, coordinadores, líderes y el área operativa.

[26] Ibid. p. 19

[27] Ibid. p. 20

Cada uno de estas agrupaciones pertenece a un conjunto interno de comités (consultivo y estrategia) y realizan reuniones denominadas de STAFF en la que se puntualizan los aspectos más relevantes a tratar de la estrategia y la operativa del negocio. Los niveles de aprobaciones para adquisiciones y compras también están definidos por estas nomenclaturas.

Todos sus procedimientos, normativas, políticas y regulaciones internas están certificados por las normas ISO 9001:2008 sobre calidad y la 14001:2004 sobre medio ambiente, lo que obliga a mantener un estándar de documentación para mantener el concepto de mejora continua sobre sus procesos. La estructura informal de la empresa no es visible, pero se observa un alto grado de apertura de la estructura de liderazgo hacia los mandos medios y bajos. Todos los requerimientos deben ir acompañados de la documentación de la estructura de mando de la cual procede.

2.9 Análisis FODA – Fortaleza, Oportunidades, Debilidades y Amenazas

Fortalezas

1. Solidez económica y financiera
2. Capital humano calificado y competente
3. Certificaciones internacionales de calidad ISO 9001, medioambiente y seguridad ISO 14000 y salud ocupacional OSHAS 18001
4. Buena percepción del servicio por parte del cliente
5. Políticas de responsabilidad social en constante maduración y mejora

Oportunidades

1. Existe disponibilidad de recursos en la Región
2. Crecimiento de la Demanda de Energía
3. Facilidades de acceso a fuentes de financiamiento
4. Posibilidades de establecer alianzas estratégicas en inversiones
5. Diversificación del negocio aplicando nuevas tecnologías

Debilidades

1. Disponibilidad en el mercado de personal especializado y técnico
2. Herramientas de gestión organizacional desactualizadas
3. Desaprovechamiento de herramientas de gestión de tecnología de información, investigación y desarrollo.
4. Falta de información sobre proyectos de alto impacto
5. Comunicación efectiva a nivel organizacional es insuficiente

Amenazas

1. Volatilidad de los costos de los combustibles
2. Frecuentes cambios del marco regulatorio
3. Incertidumbre de la política socio económica
4. Efectos del cambio climático y calentamiento global
5. Perder las concesiones para el desarrollo de proyectos de inversión

2.10 Objetivos AES Dominicana[28]

Objetivos Estratégicos y Operativas

Perspectiva de la Rentabilidad Social

Implementar un modelo empresarial sostenible y socialmente responsable

Metas Operativas:

- *Elaborar y ejecutar un plan de optimización de recursos*

- *Elaborar e implementar programas de eficiencia energética*

- *Implementar programas de responsabilidad social*

- *Identificar, formular y ejecutar proyectos de energías limpias, socialmente rentables*

[28] Templo estrategico 2013

- *Gestionar disponibilidad de recursos*

Perspectiva de la Sociedad

Consolidar a AES Dominicana como una empresa pública reconocida por sus estándares de calidad en la atención al cliente.

Metas Operativas:

- *Mejorar la gestión comercial de la Organización*

- *Mejorar la calidad técnica del servicio eléctrico*

- *Integrar la gestión de la CENTROSUR con los organismos regionales*

Perspectiva de los Procesos

Mejorar continuamente los procesos para garantizar la calidad y cobertura de la prestación del servicio eléctrico.

Metas Operativas:

- *Mejorar los procesos organizacionales*

- *Integrar los sistemas de gestión*

- *Ejecutar planes de expansión sostenibles*

Perspectiva del aprendizaje y desarrollo

Potenciar el desarrollo del Talento Humano y la gestión tecnológica

Metas Operativas:

- *Implementar planes y programas estratégicos de comunicación, formación, capacitación y motivación.*

- *Mejorar el clima laboral.*

- *Aplicar modelos de sistemas de gestión tecnológica estandarizados.*

Metas Individuales

Departamento de Recursos Humanos

- Captar talentos con alto nivel de eficiencia y productividad para las nuevas áreas que implementará este año AES Dominicana.
- Capacitar y entrenar a cada empleado de forma continua para mantener una alta productividad del personal.
- Evaluar de forma objetiva el desempeño laboral de cada departamento para detectar posibles debilidades.
- Orientar constantemente el personal sobre su función y lo importante que es para la empresa.

Departamento de Tecnología de Información

1. Dotar de la tecnología adecuada y más reciente cada una de las terminales para lograr más eficiente el manejo de Energía servida.
2. Actualizar el sistema de informática que controla las plantas durante los próximos 3 meses.

Departamento de Negocios Comerciales

1. Mejora de la gestión comercial y el flujo de caja en un 100% los próximos 6 meses.
2. Incrementar las utilidades de la empresa en un 35% durante los próximos 6 meses.
3. Aumentar la cartera de clientes en un 20% en el próximo trimestre.

Metas financieras

1. Reducir en un 50% la cantidad de préstamos durante el próximo semestre.
2. Actualizar el sistema contable en el próximo trimestre.
3. Recuperar 60% del efectivo que nos adeuda el estado, antes del cambio de gobierno.

2.11 Diseño Organizativo Estratégico[29]

AES Dominicana es una empresa con un modelo Organizativo estratégico funcional, sus oficinas administrativas mantienen concentrados las unidades de Negocios Comercial, Legal, Tecnología, Servicios Generales, Compras, Recursos Humanos, Impuestos, facturación, servicio al cliente, Mensajería. Las unidades de negocio de las plantas mantienen concentradas las áreas de operaciones, mantenimiento, subestaciones, terminal de gas natural, puerto de carbón, cancha de carbón, eléctricos, mecánicos, calderas, bomba de succión, enfriamiento, laboratorio químico, laboratorio carbón, planta desalinizadora y ciclo combinado.

Todos los departamentos mantienen agrupados funcionalmente a los colaboradores según su nivel de especialización.

2.12 Desafíos de la empresa

AES Dominicana como toda empresa a nivel nacional enfrenta desafíos establecidos en el entorno al cual pertenece, algunos de estos se remontan a la época misma de la creación del sistema eléctrico nacional, otros, son el resultado de la incursión de nuevos grupos de inversionistas, la sociedad, el entorno mismo y los niveles culturales de los sectores involucrados. Los que presentan más relevancia para la estructura organizativa actual son:

- Operar en un mercado que en sus inicios no contaba con una normativa.
- Establecer una estructura tarifaría técnica que reconozca los costos de generación, transmisión, distribución y comercialización de los combustibles que se utilizan como negocio en AES Dominicana.
- Implementar una Norma Técnica de Calidad de Servicio y Calidad de Producto.

[29] Informe estadístico AES Dominicana 2013. p. 8.

- Realizar el Estudio para el establecimiento de las normas de acceso, remuneración, peaje y expansión del sistema de transmisión. (Valor Agregado de Transmisión).

- Contratación y capacitación de personal técnico calificado para conseguir el nivel de eficiencia óptimo que demanda la Regulación de Mercados Eléctricos en ambiente competitivo.

- Estudio para el establecimiento de las normas de operación del mercado mayorista.

- Instalación de Oficinas de Protección al Consumidor en las principales provincias y/o municipios del país.

Existen diversas estrategias con las cuales se pretende paliar la situación de muchos de estos desafíos, la más importante de ellas es la captación de grupos de inversionistas locales que se comprometan a contribuir con la expansión y desarrollo de nuevas soluciones de entrega de energía y cierre de oportunidades de negocios para elevar la capacidad de producción local de energía. Otro aspecto que tienen en cuenta es la estrategia de restructuración de normativas de capacitación local de personal y mejoramiento de las relaciones con el gobierno y sus relacionados. Los usuarios no regulados también son un foco estratégico importante por ser estos los que mantienen flujo de caja constante.

2.13 Cultura Organizacional

Además de su compromiso en lo que se refiere a la seguridad y la calidad, así como su respeto por la diversidad, AES Dominicana está comprometida con una serie de valores culturales. Dichos valores vienen en parte de sus raíces y han ido desarrollándose a lo largo de su historia. Están igualmente en constante evolución para garantizar la reorganización de la Compañía.

Dichos valores pueden describirse como sigue:

- Compromiso con una fuerte ética en el trabajo, la integración, la honestidad y la calidad.

- Relaciones personales basadas en la confianza y el respeto mutuo, lo que implica una actitud sociable hacia los demás, junto con la habilidad de comunicar abierta y sinceramente.

- Una manera personalizada y directa de relacionarse entre sí, lo que implica un alto nivel de tolerancia frente a las ideas y opiniones de los demás, así como un fuerte compromiso para la cooperación activa con ellos.

- Un enfoque más pragmático de los negocios, lo que supone ser realista y basar las decisiones en hechos.

- Apertura y curiosidad frente a futuras tendencias tecnológicas dinámicas, cambios en los hábitos de los consumidores, nuevas ideas y oportunidades de negocios, manteniendo al mismo tiempo el respeto por los valores básicos, las actitudes y los comportamientos humanos.

- Orgullo de contribuir a la reputación y a los resultados de la Compañía, lo que significa un alto sentido de la calidad y de los logros a largo plazo en el trabajo diario, por encima de la forma y de la ganancia rápida.

- Lealtad a la Compañía e identificación con ella.

- Los ejecutivos de AES Dominicana, en todos los niveles jerárquicos, están más preocupados en añadir constantemente valor a la Compañía que en ejercer una autoridad formal. Esto sólo puede materializarse con un alto involucramiento por parte de cada empleado y un pensamiento común enfocado hacia los resultados. La contribución a los resultados mediante proyectos y tareas especiales es cada vez más frecuente, dejando de lado los límites convencionales con el fin de participar más ampliamente en los resultados del Grupo.

2.14 Características Observables de la Cultura Organizacional

Ritos, Rituales y Ceremonias

Todos los meses se celebra el cumpleaños de los colaboradores en todas las localidades de AES Dominicana. En la oficina principal se hace un brindis con el personal administrativo acompañado de bizcocho, decoraciones alusivas a la ocasión o de acorde a las preferencias del/los festejados, por ejemplo, si a una persona le gusta la música disco se le decora su oficina y el ambiente festivo de acuerdo a como se veía en esa época. En las plantas se hace un almuerzo y se brinda bizcocho al personal, se decora el ambiente del comedor de acuerdo a la ocasión.

En el mes de diciembre se hace una fiesta en un hotel de la ciudad en la que participan todos los empleados y contratistas de AES Dominicana con sus esposas y esposos. Se hacen rifas de premios tanto metálicos como en otros artículos de valor. El día del trabajo se celebra con un brindis en todas las unidades de negocio, el CEO de la compañía hace alocución de unas breves palabras de agradecimiento a todos los colaboradores.

Como la seguridad es su primer valor, celebran el día de la seguridad AES a nivel mundial, cada país tiene su forma de celebrarlo, en AES Dominicana se reúne el personal en una localidad fuera de la ciudad donde reciben charlas sobre diversos temas de seguridad en el hogar, en el trabajo y en las calles. Se realizan actividades de dinámica en grupo sobre temas de seguridad. Se realizan prácticas de extinción de fuegos, primeros auxilios, tratamiento de quemaduras y muchas otras actividades relacionadas con la seguridad en todos los ámbitos de la vida de las personas, no solo a nivel de trabajo.

Tiene un “Día de los valores” donde se celebran actividades relacionadas con los valores de la empresa, se hacen charlas, competencias, ejercicios de ética y orden moral.

Slogan y Logo

“La Energía de ser globales” – “The Power of being global”

Lenguaje

El lenguaje utilizado contiene tecnicismos propios del ambiente de trabajo, se utilizan diversos señalamientos a nivel de ingeniería, sistemas comerciales y legales. Aunque el departamento de servicio al cliente utiliza un lenguaje más llano para en entendimiento de los relacionados externos.

Mitos e historias

Por su mezcla cultural de personas que provienen de distintos países en AES Dominicana no se observa ninguna historia o mito que haya calado en el sentir de las personas que allí laboran para ser considerado dentro del ámbito cultural.

Entorno Físico

El entorno de trabajo de AES Dominicana está concebido para valorar la interrelación de sus colaboradores, son espacios abiertos para las gerencias medias y cerradas en cristales para la alta gerencia. Se observan algunos espacios cerrados por completo por razones de seguridad como por ejemplo el datacenter, las oficinas del departamento de infraestructura y los almacenes del departamento de relaciones públicas.

El área de presidencia concentra a las oficinas de los vicepresidentes y CEO, son oficinas semi abiertas por razones de privacidad.

Estimulo Físico

Tienen un área de comedor en todas las unidades de negocio a excepción de las oficinas administrativas las cuales utilizan el área de comida de la plaza donde está ubicada para el almuerzo. Próximamente se evaluara la posibilidad de abrir un club de empleados o colaboración con algún club local para el recreo de sus colaboradores.

2.14 Propensiones Tecnológicas

Durante los últimos años la humanidad se ha hecho eco de las innovaciones en las áreas de la informática y las comunicaciones, en cómo estas han aumentado notablemente la capacidad de adquirir, almacenar, procesar y distribuir información, creando nuevas industrias y, no menos importante, transformando sustancialmente las formas de organización, producción y comercialización en todas las actividades productivas.

2.14.1 La tecnología de la Información

En la actualidad las constantes innovaciones tecnológicas nos han permitido utilizar recursos que apenas unos años atrás no contábamos con su existencia. La capacidad de movilidad, el aumento en el procesamiento de los datos, la conexión de múltiples servicios a través de un solo terminal esta provocando que el desarrollo de las TI y las consecuentes aplicaciones sean una constante en el tiempo. De esta forma, los aplicativos desarrollados y cambiantes se convierten en servicios con el fin de satisfacer la demanda de usuarios de acceso a lo que satisface su necesidad en cualquier lugar y condición. Las aplicaciones se concentraran en arquitecturas orientadas a los servicios, las cuales le facilitaran al usuario la satisfacción de su necesidad sin las restricciones de una ubicación física o programación dedicada a un solo servicio.

2.14.2 Las Telecomunicaciones

Los servicios convergentes han sido posibles a los grandes avances realizados por el mundo de las telecomunicaciones. Los usuarios pueden situarse en cualquier parte del mundo y acceder a recursos empresariales de un país a otro, la demanda de servicios de comunicaciones va en aumento cada día. Para AES Dominicana esto es indicativo de que su infraestructura de comunicaciones debe ser revisada cuidadosamente para responder a demandas potenciales de sus clientes internos, ya que estos exigen cada vez más servicios en localidades remotas, de difícil acceso a planta externa de proveedores y con alto costo operativo. Lo anterior traerá como consecuencia que las redes híbridas alámbricas-inalámbricas sean el común denominador, con el fin de dotar de una infraestructura de servicios, siempre comunicados, independientes de su ubicación. Los equipos activos de la red mantendrán la tendencia en el uso de puertos conmutados, (switches), agregando capacidades que los convertirán en puertos inteligentes, reforzando principalmente los aspectos de seguridad de las comunicaciones.

2.14.3 Seguridad Informática

En el entorno actual no se concibe el uso de una aplicación o de un dispositivo sin que éste se encuentre conectado o interconectado en una red. De ahí que las amenazas a la información y comunicaciones siempre estarán latentes y con un riego potencial creciente; redes de igual a igual (P2P), el correo no solicitado (Spam), los virus informáticos y últimamente, los programas espía, requerirán de soluciones y acciones con un constante cambio para contra restar sus efectos.

La identificación de usuarios, la universalidad de los servicios y el impacto a la preservación del ambiente darán paso a la oficina sin papel, mediante el uso de tecnologías de identificación biométrica y con el empleo generalizado de la tecnología de llave pública (PKI). Estas tecnologías enfrentarán el reto de actualizarse de manera constante y rápida, debido al incremento exponencial de las capacidades de procesamiento de cómputo.

La seguridad se irá transformando a un concepto de seguridad "inteligente" y deberá estar presente y ser considerada como parte intrínseca en los programas, en los equipos, en las comunicaciones, en los archivos electrónicos, en los servicios y prácticamente en todas las soluciones relacionadas con las TIC en las que intervenga el ser humano.

2.15 Análisis del Entorno

En materia de progresos de las tecnologías de información y comunicación no es posible negar que hayan sido continuos, esto ha provocado la masificación del uso de estas tecnologías a través de la oferta de medios cada vez más poderosos, baratos y fáciles de usar. El potencial que ofrecen las TIC en el manejo, almacenamiento, procesamiento y transmisión de información permite nuevas formas de realizar las operaciones de las organizaciones y las interacciones sociales y económicas con medios electrónicos. En este contexto, el equipo de IT de AES Dominicana debe afrontar los retos para la planeación y el desarrollo de sus actividades con base en:

- El perfeccionamiento y explotación del conocimiento en materia de TIC de su personal;
- El fomento de una cultura y de componentes para la seguridad informática; y
- Los lineamientos que emita la casa matriz AES Corp. En materia de TI y CyberSecurity.

2.15 Creación de una ventaja competitiva

El proyecto de virtualización de Equipos de control de plantas de AES Dominicana es una prioridad del departamento de IT y establece que en términos de infraestructura el departamento de IT juega un papel importante en la adopción y enfoque tecnológico de las unidades de negocio del grupo a la vez que sirve de catalizador para la estrategia de líder en costos que se requiere implementar para la creación de una ventaja competitiva respecto al mercado.

2.16 La seguridad Informática

La masificación del CyberCrime ha hecho necesario que esto se vuelva una prioridad dentro del ámbito productivo de la empresa. Virus como Stuxnet que ataca sistemas SCADA de control de plantas representan un peligro latente para las operaciones diarias de la empresa, por ello se le debe prestar delicada atención, en este sentido el equipo de Aes Dominicana se ha volcado en el reforzamiento de CyberSecurity e ITGC (Information & Technology General Control) tomando medidas basadas en las mejores prácticas de prevención, detección y erradicación de código malicioso que pueda poner en peligro las operaciones de las unidades de negocio.

CAPITULO III

Seguridad de la información

3.1 Concepto[30]

En la seguridad de la información y su manejo no está basado solamente en la tecnología. La información es el principal activo de una empresa y su valor dependerá de los datos útiles para sus competidores. La información puede ser divulgada, mal utilizada, robada o borrada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

Crítica: Es indispensable para la operación de la empresa.

Valiosa: Es un activo de la empresa y muy valioso.

Sensible: Debe de ser conocida por las personas autorizadas

Existen dos palabras muy importantes que son riesgo y seguridad:

Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.

Seguridad: Es una forma de protección contra los riesgos.

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad de la información, comunicación, identificación de problemas, análisis de riesgos, la integridad y confidencialidad.

Precisamente la reducción o eliminación de riesgos asociado a la información es el objeto de la seguridad de la información y donde entra la seguridad informática.

[30] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Más concretamente, la **seguridad de la información tecnológica** tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de la información.

Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad la **confidencialidad**, **integridad** y **disponibilidad** de la información. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles.

Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración. Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "**C**onfidentiality,**I**ntegrity, **A**vailability") son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro.

Fuente: http://www.bitcompany.biz/gestion-de-seguridad-que-es-iso-27001/
Grafica 3.1

Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

3.2 Servicios de seguridad[31]

El objetivo de un servicio de seguridad es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los servicios de seguridad están diseñados para contrarrestar los ataques a la seguridad y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio.

No repudio

Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. El servicio de Seguridad de No repudio o irrenunciabilidad está estandarizado en la ISO-7498-2.

No Repudio de origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

- Prueba que el mensaje fue enviado por la parte específica.

No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

- Prueba que el mensaje fue recibido por la parte específica.

Si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el “no repudio” prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

[31] Ibid.

El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje.

3.3 Planificación de la seguridad[32]

Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito del plan de seguridad de la información es proporcionar una visión general de los requisitos de seguridad y se describen los controles en el lugar o los previstos para cumplir esos requisitos. El plan de seguridad también delinea las responsabilidades y el comportamiento esperado de todos los individuos que acceden a la información.

3.4 Creación de un plan de respuesta a incidentes[33]

Es importante formular un plan de respuestas a incidentes, soportarlo a lo largo de la organización y probarlo regularmente. Un buen plan de respuestas a incidentes puede no sólo minimizar los efectos de una violación sino también, salvaguardar la disponibilidad e integridad de la información.

Desde la perspectiva del equipo de seguridad, no importa si ocurre una violación, sino más bien cuando ocurre. El aspecto positivo de entender la inevitabilidad de una violación a los sistemas (cualquier sistema donde se procese información confidencial, no está limitado a servicios informáticos) es que permite al equipo de seguridad desarrollar un curso de acciones para minimizar los daños potenciales. Combinando un curso de acciones con la experiencia le permite al equipo responder a condiciones adversas de una manera formal y oportuna.

[32] Ibid

[33] Ibid.

El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- Acción inmediata para detener o minimizar el incidente.
- Investigación del incidente.
- Restauración de los recursos afectados.
- Reporte del incidente a los canales apropiados.

Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente. Debido a que hay muy poco espacio para errores, es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta. De esta forma, es posible desarrollar una metodología que fomenta la velocidad y la precisión, minimizando el impacto de la indisponibilidad de los recursos y el daño potencial causado por el sistema en peligro.

Un plan de respuesta a incidentes tiene un número de requerimientos, incluyendo:

- Un equipo de expertos locales.
- Una estrategia legal revisada y aprobada.
- Soporte financiero de la compañía.
- Soporte ejecutivo de la gerencia superior.
- Un plan de acción factible y probado.

3.5 Los 4 tipos de incidentes de seguridad[34]

- Desastres naturales
- Los ataques maliciosos
- Ataques internos
- Mal funcionamiento de equipos o error humano no intencionado

[34] Dejan Kosutic, 9 steps to cybersecurity, Ed. EPPS Services LTD, Zagreb, p.12-16

Desastres Naturales

En los últimos años el mundo ha experimentado varios desastres naturales que han ganado la atención mundial. Los huracanes, como Katrina y Sandy, el desastre de Fukushima, tsunamis y terremotos, como el de Haití todo han sido devastadores y destruyeron negocios enteros y bancos de datos. Además, los desastres como tornados, inundaciones y tormentas pueden ser suficientes para desaparecer un negocio en casi cualquier lugar. Incluso un fuego localizado puede destruir toda su data si no cuenta con un sistema de respaldo y almacenamiento en un lugar alterno a su localidad principal.

Los ataques maliciosos

Los ataques cibernéticos y brechas de seguridad están sucediendo cada minuto y son demasiado generalizadas para realizar un seguimiento. Algunos son pequeños, otros son grandes, algunos tienen éxito en su propósito y otros no.

Estos son algunos de los principales incidentes en los últimos años.

En mayo de 2006 los nombres, números de seguro social, fechas de nacimiento, y algunas clasificaciones de discapacidad para los 26,5 millones de veteranos y el personal militar en servicio activo y sus cónyuges fueron tomados del Departamento de Asuntos de Veteranos de EE.UU.

La información había estado en una portátil y un disco duro externo, fueron sustraídos en un robo. Mientras que los artículos fueron recuperados más tarde, las pérdidas estimadas y los costos de prevención podrían superar la mitad de mil millones de dólares.

06 de agosto 2006 AOL atacada; los datos de más de 650,000 usuarios, incluidas las compras y la información bancaria, fueron publicadas en un sitio web.

En marzo de 2008, una base de datos de Heartland Payment Systems fue atacado, dejando 134 millones de tarjetas de débito y de crédito expuestas. Albert González fue más tarde condenado por el crimen y condenado a 20 años de prisión federal.

En 2009, el gobierno chino lanzó un ataque masivo y sin precedentes en Google, Yahoo, y docenas de otras compañías de Silicon Valley. Google confesó que algunos de su propiedad intelectual habían sido robados.

En 2011 RSA Security reportó que un máximo de 40 millones de registros de empleados fueron robados. Este incidente se atribuye a ataques posteriores sobre Lockheed- Martin, L3, y otros. La violación ha sido descrito como absolutamente masiva desde una perspectiva potencial daño, y desde una perspectiva psicológica.

En 2011 ESTsoft perdió los datos personales de 35 millones de coreanos del sur debido a los piratas informáticos.

“Casi todo el mundo va a ser hackeado con el tiempo ", afirma Jon Callas, director de tecnología de Entrust en un post en Help Net Security.

Los ataques internos

En julio de 2007 un empleado de Fidelity National Information Services robó 3,2 millones de registros de clientes, incluyendo la tarjeta de crédito, datos bancarios y la información personal . Un administrador de base de datos llamado William Sullivan fue posteriormente condenado a cuatro años y nueve meses de prisión y al pago de una multa de $ 3,2 millones.

El famoso sitio web de Wikileaks fue frezado de acceso a información privilegiada. El jurado aún está deliberando sobre el daño y los efectos de este caso monumental.

Mal funcionamiento de equipos y error humano no intencional

Los equipos y mal funcionamiento de la infraestructura es algo que encontramos casi a diario, el fallo de los enlaces de Internet y líneas telefónicas, destrucción de unidades de disco duro, y así sucesivamente.

¿Y qué tal cuando su colega sobrescribe los datos por error? Y ¿cuándo usted derrama una taza de café sobre su computadora portátil?

Todas estas situaciones tienen dos cosas en común: primero, la consecuencia es que usted pierde sus datos o usted no será capaz de acceder a ellos, en segundo lugar, este tipo de incidentes ocurren con bastante frecuencia.

Uno de los pasos iniciales en la construcción de su ciberseguridad es ser conscientes del entorno que estamos viviendo

Supongamos que en este sentido la seguridad cibernética no es demasiado diferente de la gestión de otras partes de su empresa.

3.6 El manejo de riesgos[35]

Dentro de la seguridad en la información se lleva a cabo la clasificación de las alternativas para manejar los posibles riegos que un activo o bien puede tener dentro de los procesos de organización. Esta clasificación lleva el nombre de manejo de riegos. El manejo de riesgos, conlleva una estructura bien definida, con un control adecuado y su manejo, habiéndolos identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

Evitar. El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo.

[35] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Reducir. Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible.

Retener, Asumir o Aceptar el riesgo. Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente.

Transferir. Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo, compartiéndolo con otras entidades.

3.7 Gobierno de la Seguridad de la Información[36]

Un término a tomar en cuenta en el área de la seguridad de la información es su Gobierno dentro de alguna organización empezando por determinar los riesgos que le atañen y su forma de reducir y/o mitigar impactos adversos a un nivel aceptable mediante el establecimiento de un programa amplio y conciso en seguridad de la información y el uso efectivo de recursos cuya guía principal sean los objetivos del negocio, es decir, un programa que asegure una dirección estratégica enfocada a los objetivos de una organización y la protección de su información.

[36] Ibid.

3.8 Tecnologías[37]

Las principales tecnologías referentes a la seguridad de la información en informática son:

- Cortafuegos o Firewalls
- Administración de cuentas de usuarios
- Detección y prevención de intrusos
- Antivirus
- Infraestructura de llave publica
- Capas de Socket Segura (SSL)
- Conexión única "Single Sign on- SSO"
- Biometría
- Cifrado
- Cumplimiento de privacidad
- Acceso remoto
- Firma digital
- Intercambio electrónico de Datos "EDI" y Transferencia Electrónica de Fondos "EFT"
- Redes Virtuales Privadas "VPNs"
- Transferencia Electrónica Segura "SET"
- Informática Forense
- Recuperación de datos
- Tecnologías de monitoreo

[37] Ibid

3.9 Estándares de seguridad de la información

ISO/IEC 27000-series: La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).[38]

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.[39]

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming":PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995.[40]

[38] http://es.wikipedia.org/wiki/ISO/IEC_27000-series

[39] http://es.wikipedia.org/wiki/ISO/IEC_27001

[40] http://es.wikipedia.org/wiki/ISO/IEC_27002

3.10 La ciberseguridad Mitos[41]

Se debe explicar lo que la seguridad cibernética no es, hay muchos mitos bien establecidos que pueden obstaculizar el entendimiento del tema.

Mito # 1 - Es todo acerca de TI

Imagine este escenario: un administrador de sistemas descontentos deshabilita intencionadamente su aplicación principal y elimina las bases de datos más importantes.

¿Es esto un problema de TI? No, esto no es un problema de TI, más como una cuestión de recursos humanos. ¿Podría haberse evitado de garantías de TI? No. Se requiere que la persona en esta posición para tener acceso directo a todos sus sistemas.

Por lo tanto, la manera de prevenir este tipo de escenario se encuentra fuera del área de la tecnología y se reduce a la forma de seleccionar a sus empleados, la forma de controlar su uso, que se han firmado tipo de documentos legales, como esta persona sea tratada dentro de la compañía, y así en.

Mito # 2 - Alta Dirección no tiene nada que ver con la seguridad cibernética

Se es probablemente consciente de que las seguridades no pueden aplicarse sin el dinero y el tiempo de trabajo empleado. Pero, si los directivos de la empresa no están convencidos de esta protección contra la información, no se les van a proporcionar los recursos necesarios. Por lo tanto, el proyecto fracasará.

Si los altos ejecutivos no cumplen con las normas de seguridad y, por ejemplo, dejar el portátil (con su lista de los clientes junto con precisiones sobre las ventas y la correspondencia relacionada) no protegidas en el aeropuerto, todos los otros esfuerzos de seguridad serán en vano.

[41] Dejan Kosutic, 9 steps to cybersecurity, Ed. EPPS Services LTD, Zagreb, p.17-22.

Por lo tanto, los altos directivos son una parte muy importante de la seguridad cibernética.

Mito # 3 - La mayor parte de la inversión será en Tecnología

Falso. La información será protegida si todo el mundo con acceso sabe lo que está permitido y lo que no lo es, y quién es responsable de cada pieza de información o para cada pieza de equipo. Esto se logra mediante la definición de reglas claras, por lo general en forma de políticas y procedimientos.

Como regla principal, yo diría que la inversión en tecnología es por lo general menos de la mitad de la inversión requerida. En algunos casos, puede incluso ser menor que 10 %. La mayor parte de la inversión es por lo general en el desarrollo de las políticas y procedimientos, formación y sensibilización.

Mito # 4 - No hay retorno de la inversión en seguridad

Sí, la seguridad cuesta dinero, y por lo general esta protección no le traerá ingresos adicionales.

Toda la idea de la seguridad cibernética es disminuir los costos relacionados con los problemas de seguridad (es decir, incidentes). Las arreglas para disminuir el número y / o el alcance de los incidentes de seguridad, lograran que la empresa ahorre dinero. En la mayoría de los casos, los ahorros obtenidos son mucho mayores que el costo de las implementaciones de políticas, procedimientos y tecnologías de seguridad de información.

Mito # 5 - La seguridad cibernética es un proyecto de una sola vez

Falso. La seguridad cibernética es un proceso continuo. Por ejemplo, si desarrolla un procedimiento de respuesta a incidentes que obliga a sus empleados a notificar al Director de Seguridad en su teléfono celular sobre cada incidente, pero entonces esta persona sale de su empresa, es obvio que ya no desea que estas llamadas para ir a él o ella, si usted quiere que su sistema sea funcional. Hay que actualizar los procedimientos y políticas, sino también software, equipos, acuerdos, etc, es un proceso constante.

Mito # 6 – El mito de documentación

Redactar una cantidad enorme de políticas y procedimientos no significa que el personal iniciara automáticamente su cumplimiento.

La seguridad es normalmente un cambio bastante grande y, francamente, a nadie le gusta cambiar las prácticas establecidas. Por ejemplo, un paradigma básico y difícil de romper es el de las contraseñas; donde un usuario debe cambiar su clave de "1234 " de años a cambiarla a cada 90 días, 8 caracteres, minúsculas, mayúsculas, números y caracteres especiales.

Capitulo IV

Propuesta de gestión de la seguridad de la información en AES Dominicana

4.1 Propósito

El propósito de este documento es describir las normas de seguridad cibernética obligatorias que deberían aplicar y ser adoptadas por todas las Unidades de Negocio Estratégicas de AES (SBU). Estas normas establecen los requisitos mínimos de seguridad cibernética AES SBU. Sobre la base de los requerimientos geográficos o reglamentarios específicas, muchas unidades de negocios pueden elegir implementaciones más rigurosas de estas normas.

Considerando que las políticas de tecnología de AES Global, tienen como propósito definir las reglas de negocio de alto nivel para la seguridad cibernética, estas normas establecen requisitos más detallados sobre cómo se deben implementar las políticas. Las normas fueron escritas con una audiencia.

4.2 Alcance

El cumplimiento de estas normas seria obligatoria y seria validado a través de un curso "Confiar pero verificar" del programa. Las normas serán aumentadas en el tiempo basado en el entorno de ciberseguridad y en su rápida evolución, así como la retroalimentación de las demás SBU.

Estas normas se basan en la armonización de los dos modelos clave de seguridad cibernética: el Capability Maturity Model Electricidad Subsector Cybersecurity(ES- C2M2)[42] y TOP 20 SANS Critical Security Controls para una eficaz Ciber Defensa (SANS 20)[43].

4.3 Estándares de seguridad de la información

1) Arquitectura de Seguridad de Red (SANS 13)

Una arquitectura de red es un modelo de seguridad de comunicaciones para una red. Es un marco para la especificación de los componentes físicos de una red y de su organización funcional y configuración, sus procedimientos y principios operacionales, así como los formatos de los datos utilizados en su funcionamiento para mitigar un ataque a la seguridad. [44]

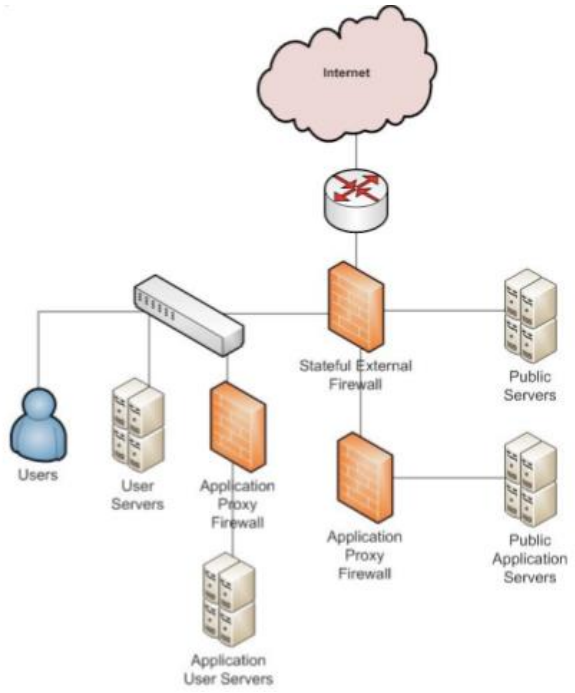
La SBU debe implementar una arquitectura de seguridad de red que cumple con los requisitos mínimos de separación entre la nube de Internet, servidores de aplicaciones locales, las empresas (usuarios), las redes, y redes de sistemas de control (SCADA).

[42] http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf

[43] Anexo II.

[44] http://es.wikipedia.org/wiki/Arquitectura_de_Red

No debe haber tráfico entre estos cuatro dominios sin necesidad de ir a través de cortafuegos configurados correctamente.



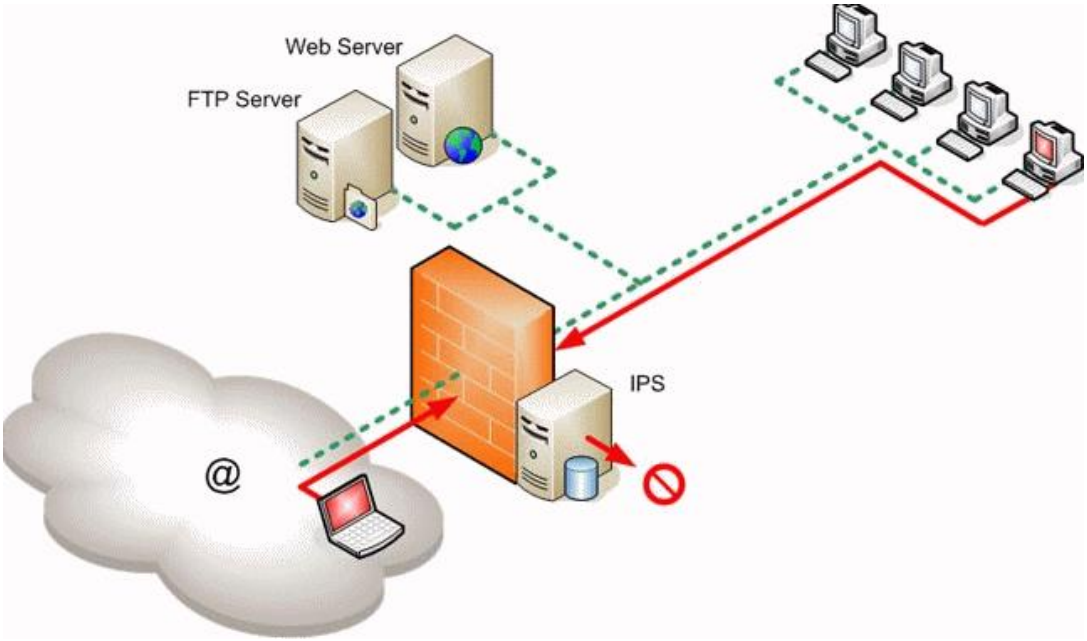
Fuente: Propia

Grafica 4.1

2) Arquitectura y Configuraciones Secure Firewall (SANS 10 y 11)

Firewall de Internet

La SBU debe implementar uno o más servidores de seguridad de Internet (Firewall), que sirven como primera línea de defensa contra los ataques cibernéticos. Este servidor de seguridad debe tener el sistema de detección de intrusos (IDS) y activar el sistema de prevención de intrusiones (IPS) con las firmas incorporadas.



Fuente: Business Network Firewall Magazine (o de servidores Firewall)

Grafica 4.2

La SBU debe implementar uno o más servidores de seguridad de red de negocios (o firewalls de granjas de servidores), que sirven como la segunda línea de defensa. Este dispositivo debe separar los servidores de aplicaciones de negocio (por ejemplo, SAP, DNS, Active Directory y Sistema de Comercio) de las redes de usuarios y otras redes.

Un enfoque múltiple virtual de red de área local (VLAN) también debe ser implementado con el fin de separar los servidores de bases de datos, aplicaciones y sistemas de archivos entre sí, permitiendo un entorno más seguro. Este cortafuego también debería incorporar los servicios de IDS e IPS integrado.

Sistema de Control de Red Firewall (ICS o industrial de la red)

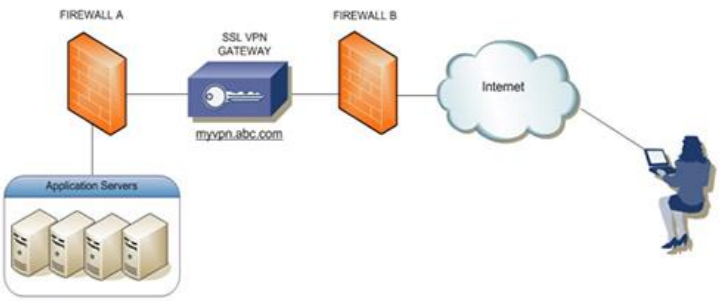
La SBU debe implementar uno o más servidores de seguridad de red para los sistemas de control, que sirven como la tercera línea de defensa contra los ataques cibernéticos. Este dispositivo se segregará a todas las aplicaciones relacionadas con el sistema de control de las redes de las empresas y de los usuarios. Por lo general tendrá al menos 3 redes:

- Sistemas de Sistema de Control Distribuido (DCS) / Sistema de Control Industrial (ICS)
- El sistema de PI
- Otras aplicaciones relacionadas con la operación de la planta

Este cortafuego también debería tener integrado los servicios de IDS e IPS. Idealmente, también tendrá firmas adicionales para IPS que se centraran en la protección de las aplicaciones de sistemas de control.

Configuración de los cortafuegos (Firewall)

Cuando se implementen los servidores de seguridad anteriores, cada negocio dentro de la SBU debe asegurarse de que los permisos de firewall que permitan el tráfico sin restricciones no estén permitidos. En los casos en que se requiere acceso remoto para fines de mantenimiento, una conexión de red privada virtual (VPN) debe ser establecida con la empresa asociada que sólo permite la conexión del protocolo específico de Internet (IP) de la empresa asociada. El equipo de AES Global Network Security puede proporcionar una configuración de ejemplo como guía si se solicita.



Fuente: Repaso de la configuración del cortafuegos y Auditoría 2012 Firewall Magazine.

Grafico 4.3

La SBU debe realizar una revisión de la configuración del firewall, al menos, dos veces al año (los administradores locales o empresas externas) con el fin de confirmar el cumplimiento de las normas mínimas.

El equipo de AES Global Network Security auditará los servidores de seguridad y los sistemas de revestimiento de Internet por lo menos una vez al año para confirmar el cumplimiento de las normas mínimas.

3) Inventario de dispositivos de red (SANS 1)

Se debe conocer e inventariar los dispositivos que forman parte o deben pertenecer a la red, y bloquear el acceso al resto.

Con el fin de reducir la capacidad de los atacantes para encontrar y explotar sistemas no autorizados y sin protección, cada negocio debe crear y mantener un inventario de los dispositivos autorizados y no autorizados conectados a la red. En este contexto, " dispositivos" se refiere a cualquier equipo con una dirección IP, incluyendo pero no limitado a las estaciones de trabajo (de escritorio / portátiles), servidores, routers, switches, firewalls, impresoras, redes de área de almacenamiento, teléfonos IP y cámaras IP. Cada negocio debe documentar un proceso para mantener el inventario hasta a la fecha y la supervisión del cumplimiento con el inventario.

4) Inventario de Software (SANS 2)

Al igual que con los dispositivos, realizar la misma tarea con el software corporativo. Esto facilitará futuras tareas ya sean de mantenimiento o actualización. Así mismo, utilizar herramientas que hagan un seguimiento del software instalado, consolas de gestión y centralización.

La SBU debe crear y mantener un inventario de software autorizado y no autorizado para cada tipo de sistema, incluyendo las estaciones de trabajo (de escritorio / portátiles) y servidores. La SBU debe documentar un proceso para mantener el inventario hasta a la fecha y la supervisión del cumplimiento con el inventario.

5) Las defensas de malware (SANS 5)

Punto clave, de nada sirve protegernos de lo que nos pueda venir de fuera, si luego se permite que la red interna este contagiada de malwares que puedan venir en dispositivos extraíbles o descargados desde internet. La protección y monitorización de estas amenazas es una responsabilidad que debe establecerse en diferentes puntos de la red, apoyándonos no sólo en las soluciones de antivirus, si no en sistemas de detección y prevención de intrusiones.

La SBU debe emplear herramientas automatizadas para monitorear continuamente las estaciones de trabajo (de escritorio / portátiles), servidores y up-to- date (antivirus) protección anti- malware.

La SBU debe o bien configurar el software anti -malware y las características de actualización automática de la firma o haber administradores que envíen manualmente las actualizaciones en todos los equipos por lo menos en una base diaria. Además, las estaciones de trabajo (de escritorio / portátiles) y servidores se deben configurar para que ejecuten contenido de ejecución automática de los dispositivos de medios extraíbles, como unidades USB, CDs y DVDs.

Las estaciones de trabajo (de escritorio / portátiles) y servidores se deben configurar para que realicen un análisis anti-malware automático de medios extraíbles cuando se inserten en el equipo.

6) Evaluaciones de Vulnerabilidad y Gestión de Actualizaciones (SANS 4)

Con el fin de proteger los activos identificados como parte del inventario de dispositivos de red, la SBU debe documentar e implementar un proceso para la identificación proactiva y remediar las vulnerabilidades de software reportadas y los analistas de seguridad. Las vulnerabilidades clasificadas como "críticas" deben ser remediadas dentro de las 48 horas de la notificación.

Como mínimo, las herramientas automatizadas de análisis de vulnerabilidades se deben ejecutar en contra de todos los sistemas, por lo menos cada tres meses. Para fines de seguimiento, las tareas de evaluación de la vulnerabilidad y la gestión de parches deben ser documentadas a través de una solicitud de gestión del cambio.

7) Respuesta a Incidentes (SANS 18)

La SBU debe documentar un plan de respuesta a incidentes de seguridad cibernética, incluyendo todas las fases del ciclo de vida del incidente (la notificación, la gestión, la comunicación, la coordinación y el cierre).

El plan también debe incluir roles y responsabilidades para respuesta a incidentes de seguridad cibernética, que incluye un plan de comunicación para los grupos internos y externos. Dependiendo de la gravedad del incidente; una reunión de emergencia del Consejo de Seguridad Global de TI puede ser convocada con el fin de compartir información sobre el incidente y dictar auditorías obligatorias por otras unidades de negocios (para proteger contra ataques similares), según sea necesario.

Dependiendo de la gravedad del incidente, las lecciones aprendidas y las recomendaciones formales deben ser presentadas al Consejo de Seguridad de TI. Para fines de seguimiento, tareas de respuesta a incidentes de seguridad cibernética deben documentarse a través de una solicitud de gestión del cambio.

8) Filtrado de Contenido Web

Para ayudar a proteger a AES personas que utilizan Internet para hacer negocios, cada negocio debe utilizar una solución de software (como Websense) para realizar el filtrado de contenidos web (basado en firmas o sitios web de la lista negra que se actualizan de forma automática por el proveedor de software).

Como mínimo, los siguientes sitios web deben ser bloqueadas:

• Los sitios web que tienen contenido ofensivo o potencialmente ofensivo (incluyendo, pero no limitado a la información que sea sexualmente explícito, racista, violento, discriminatorio, o afiliado con el terrorismo).

• Los sitios web que son una fuente conocida de las vulnerabilidades de seguridad, malware, o de otros contenidos maliciosos.

A continuación se enumeran las categorías de sitios web que deben ser bloqueadas:

1) Filtrado de seguridad

- Advanced Malware Command and Control - Protege contra las transmisiones de red salientes de una máquina comprometida a un centro de mando y control malicioso.
- Advanced Malware Payloads - Protege contra las transmisiones de red entrantes de conexiones destinadas a explotar una máquina.
- Las redes de bots - Sitios que alojan los centros de comando y control para redes de bots que se han infiltrado en los ordenadores de los usuarios. Excluye rastreadores Web.

- Keyloggers - Sitios o páginas que descargan programas que se ejecutan en segundo plano para registrar todas las pulsaciones de teclado, y que también pueden enviar aquellas combinaciones de teclas (incluyendo potencialmente las contraseñas o información confidencial) a una entidad externa.
- Sitios con enlaces maliciosos - Los sitios que están infectadas con un enlace malicioso.
- Sitios Web maliciosos - Sitios que contienen código que puede modificar intencionalmente los sistemas del usuario final sin su consentimiento y causar daño.

- Mobile Malware - Protege contra sitios web maliciosos y aplicaciones que están diseñadas para funcionar en dispositivos móviles.
- Phishing y otros fraudes - Los sitios que falsifican sitios de negocios legítimos para los fines de la obtención de información privada financiera o de otro tipo de usuarios.
- Software Potencialmente no Deseado - Sitios que utilizan tecnologías que alteran el funcionamiento del hardware del usuario, el software o la red de manera que disminuyan el control sobre del usuario, la privacidad o la recopilación y distribución de información personal.
- Spyware - Sitios o páginas que descargan software que, sin el conocimiento del usuario, generan tráfico HTTP.
- Link Embedded sospechoso - Sitios sospechosos de estar infectados con un enlace malicioso.
- Los mercados móviles no autorizadas - Protege contra los sitios web que potencialmente distribuyen aplicaciones que no están autorizados por el fabricante del sistema operativo móvil, el fabricante del dispositivo de mano o el proveedor de la red.

2) Categorías ancho de banda

- Archivos peer - to peer para compartir - Sitios que ofrecen software de cliente para permitir el intercambio y la transferencia de peer -to-peer de archivos.
- Almacenamiento en Red Personal y copia de seguridad - Los sitios que almacenan archivos personales en los servidores de Internet para la copia de seguridad o cambio.

3) Categorías de línea de base

- Web y de correo electrónico Spam - Sitios cuyos vínculos son enviados en el correo electrónico comercial no solicitado, ya sea como parte de las campañas para promocionar productos o servicios, o para atraer a los lectores a hacer clic a través de encuestas o sitios similares. También se incluyen los sitios que muestran los comentarios no deseados.

4) El cortar y Evasión de proxy.

Sitios que proporcionan información sobre el acceso ilegal o cuestionable o el uso de equipos de comunicaciones / software, o proporcionar información sobre la manera de evitar las funciones del servidor proxy o tener acceso a las direcciones URL de cualquier manera que no pasa por el servidor proxy. Por ejemplo: www.anonymizer.com / astalavista.box.sk / www.happyhacker.org / www.phreak.com

5) Descargas de Software.

Los sitios que se dedican a la descarga electrónica de paquetes de software, ya sea de pago o de forma gratuita. Por ejemplo: www.download.com / www.tucows.com

6) Streaming Media y MP3.

Los sitios que venden, entregan o reproducen música o video en cualquier formato, incluyendo sitios que ofrecen descargas de estos visores. Por ejemplo: www.mp3.com / www.windowsmedia.com / www.musiccity.com

8) Juegos.

Sitios que proporcionan información de juegos o la descarga de videojuegos, juegos de ordenador, juegos electrónicos, consejos y asesoramiento sobre juegos o cómo obtener los códigos de trucos.

9) Extended

- DNS dinámico - Los sitios que ocultan su identidad utilizando los servicios de DNS dinámico, a menudo asociados con las amenazas persistentes avanzadas.
- La exposición elevada - Sitios que camuflan su verdadera naturaleza o que incluyen elementos que sugieren una intención maligna latente.
- Contenido potencialmente dañino - Sitios que puedan contener poco o ningún contenido útil.

9) Protección contra inundaciones de tráfico

Para protegerse contra ataques de inundación de tráfico como denegación de servicio distribuida (DDoS), cada negocio debe tener un contrato de servicios de mitigación de DDoS con un proveedor de Internet y / o una estrategia de mitigación en su lugar. Este servicio se asegurará de que, en caso de un ataque, sólo el tráfico limpio será entregado a los sistemas, evitando así las interrupciones del servicio.

4.4 Seguridad Cibernética: Controles

Los controles enumerados debajo y luego descritos, engloban básicamente los métodos y procedimientos que deben ser implementados en la organización con el fin de mitigar ataques a los activos tecnológicos de la empresa.

1) Inventario de Dispositivos.
2) Inventario de Software.
3) Realización de configuraciones seguras para hardware y software de computadoras móviles, computadoras de escritorios y servidores.
4) Defensas de malware.
5) Seguridad de aplicaciones.
6) Control de dispositivos inalámbricos

7) Capacidad de recuperación de datos
8) Asegurar las configuraciones de los dispositivos de red como cortafuegos, routers and switches.
9) Limitación y Control de los puertos de red, protocolos y servicios.
10) Uso Controlado de privilegios administrativos.
11) Límites de Defensa.
12) Mantenimiento, Monitoreo y Análisis de Registros de auditoría.
13) Seguimiento y Control de Cuenta.
14) Prevención de Pérdida de Datos.
15) Capacidad de Respuesta a Incidentes.
16) Pruebas de Penetración y Ejercicios equipo rojo.

1. Inventario de dispositivos

1.1. Implementar una herramienta automatizada.

1.2. Mantener un inventario de los dispositivos conectados a la red.

1.3. Nombre de la máquina, el propósito de cada sistema, un responsable de cada dispositivo, y el departamento.

1.4. Incluir los datos de dispositivos portátiles (teléfonos móviles, tabletas, ordenadores portátiles, y otros).

1.5. Asegúrese de que las herramientas de seguimiento de inventario de la red están en funcionamiento

1.6. Asegurar los sistemas de inventario de activos.

1.7. Asegúrese de que estén incluidos en los análisis de vulnerabilidades periódicos y que la información de activos sea verificada.

1.8. Limite el acceso a estos sistemas sólo a personal autorizado, y cuidadosamente registrar todo ese acceso.

1.9. Implementar la autenticación de red a través de 802.1x para limitar y controlar los dispositivos que se pueden conectar a la red.

2. Inventario de software

2.1. Realizar una lista de software autorizado que se requiere en la empresa

2.2. Desplegar herramientas de inventario de software en toda la organización.

2.3. El sistema de inventario de software debe realizar un seguimiento de la versión del SO.

2.4. Monitoreo de software no autorizado instalado en cada máquina.

2.5. Implementar una aplicación que cree una lista blanca que permita los sistemas aprobados.

2.6. Configurar las estaciones de trabajo de clientes con entornos operativos virtualizados no persistentes que pueden ser rápida y fácilmente restaurados a una instantánea de confianza sobre una base periódica.

3. Realización de configuraciones seguras para hardware y software de computadoras móviles, computadoras de escritorios y servidores.

3.1. Crear una imagen segura que se utiliza para construir todos los nuevos sistemas que se implementan en la empresa.

3.2. Las imágenes deben tener la configuración de seguridad aprobada antes del despliegue.

3.3. Actualizar la imagen de forma periódica.

3.4. Actualización de imagen con la recomendación publicada por el NIST, NSA, Defensa Agencia de Sistemas de Información, Centro para la Seguridad en Internet, entre otros.

3.5. Eliminar cuentas innecesarias, deshabilitar o eliminación de servicios innecesarios.

3.6. Aplicar parches, cerrando puertos de red abiertos y no utilizados.

3.7. Ejecutar la última versión del software y asegúrese de que está totalmente parcheado. Quite el software obsoleto o de más del sistema.

3.8. Toda la administración remota de servidores, estaciones de trabajo, dispositivos de red y equipos similares se hará sobre canales seguros.

3.9. Ejecutar evaluación mensual de una muestra variada de sistemas para determinar brechas de seguridad.

3.10 Proporcionar los altos ejecutivos con gráficos que muestran el número de sistemas que responden a las directrices de configuración frente a los que no coinciden.

4. Defensas de malware

4.1 Emplear herramientas de anti-malware, anti -virus, anti -spyware, firewall personal, y la funcionalidad IPS basado en host automatizado.

4.2 Las organizaciones deben configurar ordenadores portátiles, estaciones de trabajo para evitar el contenido auto-run de tokens USB, discos duros USB, CDs / DVDs, u otros medios extraíbles.

4.3 Configurar los sistemas para que realicen un análisis anti-malware automatizado de medios extraíbles cuando se inserten.

4.4 Las herramientas automatizadas de control deberían utilizar la detección de anomalías basado en el comportamiento para complementar y mejorar las firmas de seguridad tradicionales.

4.5 Desplegar herramientas de control de acceso a la red para verificar la configuración de seguridad y cumplimiento a nivel de parche.

4.6 Implementar un proceso de respuesta a incidentes que le permite suministrar a su equipo de seguridad con muestras de malware ejecutándose detectados en los sistemas corporativos.

5. Seguridad de aplicaciones

5.1 Proteger aplicaciones web mediante la implementación de cortafuegos que inspeccionan todo el tráfico.

5.2 Pruebas en la empresa o de terceros desarrolladas para los errores de codificación y la inserción de malware, incluyendo puertas traseras. Si el código fuente no está disponible, estas organizaciones deberían probar el código compilado utilizando herramientas de análisis estáticos binarios.

5.3 Para las aplicaciones de bases de datos comprobar todos los ajustes para asegurar que el sistema de base de datos se ha endurecido utilizando el estándar.

5.4 Verificar que las consideraciones de seguridad se tienen en cuenta a lo largo de los requisitos, diseño, implementación, pruebas y otras fases del ciclo de vida de desarrollo de software de todas las aplicaciones.

5.5 Las organizaciones deben asegurarse de que todo el personal de desarrollo de software reciben capacitación en escribir código seguro.

6. Control de dispositivos inalámbricos.

    6.1 Asegurarse de que todos los dispositivos inalámbricos conectados a la red coincide con una configuración.

    6.2 Asegúrese de que todos los puntos de acceso inalámbricos son manejables utilizando herramientas de gestión empresarial.

    6.3 Red de herramientas de escaneo de vulnerabilidades que se deben configurar para detectar puntos de acceso inalámbricos conectados a la red cableada.

    6.4 Utilizar los sistemas inalámbricos de detección de intrusos (WIDS) para identificar los dispositivos inalámbricos y detectar intentos de ataque y compromisos exitosos.

    6.5 802.1x se debe utilizar para controlar qué dispositivos pueden conectarse a la red inalámbrica.

    6.6 Un estudio del sitio se debe realizar para determinar qué áreas dentro de la organización necesitan cobertura.

    6.7 Asegurase de que cada dispositivo inalámbrico ha sido identificado.

    6.8 La organización debe asegurarse de que todo el tráfico inalámbrico aprovecha al menos Advanced Encryption Standard (AES).

    6.9 Los puntos de acceso inalámbricos nunca deben ser conectados directamente a la red privada.

7. Capacidad de Recuperación de Datos

    7.1 Asegúrese de que cada sistema se respalda automáticamente por lo menos una vez por semana.

7.2 Asegúrese de que la capacidad de restaurar rápidamente un sistema de copia de seguridad, el sistema operativo, software de aplicación y los datos en una máquina deben ser incluidos en el procedimiento de copia de seguridad en general. Estos tres componentes de un sistema no tienen que ser incluidos en el mismo archivo de copia de seguridad o utilizar el mismo software de copia de seguridad.

7.3 El medio de copia de seguridad debe ser probado en forma regular mediante la realización de un proceso de restauración de datos.

7.4 El personal de IT debe estar capacitado en tanto la copia de seguridad y procesos de restauración.

7.5 La organización debe asegurarse de que las copias de seguridad se protegen adecuadamente a través del almacenamiento externo en una bóveda y el cifrado.

7.6 Las copias de seguridad, tales como discos duros y cintas, se deben almacenar en instalaciones físicamente seguras.

8. Asegurar las configuraciones de los dispositivos de red como cortafuegos, routers and switches.

8.1 En los puntos de interconexión de red, implementar el filtrado de entrada y salida para permitir que sólo los puertos y protocolos debidos tengan acceso.

8.2 Todas las nuevas reglas de configuración más allá de una línea de base segura deben ser documentadas y registradas en un sistema de gestión de cambios.

8.3 Tecnologías de filtrado de red empleadas entre redes con diferentes niveles de seguridad deben implementarse con capacidad de filtrar el Protocolo de Internet versión 6 del tráfico (IPv6).

8.4 La última versión estable de un dispositivo de red (IOS) o firmware debe instalarse dentro de los 30 días posteriores a la actualización que sea liberada por el proveedor.

9. Limitación y Control de los puertos de red, protocolos y servicios.

9.1 Firewalls o herramientas de filtrado de puerto deben ser aplicados en los sistemas, con una regla de denegación que despliega todo tráfico excepto aquellos servicios y puertos que se hayan permitido explícitamente.

9.2 Análisis de puertos automatizados deben realizarse sobre una base regular contra todos los servidores.

9.3 Cualquier servidor que es visible desde Internet o desde una red no confiable debe ser verificado, y si no es necesario para fines de negocios deben ser removidos a un VLAN interna y dan una dirección privada.

9.4 Servicios necesarios para el uso del negocio a través de la red interna deben revisarse trimestralmente a través de un control de cambios.

9.5 Los cortafuegos de aplicación deben ser colocados en frente de los servidores críticos para verificar y validar el tráfico que va al servidor. Cualquier servicio o el tráfico no autorizado debe ser bloqueadas y se genere una alerta.

10. Uso Controlado de privilegios administrativos

10.1 Las organizaciones deben utilizar herramientas automatizadas para inventariar todas las cuentas administrativas.

10.2 Cuando nuevos dispositivos se despliegan en la red, todas las contraseñas por defecto para las aplicaciones, los sistemas operativos, routers, cortafuegos, puntos de acceso inalámbricos y otros de esos dispositivos se deben cambiar.

10.3 Configurar todas las cuentas de nivel administrativo para requerir cambios de contraseña regulares en un intervalo de frecuencia de no más de 60 días.

10.4 La organización debe asegurarse de que todas las cuentas de servicio tienen una contraseña compleja y difícil de descifrar.

10.5 Las contraseñas de usuarios deben ser cambiadas de forma periódica, en un intervalo de frecuencia de no más de 90 días.

10.6 Las contraseñas para todos los sistemas deben ser almacenados en un formato cifrado

10.7 Establecer únicas y diferentes contraseñas para sus cuentas de administrador y no administrativos.

11. Límites de Defensa

11.1 Denegar las comunicaciones con direcciones IP maliciosas conocidas (listas negras).

11.2 Implementar sensores IDS basados en red de los sistemas y redes que buscan ataque inusual DMZ Internet y extranet.

11.3 Implementar dispositivos IPS basados en la red para complementar los sistemas IDS bloqueando en caso de un comportamiento detectado de ataques.

11.4 Gestión de la Información del sistema (SEIM), de modo que los eventos pueden ser correlacionados a partir de todos los dispositivos de la red.

11.5 Definir una arquitectura de red que separa claramente los sistemas internos de DMZ y sistemas de extranet.

11.6 Idear esquemas de segmentación de red internos para limitar el tráfico sólo a los servicios necesarios para el uso del negocio a través de la red interna.

11.7 Desarrollar planes para desplegar rápidamente los filtros en las redes internas para ayudar a detener la propagación de malware o un intruso.

12. Mantenimiento , Monitoreo y Análisis de Registros de auditoría

12.1 Asegúrese de que todos los sistemas que almacenan registros tienen suficiente espacio de almacenamiento para los registros generados de forma regular, por lo que los archivos de registro no se llenarán.

12.2 Los registros deben ser archivados y firmados digitalmente sobre una base periódica.

12.3 Todo el acceso remoto a la red, debe generar registros más detallados.

12.4 Los sistemas operativos deben ser configurados para registrar los eventos de control de acceso asociadas a un usuario intentado acceder a un recursos sin los permisos adecuados.

12.5 El personal de seguridad y / o administradores de sistemas deben ejecutar informes quincenales que identifican anomalías en los registros.

12.6 Implementación de una herramienta del sistema SEIM para la agregación de registro y consolidación de varias máquinas y para la correlación de eventos y análisis.

13. Seguimiento y Control de Cuenta

13.1 Revisión de todas las cuentas del sistema y deshabilitar cualquier cuenta que no puede ser asociada a un proceso de negocio y el propietario.

13.2 Establecer y seguir un proceso para revocar el acceso al sistema mediante la desactivación de cuentas inmediatamente después de la desvinculación de un empleado o contratista.

13.3 Monitorear regularmente el uso de todas las cuentas, el registro de forma automática a los usuarios después de un período normal de inactividad.

13.4 Monitorear las cuentas para determinar cuáles no han sido utilizadas durante un período determinado, como por ejemplo 30 días. Después de un período más largo, por ejemplo, de 60 días, la cuenta debe ser desactivada.

13.5 Todas las cuentas que no son administradores deberían ser obligados a tener una longitud mínima de 12 caracteres, contener letras, números y caracteres especiales, cambiarse al menos cada 90 días, tener una edad mínima de un día, y no se le permita utilizar las 15 contraseñas anteriores como una nueva contraseña.

13.6 Después de ocho intentos fallidos de inicio de sesión dentro de un período de 45 minutos, la cuenta debe estar bloqueado durante 120 minutos

13.7 Perfil de uso de la cuenta típica de cada usuario, determinando el acceso normal de hora del día y la duración de acceso para cada usuario.

14. Prevención de Pérdida de Datos

14.1 Implementar software de cifrado de disco duro para máquinas móviles que contienen datos sensibles.

14.2 Analizar una herramienta de monitoreo de red para analizar el tráfico saliente en busca de una variedad de anomalías, incluyendo archivos de gran tamaño, las conexiones persistentes desde hace mucho tiempo, las conexiones a intervalos regulares repetidos, protocolos inusuales y puertos en uso y posiblemente la presencia de ciertas palabras clave en los datos.

14.3 Los datos almacenados en medios de almacenamiento extraíbles y fácilmente transportables, como memorias USB, discos duros portátiles y CDs / DVDs deben estar cifrados.

14.4 Uso de soluciones DLP basados en la red para supervisar y controlar el flujo de datos dentro de la red. Cualquier anomalía que superar los patrones de tráfico normales deben tenerse en cuenta y reciba los cuidados necesarios para hacerles frente.

15. Capacidad de Respuesta a Incidentes

15.1 Asegúrese de que usted ha escrito los procedimientos de respuesta a incidentes que incluyen una definición de las funciones del personal para el manejo de incidentes.

15.2 Asignación de títulos de trabajo y los deberes para el manejo de incidentes informáticos y de red.

15.3 Definir el personal de gestión que apoyen el proceso de gestión de incidentes, actuando en roles de toma de decisiones.

15.4 Publicar información para todo el personal, incluyendo a los empleados y contratistas, en cuanto a anomalías informáticas de informes y los incidentes al equipo de gestión de incidentes.

15.5 Llevar a cabo sesiones de escenarios de incidentes periódica para el personal relacionado con el equipo de gestión de incidentes para asegurar que se comprenden las amenazas actuales y los riesgos, así como sus responsabilidades en el apoyo.

16. Pruebas de Penetración y Ejercicios equipo rojo

16.1 Llevar a cabo pruebas de penetración externas e internas periódicas para identificar las vulnerabilidades y los vectores de ataque que pueden ser utilizados para explotar los sistemas empresariales con éxito.

16.2 La prueba de penetración debe reproducir eventos desde fuera del perímetro de la red, así como desde dentro.

16.3 Realizar ejercicios periódicos del equipo rojo para poner a prueba la disposición de las organizaciones para identificar y detener los ataques o para responder con rapidez y eficacia.

16.4 Asegurar que los problemas sistémicos detectados en las pruebas de penetración y ejercicios en equipo rojo están completamente mitigados.

16.5 Medida de qué tan bien la organización ha reducido

16.6 La ingeniería social se debe incluir dentro de una prueba de penetración.

16.7 Idear un método de puntuación para determinar los resultados de los ejercicios del equipo rojo de modo que los resultados puedan ser comparados

16.8 Crear un banco de pruebas que simula un entorno de producción para pruebas de penetración específicos y los ataques del equipo rojo contra elementos que no se suelen probarse en producción.

Capítulo V

Análisis mundial de la seguridad de la información tecnológica

La seguridad de la información no tiene fronteras, raza, estatus social, industria o gobierno. Desde cualquier parte del mundo una persona o empresa puede ser atacada y dependiendo de las circunstancias del momento pueden elevar el nivel de riesgo que un estado puede afrontar.

Un ejemplo actual es la ocupación rusa de Crimea que ha causado desde una tensión diplomática entre los estados que están a favor y en contra hasta alertas de ciberguerra, según informo la agencia de noticias Reuters el 4 de marzo del 2014: "**El sistema de telecomunicaciones de Ucrania está bajo ataque**, desde Crimea se están interfiriendo los teléfonos móviles de los miembros del parlamento, ha afirmado el jefe del Servicio de Seguridad de Ucrania". Equipos rusos instalados en la empresa de telecomunicaciones Ukrtelecom estaría bloqueando los teléfonos de los parlamentarios de Ucrania.

Hace algunos años las fuerzas militares estadounidense además de sus escuadrones como el ejército, la marina y la fuerza área; creo su propio ejército de “cyber-soldados” entrenados para una ciberguerra. El mundo está siendo azotado por diferentes ciberguerras, cada vez más se ven noticias sobre los escuadrones de hackers chinos, el espionaje de la Agencia de Seguridad Nacional norteamericana (NSA) que es titular semanalmente desde hace meses o los ataques del grupo Sirian Electronic Army.

Tomando esto en cuenta, es un reto para los actuales ejecutivos tomar las decisiones correctas contra estas amenazas que las empresas están expuestas dependiendo del entorno donde desarrollan sus negocios.

5.1 Análisis demográfico de la ciberseguridad en la Republica Dominicana

Las siguientes estadísticas que se presentan fueron generadas por los programas de seguridad de Microsoft y los servicios que se ejecutan en las computadoras en la República Dominicana en el segundo trimestre del año 2013 y el anterior trimestre en el Microsoft Intellegent Report 2013.

Estos datos son proporcionados por los administradores o los usuarios que deciden compartir con Microsoft sus eventos de vulnerabilidades y se utiliza la dirección IP de para determinar país o región.

Durante varios años, el Reporte de Inteligencia de Seguridad de Microsoft ha informado de las infecciones y tipos de infecciones usando una métrica llamada equipos limpiados por mil (CCM). CCM representa el número de equipos limpiados por cada 1.000 ejecuciones de software malicioso con la Herramienta de eliminación de software malicioso (MSRT).

Para comprender mejor la totalidad del software maliciosos, Microsoft está introduciendo un nuevo indicador denominado tasa de encuentro. Esta métrica es el porcentaje de equipos con seguridad en tiempo real

Utilizando en combinación, estas dos perspectivas, proporcionan a Microsoft una valoración global del impacto de software malicioso y sus riesgos.

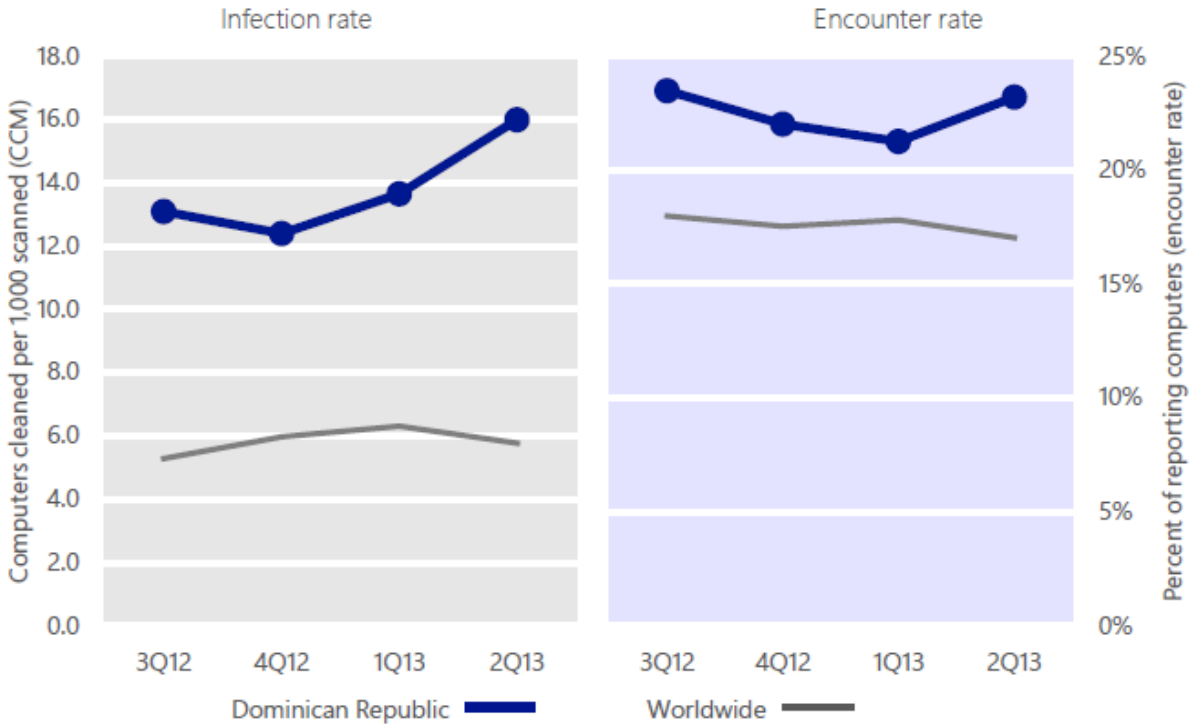
Metric	3Q12	4Q12	1Q13	2Q13
CCM, Dominican Republic	13.1	12.4	13.7	16.0
Worldwide average CCM	*5.3*	*6.0*	*6.3*	*5.8*
Encounter rate, Dominican Republic	23.5%	22.0%	21.3%	23.2%
Worldwide average encounter rate	*18.0%*	*17.5%*	*17.8%*	*17.0%*

Fuente: Microsoft Security Intelligent Report 2013

Tabla 5.1

Tendencias de la infección y la tasa de encuentro

El MSRT limpiar el malware en 16,0 de cada 1.000 ordenadores analizados en la República Dominicana en el periodo analizado (una puntuación de CCM de 16,0, en comparación CCM promedio mundial de 5,8). Un 23,2% de los equipos de la República Dominicana se encontró software malicioso, en comparación con el promedio mundial de 21,7%. La siguiente figura muestra la infección y la evolución de los tipos encuentro para la República Dominicana en los últimos cuatro trimestres, en comparación con el mundo en su conjunto.

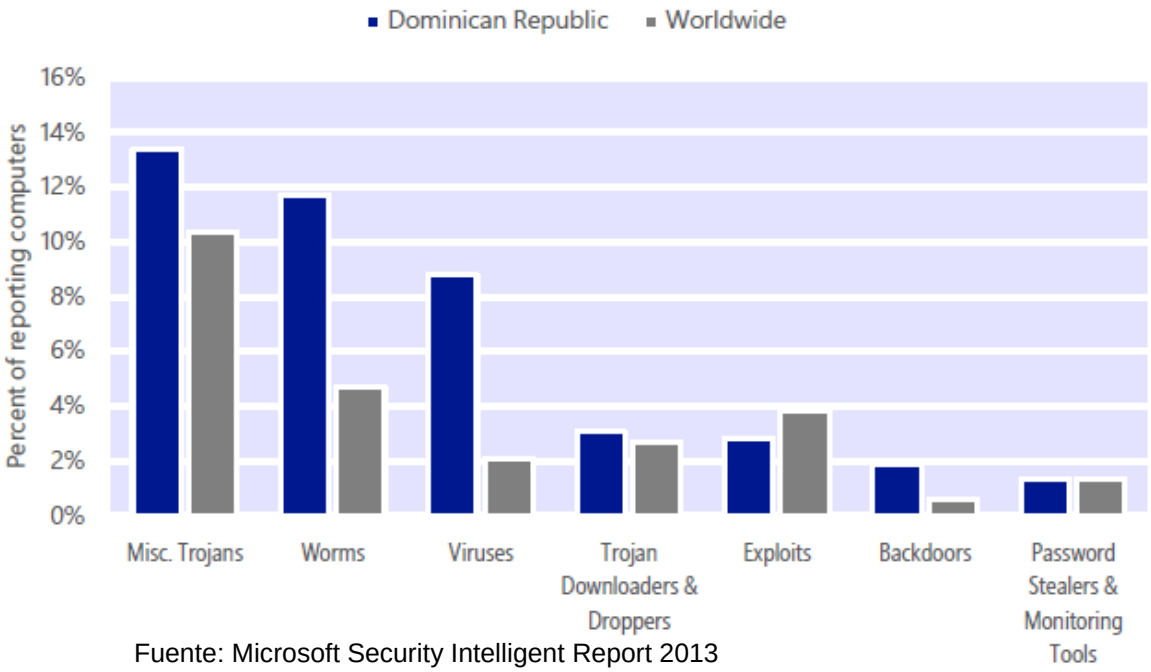


Fuente: Microsoft Security Intelligent Report 2013

Grafica 5.2

.

Categorías de amenazas



Fuente: Microsoft Security Intelligent Report 2013

Grafica 5.3

- La categoría más común en la República Dominicana fueron varias versiones de troyanos. Se encontró un 13,4% de equipos comprometidos, frente al 12,2%.
- La segunda categoría más común en la República Dominicana fue de gusanos. Se encontró un 11,7 % de infecciones, frente al 10,1 por ciento en el trimestre anterior.
- La tercera categoría más común en la República Dominicana fueron infecciones de virus, determinándose en un 11,7% de infecciones, frente al 7,7% del trimestre anterior.

5.2 Conciencia sobre la seguridad de la información

Cada país enfrenta indistintamente la seguridad cibernética, dependiendo de su entorno económico, político y cultural. Algunos países toman en cuenta la seguridad cibernética como un asunto de seguridad nacional y otros como defensa. Otros entienden que tiene un mayor impacto económico o impacta la competitividad. A pesar de la diversidad de opiniones, están surgiendo estudios de casos que ayudarán más eficientemente a mejorar las políticas de seguridad cibernética.

Los gobiernos están enfrentando los avances tecnológicos rápidos con procesos burocráticos que se adaptan con lentitud, lo que juega en contra de ellos mismos y a las organizaciones ilícitas le ofrece vías para operar sin preocuparse mucho. Uno de los principales problemas contra las actividades cibernéticas ilícitas ha sido la falta de legislaciones adecuadas y políticas duras de seguridad cibernética. Conjuntamente la inexperiencia de los investigadores forenses tecnológicos y la escasez de integrantes de la justicia especializados en delitos tecnológicos.

La mayoría de los ataques y sumando a esto la publicidad que se recibe a diario, han logrado modificar las actitudes y mejoras concretas en la seguridad cibernética. Aunque los usuarios del internet siguen ignorando en gran medida los riesgos, los gobiernos se están motivando a enfrentar y buscar resultados positivos. Algunos países han adoptado marcos integrales contra la delincuencia tecnológica. Otros han expresado interés por adoptar este tipo de leyes y han empezado a reunir recursos y voluntad política para ello.

Los países que poseen leyes jurídicas establecidas en marcos sólidos, continúan luchando contra muchas dificultades para establecerla, sumando a esto el efecto los bajos niveles técnicos en seguridad de la información.

Existen países que iniciaron sus esfuerzos en materia de seguridad cibernética con el establecimiento de Computer Security Incident Response Team Services. De hecho, muchos países de Latinoamérica, menos algunos del Caribe, ya disponen de capacidad de respuesta a incidentes.

Incluso los países del Caribe que no han creado todavía un Computer Security Incident Response Team Services reconocen la importante función que desempeña la seguridad cibernética en el desarrollo social y económico. Algunos poseen laboratorios forenses de tecnología o crearan su Computer Security Incident Response Team Services en un futuro cercano. De todas maneras continúan habiendo obstáculos significativos.

Preocupaciones sobre los sistemas de control industrial

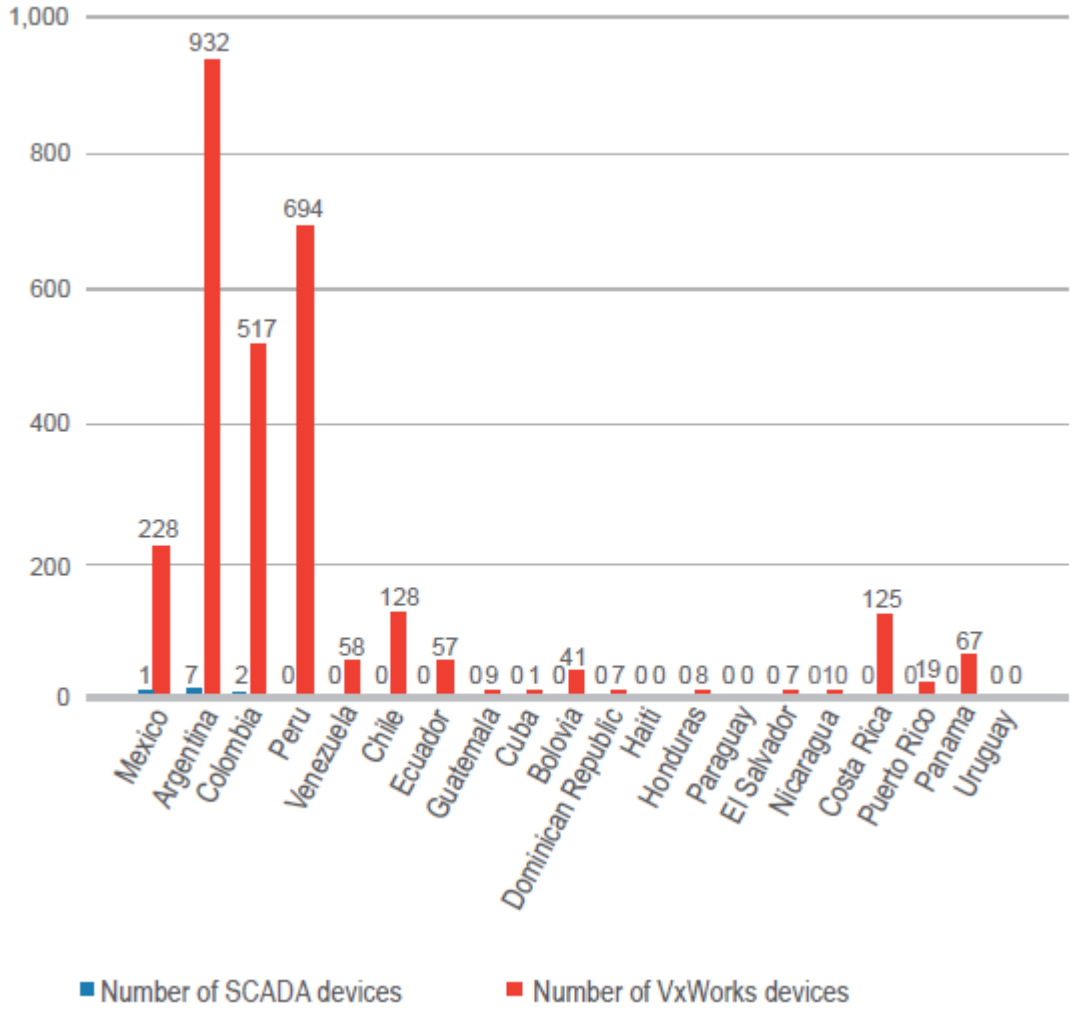
Las estadísticas muestran aumento en los ataques contra infraestructuras críticas. Estas infraestructuras críticas incluyen las que manejan los sectores financieros, de energía y de la salud que dependan de sistemas de control industrial.

Varios de estos sistemas, se conectan a internet, lo que facilita los posibles ataques. Existen estudios de casos que muestras estas amenazas para los sistemas de control industrial.

Gobiernos han reportado ataques contra instituciones financieras de su entorno económico. Estos ataques no solo pueden provocar pérdidas millonarias en el sector sino que pueden contribuir contrariamente a las políticas de inversión extrajeran.

Aunque no existen registros de ataques relacionados con infraestructura crítica que hayan provocado pérdidas millonarias o daños físicos en Américas y el Caribe, sí se hace énfasis en la necesidad de mantener la vigilancia y de mejorar las barreras contra los ataques, porque muchos sistemas continúan estando expuestos.

Un estudio del año 2012 a proveedores de seguridad de sistemas de control industrial, presento que se registraron 171 vulnerabilidades en diversos sistemas de control. Analizando los dos tipos de sistemas de control más comunes, se concluyó que muchos de estos dispositivos estaban conectados al internet.[45]



Fuente: http://www.shodanhq.com/

Grafica 5.4

.

[45] http://www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf, p. 6

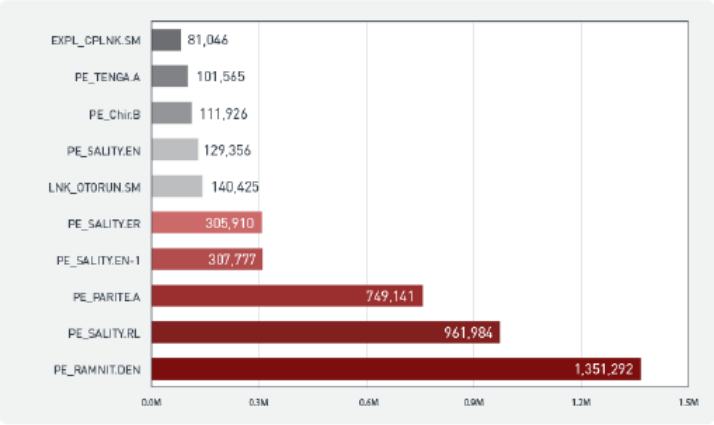
Aunque el uso de sistemas de control industrial conectados al internet no es peligroso en sí, muchos de los sistemas que se muestran no tenían protección por contraseña ni mantenían actualizados los parches de seguridad más recientes, lo cual los dejaba expuestos a ataques.

Un estudio realizado por Trend Micro indicó que los sistemas de control industrial conectados al internet sufren ataques diariamente. Los datos demuestran que en un lapso de 28 días se registró un total de 39 ataques de 14 países distintos. De estos 39 ataques, 12 fueron únicos y podrían clasificarse como "focalizados", mientras que 13 fueron repetidos por varios de los mismos agentes en el transcurso de varios días y podrían considerarse "focalizados" o "automatizados."[46]

5.3 Medición y métricas

Malware[47]

América Latina y el Caribe se vieron afectados más por infecciones de archivos que por cualquier otro tipo de software malicioso, lo que a menudo indica la prevalencia de dispositivos de almacenamiento portables insuficientemente asegurados y la falta de parches en los sistemas operativos o aplicaciones.



Fuente: Trend Micro Smart Protection Network. Grafica 5.5

[46] Ibid

[47] Ibid, p.13

Spam[48]

El volumen mundial de spam (o “correos basura”) se ha ido reduciendo desde 2011debido a enormes desmantelamientos de botnets y otras operaciones policiales seleccionadas con este tipo de mensajes de correo. Sin embargo, falta mucho para que el volumen de spam toque fondo. En 2012, entre los países de América Latina y el Caribe, el principal país originador de spam fue México, seguido por Argentina y Colombia.

Fuente: Tendencias de la seguridad año 2012. Grafica 5.6

[48] Ibid. p 12.

URLs maliciosos[49]

El hospedaje de sitios maliciosos es un grave problema en las Américas y el Caribe.

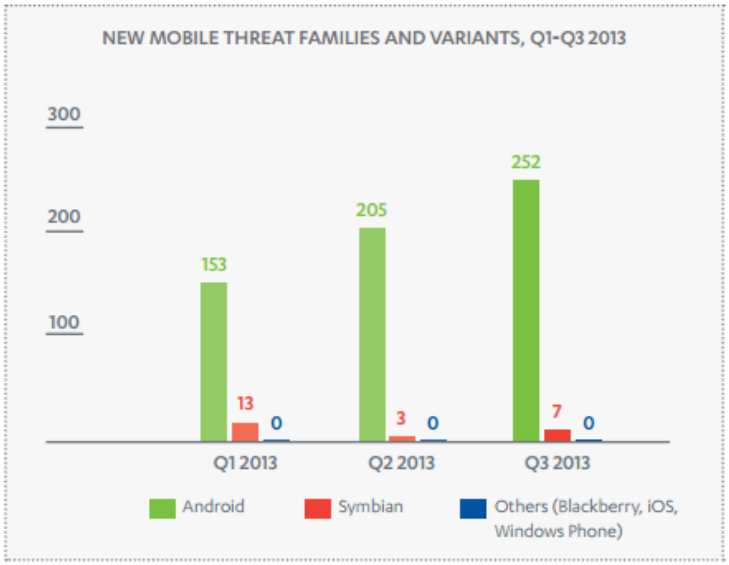
Los dos principales países originarios de spam también ocupan los primeros lugares en la lista de países que albergaron el mayor número de URLs maliciosos. Colombia país que ocupó el tercer lugar en envío de spam fue reemplazado por Chile en la lista de principales alojadores de URLs maliciosos.

Fuente: Tendencias de la seguridad año 2012. Grafica 5.7

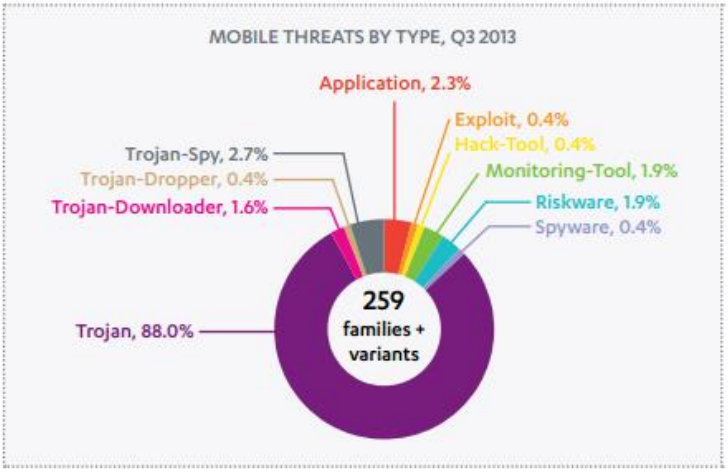
[49] Ibid, p.13.

Malware a móviles

La estadística debajo muestra un crecimiento continua en la cantidad de ataques efectuados entre tres trimestres del año 2013 a los sistemas operativos de celulares Android tomando en consideración que es el sistema operativo más utilizado en los teléfonos inteligentes. En la imagen 5.8 se observa el reporte por tipos de software maliciosos que fueron los ataques.



Fuente: Mobile Threat Report July-September 2013 F-Secure. Grafica 5.8



Fuente: Mobile Threat Report July-September 2013 F-Secure. Grafica 5.9

Conclusión

La implementación de políticas de seguridad informática buscan de una manera integrar, proteger, preservar y gestionar eficientemente los recursos de la organización. También van más lejos, buscando solucionar, evitar y capacitar al personal en cómo enfrentar incidentes que pudieran presentarse con el fin de responder en forma óptima.

Totalmente contrario a lo que se piensa de que la seguridad informática es una barrera para las diversas actividades que se realizan por el hecho de que se deben seguir y respetar procedimientos, recomendaciones, reglas, normas o protocolos que en un momento determinado pudiesen ralentizar una actividad o trabajo que se ejecuta; es un pensamiento equivocado. Debido a que la seguridad de la información con sus normas y procedimientos solo busca realizar un análisis detallado antes y después de una actividad con el fin de garantizar la integridad del activo más importante dentro de la organización que es su información.

Esto es lo que busca esta propuesta; lograr por encima de colocar a AES Dominicana dentro de los estándares mundiales de la seguridad de información sino garantizar de manera íntegra la información, apoyar la continuidad del negocio y trabajar en conjunto la gestión del negocio.

Las políticas de seguridad informática son el sustento para toda iniciativa de este tipo, por lo que es primordial tener una documentación acorde, debe contener protocolos de difusión, revisión, control y actualización como parte de su cilco de vida. Es de extrema importancia que se cuente con el personal capacitado para lograr una buena implementación completa.

En conclusión, se propone la implementación de políticas, procedimientos y normas de seguridad de la información en AES Dominicana, cuyos controles sean seguidos, gestionados y controlados desde el inicio del ciclo de seguridad desde el inicio hasta el final.

Lista de referencias

Bibliográficas

- Kosutic, Dejan (2012). *9 Steps to Cybersecurity* (1ra Ed). EPPS Services LTD, Zagreb, Croazia.
- Clemente, Dave (2013). *Cyber Security and Global Interdependence: What is critical?* (1ra Ed). Chatam House, Estados Unidos.
- Bosworth, Seymour (2008). *Computer Security* (5ta Ed). John Wiley & Sons, Inc. Estados Unidos.

Articulos

- F-Secure Labs (2013). *Mobile Threat Report*. Estados Unidos.
- Tren Micro (2012). *Tendencias en la seguridad cibernética en América Latina y el Caribe*. Centro América.
- Microsoft (2013). *Microsoft Security Intelligences Report*. Estados Unidos.
- Microsoft (2014). *The Cybersecurity Risk Paradox*. Republica Dominicana.

Informes

- Organismo Coordinado del Sistema Eléctrico Nacional Interconectado de la Republica Dominicana (2013). *Informe de operaciones real del año 2013*. República Dominicana.
- Instituto nacional de estadísticas e informática (2012). *Guía práctica para el desarrollo de planes de contingencia de sistemas de información*. Lima, Perú.
- AES Dominicana. *Informe estadístico 2013*. República Dominicana

Referencias web

- Empresa de distribución de electricidad del norte (2011). Reseña del sector eléctrico dominicana. http://www.edenorte.com.do/nuestra-empresa/resena-del-sector-electrico-dominicano/.
- www.aes.com
- www.aesdominicana.com.do
- http://es.wikipedia.org/wiki/Sector_el%C3%A9ctrico_en_la_Rep%C3%BAblica_Dominicana
- http://www.computerworldmexico.mx/Articulos/21498.htm
- http://es.wikipedia.org/wiki/ISO/IEC_27000-series
- http://es.wikipedia.org/wiki/ISO/IEC_27001
- http://es.wikipedia.org/wiki/ISO/IEC_27002
- Electricity Subsector Cybersecurity Capability Maturity Model (Version 1.0 – 31 de mayo del 2012).

  http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf

Anexo 1

Ante Proyecto de Investigación

UNIVERSIDAD APEC

Decanato de Escuela de graduados

TEMA:

"Propuesta de las políticas y procedimientos para la seguridad de la información tecnológica (CYBERSECURITY) en la empresa AES Dominicana, año 2014"

NOMBRE:

Yoel Fabian 2004-0544

"Anteproyecto de la monografía para optar por el título de Maestría de Gerencia y Productividad"

PROFESORA:

Edda Freites

SANTO DOMINGO, R.D. 2014

1. Preguntas de partida

1. ¿De qué se trata la investigación propuesta?

Proponer la implementación de políticas y procedimientos con un mínimo de complimiento del estándar de seguridad de la información de AES Corp en AES Dominicana a ser realizado en el año 2014.

2. ¿En qué contexto se ubica?

Políticas de seguridad de la información de AES Corp en AES Dominicana.

3. ¿Es de interés el tema?

Sí, porque con la implementación y cumplimiento de las políticas y procedimiento de seguridad de la información se garantiza la integridad y confidencialidad de los activos de la empresa frente a las amenazas tecnológicas de hoy en día.

4. ¿Existe información sobre el mismo?

Sí. AES Corp cuenta con las políticas y procedimientos ya documentadas con las que entienden se asegura la información de la empresa frente a intrusos, estándares internacionales, libros, páginas de internet oficiales dedicadas a este fin y enciclopedias.

5. ¿Dónde se puede encontrar o quien tiene la información?

El departamento de seguridad de la información regional y el departamento global de seguridad de la información. Además de libros, manuales, estándares y paginas oficiales de internet.

6. ¿Cuáles son los resultados personales que se esperan?

Lograr que la información como uno de los activos más importante con lo que cuenta la empresa, sea preservada íntegramente por medio de políticas que sean implementadas, cumplidas y se logre la concientización de su importación.

7. ¿Cuáles son los resultados generales que se esperan?

Se espera que se mejore el proceso de gestión de la información y se garantice su seguridad para lograr la confianza de los diferentes departamentos internos de la región. Que AES Dominicana sea ejemplo en materia de seguridad para los demás países de la corporación.

2. Problema de la investigación

2.1 Planteamiento del problema

AES Corporation como una empresa de fama mundial, Fortune 200 de las empresas de generación eléctrica y con presencia en 27 países; adaptándose a las amenazas que se presentan cada día, ha formulado su estándar de seguridad de la información (CYBERSECURITY) para garantizar que la información de la empresa sea gestionada por el personal autorizado.

El propósito de este documento es describir las normas de seguridad obligatorias que deben ser aplicaras y adoptadas por todas las Unidades de Negocio AES estratégicas (SBU). Estas normas establecen los requisitos mínimos de seguridad. Sobre la base de los requerimientos geográficos o reglamentarios específicos, muchas unidades de negocios pueden elegir implementaciones más rigurosas de estas normas.

Considerando que las políticas AES Global de TI tienen como propósito definir las reglas de negocio de alto nivel para la seguridad de la información, estas normas establecen requisitos más detallados sobre cómo se deben implementar las políticas. Las normas fueron escritas con una audiencia prevista de SBU TI directores (y sus equipos).

El cumplimiento de estas normas es obligatoria y será validado a través de un curso "confiar pero verificar" del programa (un esfuerzo de colaboración entre la empresa y las SBUs).

AES Dominicana que pertenece a la SBU MCA&C debe alinearse al estándar de seguridad de la información adecuando la tecnología y procesos necesarios para cumplir con estos requerimientos.

Estas normas se basan en la armonización de los dos modelos clave de seguridad de la informacion: the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the SANS 20 Critical Security Controls for Effective Cyber Defense (SANS 20).

2.2 Formulación del problema

¿Cuáles son las razones de que por la que la empresa AES Dominicana debería implementar políticas y procedimientos que busquen robustecer la seguridad de la información?

2.3 Sistematización del problema

- ¿Por qué AES Corp busca alinear a sus negocios de manera global bajo estándares de seguridad?
- ¿Qué es seguridad de la información y su impacto en el negocio de AES Dominicana?
- ¿Cómo mejorarían la seguridad de la información la implementación de los controles de seguridad?

- ¿Cuáles son los hallazgos o brechas de seguridad de la información presentes en la empresa?
- ¿Qué aportes se obtienen más allá de la seguridad de la información?

3. Objetivos

3.1 Objetivo general

Propuesta de las políticas y procedimientos para la seguridad de la información tecnológica (CYBERSECURITY) en la empresa AES Dominicana, año 2014

Proponer la implementación de las políticas y procedimientos de seguridad de la informacion tecnológica (Cybersecurity) y su impacto en la mejora de los procesos internos de AES Dominicana, durante el año 2014.

3.2 Objetivos específicos

- Identificar las necesidades y el impacto en la implementación de los estándares de seguridad de la información tecnológica (Cybersecurity).
- Presentar los estándares de políticas y procedimientos de seguridad de la información tecnológica (Cybersecurity).
- Recomendar la aplicación de los estándares mínimos de cumplimientos con estándares corporativos de seguridad de la información tecnológica (Cybersecurity). .

.

4. Justificación de la investigación

4.1 Justificación Teórica

La investigación es teórica, porque existe material documental que será soporte para la demostración de la investigación en las diferentes teorías. También existe material teórico en el internet, manuales e instrucciones, en los libros, y conocimientos de los expertos en el área.

4.2 Justificación Metodológica

Se harán entrevistas y cuestionarios a las personas encargadas de la gestión y soporte a la implementación de las políticas y procedimientos de seguridad de la información (Cybersecurity) alineadas a la corporación, para identificar los puntos de mejoras y determinar cuál es la mejor manera de hacer la implementación para el minimo de cumplimiento.

Se realizaran comparaciones con el estado actual y el estado al que se quiere llegar para obtener una referencia del nivel que se lograría alcanzar.

4.3 Justificación Práctica

La investigación es práctica ya que ayuda a aumentar el conocimiento sobre el manejo y control de la información por medio de estándares de clase mundial de seguridad de la información (Cybersecurity) y ayudara robustecer los accesos de materiales en una linea de producción.

5. Marco Referencial

5.1 Marco Teórico

Es importante destacar que en la seguridad de la información no son los datos en sí mismo los que poseen el valor, sino el contenido de la información. Por tal razón, el motivo o el motor para la implementación de medidas de protección, por parte de la empresa o persona que gestiona los datos, es la obligación legal y/o ética personal, de evitar consecuencias negativas para la empresa o personas de las cuales se trata la información. La seguridad de la información debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo para implementar medidas, políticas y procedimientos de protección, que responden a la Seguridad de la Información, es el propio interés de la empresa o persona que gestiona los datos, porque la pérdida de la integridad de los datos, le puede causar un daño (material y/o financiero).

Es importante destacar que en la seguridad de la información no son los datos en sí mismo que guardan poseen el valor, sino el contenido de la información. Por tal razón, el motivo o el motor para la implementación de medidas de protección, por parte de la empresa o persona que gestiona los datos, es la obligación legal y/o ética personal, de evitar consecuencias negativas para la empresa o personas de las cuales se trata la información.

Para proteger contra los ataques cibernéticos, las empresas deben defender vigorosamente sus redes y sistemas de una variedad de amenazas internas y externas. También deben estar preparados para detectar e impedir daños en las actividades de seguimiento de ataque en el interior de una red que ya se ha visto comprometida.

En el periodo 2014, AES Corp además de lineamiento corporativo de este año la implementación de un cumplimiento mínimo de políticas y procedimientos del proyecto de seguridad de la información (Cybersecurity) que es una convergencia de varios estándares internacionales como ISO27000, NERC, SANS e ITIL.

Este proyecto pretende proponer y ayudar a la implementación de las políticas y procedimientos de seguridad de la información para lograr que AES Dominicana no solo alcance su objetivo corporativo como empresa sino que sea menos susceptible a un ataque cibernético que comprometa la integridad de la información.

5.2 Marco Conceptual

Autenticación: La autentificación es el proceso de detectar y comprobar la identidad de una entidad de seguridad examinando las credenciales del usuario y validando esas credenciales contra alguna autoridad.

(http://msdn.microsoft.com/es-es/library/syf5yeat(v=vs.110).aspx)

Confidencialidad: Consiste en asegurar que a la información solo accede quien está autorizado para ellos.

Firewall: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

(http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica))

Identificación (Autenticación): Es el proceso de identificar al cliente de la aplicación o servicio. No olvidar que los clientes pueden ser tanto personas, como otros servicios, procesos y otros ordenadores. (La seguridad, confidencialidad y disponibilidad de la información clínica, Jose Antonio Garbayo, p. 5.),

Integridad: Conjunto de acciones que garantizan que la información no se ha transformado durante su procesado, transporte o almacenamiento. (La seguridad, confidencialidad y disponibilidad de la información clínica, Jose Antonio Garbayo, p. 5.).

ISO: La Organización Internacional de Normalización o ISO, nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. (http://www.iso.org/iso/home.html).

ITIL: La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. (http://www.itil-officialsite.com/)

Procedimientos es el cauce formal de la serie de actos en que se concreta la actuación administrativa para la realización de un fin.

SANS: El Instituto SANS (SysAdmin Audit, Networking and Security Institute) es una institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios, agencias gubernamentales, etc.). (http://www.sans.org/)

Seguridad: Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

Seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

5.3 Marco Espacial

El proyecto se realizará en la empresa AES Dominicana, Santo Domingo, Distrito Nacional, Republica Dominicana.

5.4 Marco Temporal

La investigación se realizará durante el año 2014

6. Hipótesis

6.1 Primer grado

La corporación AES ha desarrollado un plan de gestión y control de la información, donde cada negocio deberá duran el año 2014 al menos cumplir con el estándar mínimo de Seguridad de la Información (Cybersecurity). Se realizaran las propuestas de implementación.

6.2 Segundo grado

AES Dominicana debe adecuarse por medio de sus diferentes sistemas y procesos al mínimo de las políticas y procedimientos de seguridad de la información (Cybersecury) de AES Corp. Aunque cuenta con sistemas de seguridad avanzados poseen puntos de mejoras.

7. Aspectos Metodológicos

7.1 Tipos de estudio

En la presente investigación se utilizaran los siguientes tipos de estudio:

Descriptivo, este será utilizado para dar detalles de las variables que intervienen. Esta investigación detallará las razones por la cual AES Corp coloca como un objetivo de alto grado de importancia la implementación de estos estándares de seguridad de la información en sus empresas y la propuesta de implementación en AES Dominicana.

Explicativo, este estudio será utilizado para dar explicación a los hechos y fenómenos planteados de la investigación.

7.2 Métodos de investigación

Explicativo: El tipo de método empleado en este proyecto es explicativo, puesto que se podrá realizar una relación causa y efecto sobre la propuesta de la propuesta de políticas y procedimientos para la seguridad de la información en AES Dominicana.

7.3 Fuentes y técnicas de la investigación

7.3.1 Fuentes Documentales

Fuentes primarias: las fuentes seleccionadas serán los documentos levantados por AES Corp.

Fuentes secundarias: las fuentes secundarias serán los documentos soporte que utiliza el equipo de Cybersecurity de AES Dominicana para apoyar sus labores dentro del tema.

7.3.2 Fuentes técnicas

Entre las técnicas de recolección de información que se utilizarán en la investigación serán:

Encuestas: se realizara una encuesta como método de recopilación de la información para determinar el estado actual de la seguridad en la empresa.

Entrevistas: se realizaran entrevistas al encargado del área de seguridad de la información, al encargado del área de networking, al encargado del área de computación personal y al encargado del are de Hosting DataCenter.

Análisis de documentación: se analizarán las informaciones de las fuentes primarias y secundarias como son los artículos en Internet, libros, manuales, entre otros.

8. Tabla de contenido

9. Bibliografía preliminar

9.1 Libros

- Whyne, Eric, *Computer Security*, Seymour Boswoth, 5ta Edición, Volumen 1
- Clemente, Dave, *Cyber Security and Global Interdependence: What is critical?*, Chatam House
- Sommer, Peter, *Reducing Systemic Cybersecurity Risk*, OECD, Febrero 2013

9.2 Diccionario

- http://lema.rae.es/drae/, Diccionario en línea de la Real Academia de la Lengua Española. .

9.3 Manuales

- Introducción a la seguridad de la información, Junio 2006
- Guía práctica para el desarrollo de planes de contingencia de sistemas de información.
- AES Cybersecurity mínimum requirements, Agosto 2013
- Cybersecurity Risk Paradox, Microsoft Febrero 2014
- 9 Steps to Cybersecurity, Dejan Kosutic, 2012
- Sans Analyst Program, Junio 2013
- Seguridad por niveles, Alejandro Coerletti Estrada

10. Cronograma de trabajo

Actividades	Meses												
	1			2				3				4	
	Semanas												
	2	3	4	1	2	3	4	1	2	3	4	1	2
Etapa #1													
Ajuste del Anteproyecto													
Entrevistas con los usuarios y expertos en el tema													
Etapa #2													
Ajuste de instrumentos para la recolección de información													
Recolección de Datos													
Tabulación de la información													
Análisis e Interpretación de la información													
Etapa #3													
Elaboración del informe final													
Revisión del informe por parte del asesor													
Reajuste luego de revisión final													
Entrega del informe final													

11. Presupuesto

	Monto Estimado	
	Ingresos	**Egresos**
Recursos Propios	RD$64,600.00	
Total Ingresos	**RD$64,600.00**	
Gastos:		
Honorarios de los investigadores		RD$30,000.00
Pago De Asesores		RD$20,000.00
Pago digitación, encuadernación e impresión de informaciones		RD$ 2,500.00
Compra de papel para impresión		RD$ 600.00
Empastado		RD$ 600.00
Fotocopias		RD$ 400.00
Transporte		RD$ 5,500.00
Pago De Internet		RD$ 1,500.00
otros gastos		RD$ 3,500.00
Total Egresos		**RD$64,600.00**

Anexo II

20 SANS Top Critical Security Controls